```
################################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                     20 21222324


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                     20 21222324


    personal_str is  <empty>
```

```
    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                      01 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                 D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


    temp =
                 D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                      02 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                 79901438 34A5C256 AB283936 6D96348C FE8C97AB


    temp =
                         D08FB441 F2F4CB37 CF6C2420 A82C7427
        ACF7FCFD 79901438 34A5C256 AB283936 6D96348C FE8C97AB
```

```
    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                        03 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                6767B05E 83A98040 6D94BEE3 3CBB8905 551B5451


    temp =
                                               D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


  V is
                                               D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC
```

```
    temp =
                54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    temp =
                          54C5217B 5102D8DA 8BF1686E DBAB2BBC
        0C11B0CC B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                               03 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                863DA881 FFCBB434 A6CCB7DA 2FB21018 3D9DB3CF


    temp =
                                              54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


  C is
                                              54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


----------------------------------------------------------------

First call to Generate
```

```
************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    w_i is
                 9F7CFF1E CA23E750 F6632696 9F11800F 12088BA6


    W is
                 9F7CFF1E CA23E750 F6632696 9F11800F 12088BA6


    ------------

    i = 2

    data is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB8A


    w_i is
                 8E441D15 D888B3FE 12BF66FE 057494F4 546DE2F1


    W is
                         9F7CFF1E CA23E750 F6632696 9F11800F
        12088BA6 8E441D15 D888B3FE 12BF66FE 057494F4 546DE2F1
```

```
  returned_bits is
                          9F7CFF1E CA23E750 F6632696 9F11800F
        12088BA6 8E441D15 D888B3FE 12BF66FE 057494F4 546DE2F1


---------------------------

  Update V

    0x03||V is
                                             03D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    H is
                50888157 B42BE85F 4C53E8A1 B0AE46F9 91961027


  Updated values

  V is
                                               2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9DF A7D00ABE 4E198DB8 2CD75DD6 25C2A870 4F027DC1


  reseed_counter is
                                                 0000 00000002


rnd_val is
                          9F7CFF1E CA23E750 F6632696 9F11800F
        12088BA6 8E441D15 D888B3FE 12BF66FE 057494F4 546DE2F1


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen
```

```
    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9DF A7D00ABE 4E198DB8 2CD75DD6 25C2A870 4F027DC1


    w_i is
                 B77AA5C0 CD55BBCE ED7574AF 223AFD98 8C7EEC8E


    W is
                 B77AA5C0 CD55BBCE ED7574AF 223AFD98 8C7EEC8E


    ------------

    i = 2

    data is
                                                2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9DF A7D00ABE 4E198DB8 2CD75DD6 25C2A870 4F027DC2


    w_i is
                 FF4A94E5 E89D26A0 4F58FA79 F5E0D370 2D7A9A6A


    W is
                          B77AA5C0 CD55BBCE ED7574AF 223AFD98
        8C7EEC8E FF4A94E5 E89D26A0 4F58FA79 F5E0D370 2D7A9A6A


  returned_bits is
                          B77AA5C0 CD55BBCE ED7574AF 223AFD98
        8C7EEC8E FF4A94E5 E89D26A0 4F58FA79 F5E0D370 2D7A9A6A


---------------------------

  Update V

    0x03||V is
                                              032554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9DF A7D00ABE 4E198DB8 2CD75DD6 25C2A870 4F027DC1
```

```
    H is
                4B2D04CB 62511A9A 13BDB8D9 BFBFB8A2 C42435B5


  Updated values

  V is
                                                7A19F7 3894FA7C
        ECE74EF4 FE5F82CB 9FC51B5E 96DB7172 7ECCEF60 8284B9CF
        A9F1FD8A BD460C58 9EF0E5FA C294E264 1A292DCA ED566588


  reseed_counter is
                                                 0000 00000003


rnd_val is
                          B77AA5C0 CD55BBCE ED7574AF 223AFD98
        8C7EEC8E FF4A94E5 E89D26A0 4F58FA79 F5E0D370 2D7A9A6A


###############################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                               000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                               808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                               C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                 20 21222324
```

```
    PersonalizationString = <empty>

    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##############################################################

**************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    no_of_bits_to_return = 440

    ------------

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
                  01 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


temp =
             D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


------------

i = 2

counter||no_of_bits_to_return||input_string is
                  02 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             79901438 34A5C256 AB283936 6D96348C FE8C97AB


temp =
                     D08FB441 F2F4CB37 CF6C2420 A82C7427
    ACF7FCFD 79901438 34A5C256 AB283936 6D96348C FE8C97AB


------------

i = 3

counter||no_of_bits_to_return||input_string is
                  03 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             6767B05E 83A98040 6D94BEE3 3CBB8905 551B5451


temp =
                                          D08FB4 41F2F4CB
    37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
    366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89
```

```
  V is
                                                 D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


    temp =
                54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    temp =
```

```
                        54C5217B 5102D8DA 8BF1686E DBAB2BBC
        0C11B0CC B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                               03 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                863DA881 FFCBB434 A6CCB7DA 2FB21018 3D9DB3CF


    temp =
                                              54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


  C is
                                              54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


--------------------------

  Process additional_input

    0x02||V||additional_input is
                           02D08F B441F2F4 CB37CF6C 2420A82C
```

```
        7427ACF7 FCFD7990 143834A5 C256AB28 39366D96 348CFE8C
        97AB6767 B05E83A9 80406D94 BEE33CBB 89606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    w=Hash(0x02||V||additional_input) is
                 9D19D4FF 31B805CA 44B1220A 8363DFCC F2F10DE2


    V is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9635 2A186196 DD1F6D7A A334CB8A C3D1748B D62DC96B


---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9635 2A186196 DD1F6D7A A334CB8A C3D1748B D62DC96B


    w_i is
                 E76B4EDD 5C865BC8 AFD809A5 9B69B429 AC7F4352


    W is
                 E76B4EDD 5C865BC8 AFD809A5 9B69B429 AC7F4352


    ------------

    i = 2

    data is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9635 2A186196 DD1F6D7A A334CB8A C3D1748B D62DC96C


    w_i is
                 A579BCF3 F75E5624 9A3491F8 7C3CA684 8B0FAB25
```

```
    W is
                          E76B4EDD 5C865BC8 AFD809A5 9B69B429
        AC7F4352 A579BCF3 F75E5624 9A3491F8 7C3CA684 8B0FAB25


  returned_bits is
                          E76B4EDD 5C865BC8 AFD809A5 9B69B429
        AC7F4352 A579BCF3 F75E5624 9A3491F8 7C3CA684 8B0FAB25


---------------------------

  Update V

    0x03||V is
                                             03D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9635 2A186196 DD1F6D7A A334CB8A C3D1748B D62DC96B


    H is
                CA5C66D5 67C78BEF B7A32D13 387D5315 93268E18


  Updated values

  V is
                                               2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9E0 BEBDC53B 336D3712 DCD7C452 30F59459 43840994


  reseed_counter is
                                                0000 00000002


rnd_val is
                          E76B4EDD 5C865BC8 AFD809A5 9B69B429
        AC7F4352 A579BCF3 F75E5624 9A3491F8 7C3CA684 8B0FAB25


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320
```

```
  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Process additional_input

    0x02||V||additional_input is
                            022554 D5BD43F7 A4125B5D 8C8F83D7
        9FE3B909 ADCA2A80 C35B80CA 916C97F1 04702FC9 E0BEBDC5
        3B336D37 12DCD7C4 5230F594 59438409 94A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                 FF5BDE25 5EE18D94 DB9ACE0C 1784FFD2 23E36123


    V is
                                                  2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9E1 BE19A360 924EC4A7 B872925E 487A942B 67676AB7


---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                  2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9E1 BE19A360 924EC4A7 B872925E 487A942B 67676AB7


    w_i is
                 6577B6B4 F87A9324 0B199FE5 1A3B3353 13683103


    W is
                 6577B6B4 F87A9324 0B199FE5 1A3B3353 13683103
```

```
    ------------

    i = 2

    data is
                                              2554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9E1 BE19A360 924EC4A7 B872925E 487A942B 67676AB8


    w_i is
                DECE171E 3256FB7E 803586CA 4E45DD24 2EB01F70


    W is
                         6577B6B4 F87A9324 0B199FE5 1A3B3353
        13683103 DECE171E 3256FB7E 803586CA 4E45DD24 2EB01F70


  returned_bits is
                         6577B6B4 F87A9324 0B199FE5 1A3B3353
        13683103 DECE171E 3256FB7E 803586CA 4E45DD24 2EB01F70


---------------------------

  Update V

    0x03||V is
                                             032554D5 BD43F7A4
        125B5D8C 8F83D79F E3B909AD CA2A80C3 5B80CA91 6C97F104
        702FC9E1 BE19A360 924EC4A7 B872925E 487A942B 67676AB7


    H is
                DECE171E 3256FB7E 803586CA 4E45DD24 2EB01F70


  Updated values

  V is
                                               7A19F7 3894FA7C
        ECE74EF4 FE5F82CB 9FC51B5E 96DB7172 7ECCEF60 8284B9CF
        A9F1FD8D 1D51776A 1C4320BD C8F3C8D9 5A40D7CE 6D14D5FC


  reseed_counter is
                                                 0000 00000003


rnd_val is
```

```
                        6577B6B4 F87A9324 0B199FE5 1A3B3353
        13683103 DECE171E 3256FB7E 803586CA 4E45DD24 2EB01F70


###############################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                              C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                 20 21222324


    PersonalizationString =
                                              404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
```

```
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                   000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
        01000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


    temp =
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


    ------------

    i = 2
```

```
    counter||no_of_bits_to_return||input_string is
        02000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    temp =
                          99B9537B 8427B8CE 23219A61 1CBE6106
        44CF8503 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
        03000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 E02E85A2 314CE3D7 4A93324B 27BDE85F 5498B7AC


    temp =
                                             99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  V is
                                             99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                           0099B953 7B8427B8
```

```
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


Hash(counter||no_of_bits_to_return||input_string) is
             A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


temp =
             A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


Hash(counter||no_of_bits_to_return||input_string) is
             D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


temp =
                      A70266F7 F91EC4D2 88731479 34CEAF2A
    2CC35A0F D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                 F485DA6C BF0416DC DC5FB8BC 9C94B6BC 511E0813


    temp =
                                                A70266 F7F91EC4
         D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
         F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


  C is
                                                A70266 F7F91EC4
         D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
         F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                99B953 7B8427B8
         CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
         8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    w_i is
                 AB438BD3 B01A0AF8 5CFEE29F 7D7B7162 1C4908B9


    W is
                 AB438BD3 B01A0AF8 5CFEE29F 7D7B7162 1C4908B9
```

```
    ------------

    i = 2

    data is
                                                99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE9


    w_i is
                09124D43 0E7B406F B1086EA9 94C582E0 D656D989


    W is
                         AB438BD3 B01A0AF8 5CFEE29F 7D7B7162
        1C4908B9 09124D43 0E7B406F B1086EA9 94C582E0 D656D989


  returned_bits is
                         AB438BD3 B01A0AF8 5CFEE29F 7D7B7162
        1C4908B9 09124D43 0E7B406F B1086EA9 94C582E0 D656D989


---------------------------

  Update V

    0x03||V is
                                              0399B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    H is
                5A78428C 33721011 3DA9EB00 17A5D327 B3372ACB


  Updated values

  V is
                                                40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976472 0DB05097 A746C471 4C9A3BFA CBCCC612 BAFB7D6A


  reseed_counter is
                                                  0000 00000002


rnd_val is
```

```
                        AB438BD3 B01A0AF8 5CFEE29F 7D7B7162
        1C4908B9 09124D43 0E7B406F B1086EA9 94C582E0 D656D989


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                            40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976472 0DB05097 A746C471 4C9A3BFA CBCCC612 BAFB7D6A


    w_i is
                29D9098F 987E7005 314A0F51 B3DD2B81 22F4AED7


    W is
                29D9098F 987E7005 314A0F51 B3DD2B81 22F4AED7


    ------------

    i = 2

    data is
                                            40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976472 0DB05097 A746C471 4C9A3BFA CBCCC612 BAFB7D6B


    w_i is
                06735DE6 AD5DDBF2 23177C1E 5F3AEBC5 2FAB90B9
```

```
    W is
                          29D9098F 987E7005 314A0F51 B3DD2B81
        22F4AED7 06735DE6 AD5DDBF2 23177C1E 5F3AEBC5 2FAB90B9


  returned_bits is
                          29D9098F 987E7005 314A0F51 B3DD2B81
        22F4AED7 06735DE6 AD5DDBF2 23177C1E 5F3AEBC5 2FAB90B9


---------------------------

  Update V

    0x03||V is
                                            0340BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976472 0DB05097 A746C471 4C9A3BFA CBCCC612 BAFB7D6A


    H is
                800B98DD 1013A49B 0851E244 7961FB97 F3733076


  Updated values

  V is
                                              E7BE21 6B766542
        733407C3 53865BBF 5A9E5639 239A85CF 98AD563E D3832833
        7A908D54 1A1F1002 D24EEEE6 C1AB2256 220B2163 6B0B4298


  reseed_counter is
                                                0000 00000003


rnd_val is
                          29D9098F 987E7005 314A0F51 B3DD2B81
        22F4AED7 06735DE6 AD5DDBF2 23177C1E 5F3AEBC5 2FAB90B9


################################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
```

```
    EntropyInput =
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                    20 21222324


    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                    20 21222324


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                   000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
        01000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


    temp =
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
        02000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
```

```
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    temp =
                          99B9537B 8427B8CE 23219A61 1CBE6106
        44CF8503 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
        03000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 E02E85A2 314CE3D7 4A93324B 27BDE85F 5498B7AC


    temp =
                                              99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  V is
                                              99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8
```

```
no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


Hash(counter||no_of_bits_to_return||input_string) is
             A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


temp =
             A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


Hash(counter||no_of_bits_to_return||input_string) is
             D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


temp =
                      A70266F7 F91EC4D2 88731479 34CEAF2A
    2CC35A0F D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 0099B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


Hash(counter||no_of_bits_to_return||input_string) is
             F485DA6C BF0416DC DC5FB8BC 9C94B6BC 511E0813
```

```
    temp =
                                                A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


  C is
                                                A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Process additional_input

    0x02||V||additional_input is
                            0299B9 537B8427 B8CE2321 9A611CBE
        610644CF 8503EEC5 BA22DE1A B212C3D0 858E9E3B 9026D4E7
        7D58E02E 85A2314C E3D74A93 324B27BD E8606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    w=Hash(0x02||V||additional_input) is
                 AC253890 BEDFF91D BCBB8272 D02C21DA F03A34F0


    V is
                                                99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 D2FA200E 17C027A3 5EECCF56 A776B50D 3B61F2D8
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 D2FA200E 17C027A3 5EECCF56 A776B50D 3B61F2D8


    w_i is
                F1BC207E EB432886 094421F3 A63493FA 666DC2C4


    W is
                F1BC207E EB432886 094421F3 A63493FA 666DC2C4


    ------------

    i = 2

    data is
                                                99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 D2FA200E 17C027A3 5EECCF56 A776B50D 3B61F2D9


    w_i is
                2AC598CA 0986F692 9FE367F8 0311CA5A B9880D80


    W is
                         F1BC207E EB432886 094421F3 A63493FA
        666DC2C4 2AC598CA 0986F692 9FE367F8 0311CA5A B9880D80


  returned_bits is
                         F1BC207E EB432886 094421F3 A63493FA
        666DC2C4 2AC598CA 0986F692 9FE367F8 0311CA5A B9880D80


---------------------------

  Update V
```

```
    0x03||V is
                                                0399B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 D2FA200E 17C027A3 5EECCF56 A776B50D 3B61F2D8


    H is
                 FCC41757 C0FC70A2 8251F561 A52504F5 BD602531


  Updated values

  V is
                                                  40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976473 5C215DF3 F3B11E20 4DFDC8CF 297819BB B55EACC0


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          F1BC207E EB432886 094421F3 A63493FA
        666DC2C4 2AC598CA 0986F692 9FE367F8 0311CA5A B9880D80


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


--------------------------

  Process additional_input

    0x02||V||additional_input is
                            0240BB BA737D46 7DA0AB94 AEDA518D
        10307192 DF13C4A5 C4DDC5B8 7873237C 5C849764 735C215D
        F3F3B11E 204DFDC8 CF297819 BBB55EAC C0A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
```

```
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                 108B9D20 24618A08 D862EABD CACBFC4D 261DB816


    V is
                                                40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976473 6CACFB14 1812A829 2660B38C F4441608 DB7C64D6


----------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976473 6CACFB14 1812A829 2660B38C F4441608 DB7C64D6


    w_i is
                 CEF3D601 F2744E37 16A9D04F 9AA8481A 98D74518


    W is
                 CEF3D601 F2744E37 16A9D04F 9AA8481A 98D74518


    ------------

    i = 2

    data is
                                                40BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976473 6CACFB14 1812A829 2660B38C F4441608 DB7C64D7


    w_i is
                 D223014F EF8C8456 2708F833 A99817DD 62B7C90B


    W is
```

```
                        CEF3D601 F2744E37 16A9D04F 9AA8481A
        98D74518 D223014F EF8C8456 2708F833 A99817DD 62B7C90B


  returned_bits is
                        CEF3D601 F2744E37 16A9D04F 9AA8481A
        98D74518 D223014F EF8C8456 2708F833 A99817DD 62B7C90B


---------------------------

  Update V

    0x03||V is
                                            0340BBBA 737D467D
        A0AB94AE DA518D10 307192DF 13C4A5C4 DDC5B878 73237C5C
        84976473 6CACFB14 1812A829 2660B38C F4441608 DB7C64D6


    H is
                3018C221 DFEEDDF0 43315A7D A9F4DC3A 91A0E9F1


  Updated values

  V is
                                              E7BE21 6B766542
        733407C3 53865BBF 5A9E5639 239A85CF 98AD563E D3832833
        7A908D55 2928E3C4 12F60BF3 D6511221 7B1551FC 29B9E37F


  reseed_counter is
                                                0000 00000003


rnd_val is
                        CEF3D601 F2744E37 16A9D04F 9AA8481A
        98D74518 D223014F EF8C8456 2708F833 A99817DD 62B7C90B


##############################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
```

```
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                    20 21222324


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324
```

```
no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                  01 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


temp =
             D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


------------

i = 2

counter||no_of_bits_to_return||input_string is
                  02 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             79901438 34A5C256 AB283936 6D96348C FE8C97AB


temp =
                     D08FB441 F2F4CB37 CF6C2420 A82C7427
    ACF7FCFD 79901438 34A5C256 AB283936 6D96348C FE8C97AB


------------

i = 3

counter||no_of_bits_to_return||input_string is
                  03 000001B8 00010203 04050607 08090A0B
    0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
    24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


Hash(counter||no_of_bits_to_return||input_string) is
             6767B05E 83A98040 6D94BEE3 3CBB8905 551B5451
```

```
    temp =
                                                D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


  V is
                                                D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


----------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                 54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


    temp =
                 54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                 B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    temp =
                          54C5217B 5102D8DA 8BF1686E DBAB2BBC
        0C11B0CC B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                03 000001B8 00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    Hash(counter||no_of_bits_to_return||input_string) is
                 863DA881 FFCBB434 A6CCB7DA 2FB21018 3D9DB3CF


    temp =
                                               54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


  C is
                                               54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


-----------------------------------------------------------------

First call to Generate

*****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

Generate FAILED: Reseed is required
-----------------------------------------------------------------
```

```
Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input <empty>

----------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                           01D08F B441F2F4 CB37CF6C 2420A82C
        7427ACF7 FCFD7990 143834A5 C256AB28 39366D96 348CFE8C
        97AB6767 B05E83A9 80406D94 BEE33CBB 89808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                01000001 B801D08F B441F2F4 CB37CF6C 2420A82C
        7427ACF7 FCFD7990 143834A5 C256AB28 39366D96 348CFE8C
        97AB6767 B05E83A9 80406D94 BEE33CBB 89808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                0A0441A5 2BEDF794 F5AA627B CBD81F93 E011D51F


    temp =
                0A0441A5 2BEDF794 F5AA627B CBD81F93 E011D51F


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                02000001 B801D08F B441F2F4 CB37CF6C 2420A82C
        7427ACF7 FCFD7990 143834A5 C256AB28 39366D96 348CFE8C
        97AB6767 B05E83A9 80406D94 BEE33CBB 89808182 83848586
```

```
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                 3474802C 37507675 51B45B69 F3D35939 C932AE1C


    temp =
                          0A0441A5 2BEDF794 F5AA627B CBD81F93
        E011D51F 3474802C 37507675 51B45B69 F3D35939 C932AE1C


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                 03000001 B801D08F B441F2F4 CB37CF6C 2420A82C
        7427ACF7 FCFD7990 143834A5 C256AB28 39366D96 348CFE8C
        97AB6767 B05E83A9 80406D94 BEE33CBB 89808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                 B7C9894F B88465E0 CFD1CC26 1E22C5CB 08918264


    temp =
                                              0A0441 A52BEDF7
        94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
        69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


  V is
                                              0A0441 A52BEDF7
        94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
        69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            000A0441 A52BEDF7
        94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
        69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


    no_of_bits_to_return = 440
```

```
------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 000A0441 A52BEDF7
    94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
    69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


Hash(counter||no_of_bits_to_return||input_string) is
             0411C8B0 DBA756E8 842B3FB0 2D2FEB7C EEA56742


temp =
             0411C8B0 DBA756E8 842B3FB0 2D2FEB7C EEA56742


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 000A0441 A52BEDF7
    94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
    69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


Hash(counter||no_of_bits_to_return||input_string) is
             EE9379C9 0E6D3B2F 1010D40F 4F4DCADA 61CFDFB4


temp =
                       0411C8B0 DBA756E8 842B3FB0 2D2FEB7C
    EEA56742 EE9379C9 0E6D3B2F 1010D40F 4F4DCADA 61CFDFB4


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 000A0441 A52BEDF7
    94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
    69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


Hash(counter||no_of_bits_to_return||input_string) is
             8AF847CA CC4C92C6 144485C2 27CA05B7 A3796150
```

```
    temp =
                                                0411C8 B0DBA756
        E8842B3F B02D2FEB 7CEEA567 42EE9379 C90E6D3B 2F1010D4
        0F4F4DCA DA61CFDF B48AF847 CACC4C92 C6144485 C227CA05


  C is
                                                0411C8 B0DBA756
        E8842B3F B02D2FEB 7CEEA567 42EE9379 C90E6D3B 2F1010D4
        0F4F4DCA DA61CFDF B48AF847 CACC4C92 C6144485 C227CA05


************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                0A0441 A52BEDF7
        94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
        69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


    w_i is
                56EF4913 373994D5 539F4D7D 17AFE744 8CDF5E72


    W is
                56EF4913 373994D5 539F4D7D 17AFE744 8CDF5E72


    ------------

    i = 2

    data is
                                                0A0441 A52BEDF7
        94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
        69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C6
```

```
    w_i is
                416CC6A7 1A340059 FA0D5AE5 26B23250 C46C0944


    W is
                         56EF4913 373994D5 539F4D7D 17AFE744
         8CDF5E72 416CC6A7 1A340059 FA0D5AE5 26B23250 C46C0944


  returned_bits is
                         56EF4913 373994D5 539F4D7D 17AFE744
         8CDF5E72 416CC6A7 1A340059 FA0D5AE5 26B23250 C46C0944


---------------------------

  Update V

    0x03||V is
                                            030A0441 A52BEDF7
         94F5AA62 7BCBD81F 93E011D5 1F347480 2C375076 7551B45B
         69F3D359 39C932AE 1CB7C989 4FB88465 E0CFD1CC 261E22C5


    H is
                2681DFB1 64FD2DE2 4340EDAF 404D2DC2 E732C72E


  Updated values

  V is
                                              0E160A 5607954E
         7D79D5A2 2BF9080B 10CEB73C 622307F9 F545BDB1 A461C52F
         79432124 3AACE23F 363FEFB3 5DC5BEA7 E7314414 CF78B3F9


  reseed_counter is
                                                0000 00000002


rnd_val is
                         56EF4913 373994D5 539F4D7D 17AFE744
         8CDF5E72 416CC6A7 1A340059 FA0D5AE5 26B23250 C46C0944


---------------------------------------------------------------

Second call to Generate

***************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            010E16 0A560795 4E7D79D5 A22BF908
        0B10CEB7 3C622307 F9F545BD B1A461C5 2F794321 243AACE2
        3F363FEF B35DC5BE A7E73144 14CF78B3 F9C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                01000001 B8010E16 0A560795 4E7D79D5 A22BF908
        0B10CEB7 3C622307 F9F545BD B1A461C5 2F794321 243AACE2
        3F363FEF B35DC5BE A7E73144 14CF78B3 F9C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                DC24DF10 2FA9F96C C1CFF8C1 16C79D14 97D7C27B


    temp =
                DC24DF10 2FA9F96C C1CFF8C1 16C79D14 97D7C27B
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                 02000001 B8010E16 0A560795 4E7D79D5 A22BF908
        0B10CEB7 3C622307 F9F545BD B1A461C5 2F794321 243AACE2
        3F363FEF B35DC5BE A7E73144 14CF78B3 F9C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                 BA5BA801 E1562193 353F31E3 22395784 69B80F2F


    temp =
                           DC24DF10 2FA9F96C C1CFF8C1 16C79D14
        97D7C27B BA5BA801 E1562193 353F31E3 22395784 69B80F2F


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                 03000001 B8010E16 0A560795 4E7D79D5 A22BF908
        0B10CEB7 3C622307 F9F545BD B1A461C5 2F794321 243AACE2
        3F363FEF B35DC5BE A7E73144 14CF78B3 F9C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                 51645437 28717F17 1FDB02B2 AD5795F2 3D794EBE


    temp =
                                              DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


  V is
                                              DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


---------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                                          00DC24DF 102FA9F9
      6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
      E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                             01 000001B8 00DC24DF 102FA9F9
      6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
      E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


  Hash(counter||no_of_bits_to_return||input_string) is
               FFAF4566 5B110CA1 335A3FCE 73A7981D 0FD5C8D9


  temp =
               FFAF4566 5B110CA1 335A3FCE 73A7981D 0FD5C8D9


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                             02 000001B8 00DC24DF 102FA9F9
      6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
      E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


  Hash(counter||no_of_bits_to_return||input_string) is
               03F65FAA 46A3D597 BF34C4E0 CC167560 AB94EC10


  temp =
                       FFAF4566 5B110CA1 335A3FCE 73A7981D
      0FD5C8D9 03F65FAA 46A3D597 BF34C4E0 CC167560 AB94EC10


  ------------

  i = 3
```

```
    counter||no_of_bits_to_return||input_string is
                                03 000001B8 00DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


    Hash(counter||no_of_bits_to_return||input_string) is
                 D6415F37 83B01567 891B5766 2ABB39CD 3B7734E9


    temp =
                                               FFAF45 665B110C
        A1335A3F CE73A798 1D0FD5C8 D903F65F AA46A3D5 97BF34C4
        E0CC1675 60AB94EC 10D6415F 3783B015 67891B57 662ABB39


  C is
                                               FFAF45 665B110C
        A1335A3F CE73A798 1D0FD5C8 D903F65F AA46A3D5 97BF34C4
        E0CC1675 60AB94EC 10D6415F 3783B015 67891B57 662ABB39


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                               DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


    w_i is
                 575B37A2 739814F9 66C63B60 A2C4F149 CA9ACC84


    W is
                 575B37A2 739814F9 66C63B60 A2C4F149 CA9ACC84
```

```
    ------------

    i = 2

    data is
                                                DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5796


    w_i is
                 FC4B2549 3289B085 C67B2E30 F5F0B99A 2C349E2A


    W is
                          575B37A2 739814F9 66C63B60 A2C4F149
        CA9ACC84 FC4B2549 3289B085 C67B2E30 F5F0B99A 2C349E2A


  returned_bits is
                          575B37A2 739814F9 66C63B60 A2C4F149
        CA9ACC84 FC4B2549 3289B085 C67B2E30 F5F0B99A 2C349E2A


---------------------------

  Update V

    0x03||V is
                                               03DC24DF 102FA9F9
        6CC1CFF8 C116C79D 1497D7C2 7BBA5BA8 01E15621 93353F31
        E3223957 8469B80F 2F516454 3728717F 171FDB02 B2AD5795


    H is
                 756401AD FDF039BC B59817FD 00828E2F 56BF8C85


  Updated values

  V is
                                                DBD424 768ABB06
        0DF52A38 8F8A6F35 31A7AD8B 54BE5207 AC27F9F7 2AF473F6
        C3EE4FCD 5A794EA9 3E17DF70 24443991 7F2B8489 6F979F54


  reseed_counter is
                                                  0000 00000002
```

```
rnd_val is
                        575B37A2 739814F9 66C63B60 A2C4F149
        CA9ACC84 FC4B2549 3289B085 C67B2E30 F5F0B99A 2C349E2A


##############################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                              C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  20 21222324


    PersonalizationString = <empty>

    AdditionalInput1 =
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                              A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##############################################################
```

```
************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                        01 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                 D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


    temp =
                 D08FB441 F2F4CB37 CF6C2420 A82C7427 ACF7FCFD


    ------------

    i = 2
```

```
    counter||no_of_bits_to_return||input_string is
                        02 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                 79901438 34A5C256 AB283936 6D96348C FE8C97AB


    temp =
                           D08FB441 F2F4CB37 CF6C2420 A82C7427
        ACF7FCFD 79901438 34A5C256 AB283936 6D96348C FE8C97AB


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                        03 000001B8 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    Hash(counter||no_of_bits_to_return||input_string) is
                 6767B05E 83A98040 6D94BEE3 3CBB8905 551B5451


    temp =
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


  V is
                                              D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00D08FB4 41F2F4CB
        37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
        366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


    no_of_bits_to_return = 440
```

```
------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00D08FB4 41F2F4CB
    37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
    366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


Hash(counter||no_of_bits_to_return||input_string) is
             54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


temp =
             54C5217B 5102D8DA 8BF1686E DBAB2BBC 0C11B0CC


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00D08FB4 41F2F4CB
    37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
    366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


Hash(counter||no_of_bits_to_return||input_string) is
             B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


temp =
                      54C5217B 5102D8DA 8BF1686E DBAB2BBC
    0C11B0CC B0F0AF23 4C24CF15 ECC8CB39 C233AACA 48FCCEEE


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 00D08FB4 41F2F4CB
    37CF6C24 20A82C74 27ACF7FC FD799014 3834A5C2 56AB2839
    366D9634 8CFE8C97 AB6767B0 5E83A980 406D94BE E33CBB89


Hash(counter||no_of_bits_to_return||input_string) is
             863DA881 FFCBB434 A6CCB7DA 2FB21018 3D9DB3CF
```

```
    temp =
                                                54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


  C is
                                                54C521 7B5102D8
        DA8BF168 6EDBAB2B BC0C11B0 CCB0F0AF 234C24CF 15ECC8CB
        39C233AA CA48FCCE EE863DA8 81FFCBB4 34A6CCB7 DA2FB210


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01D0 8FB441F2 F4CB37CF 6C2420A8 2C7427AC F7FCFD79
        90143834 A5C256AB 2839366D 96348CFE 8C97AB67 67B05E83
```

```
    A980406D 94BEE33C BB898081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    01B801D0 8FB441F2 F4CB37CF 6C2420A8 2C7427AC F7FCFD79
    90143834 A5C256AB 2839366D 96348CFE 8C97AB67 67B05E83
    A980406D 94BEE33C BB898081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
             8FDEC9E6 189636F0 A5CE53E8 1C13AC93 84FAFBA0


temp =
             8FDEC9E6 189636F0 A5CE53E8 1C13AC93 84FAFBA0


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    01B801D0 8FB441F2 F4CB37CF 6C2420A8 2C7427AC F7FCFD79
    90143834 A5C256AB 2839366D 96348CFE 8C97AB67 67B05E83
    A980406D 94BEE33C BB898081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
             EE50C1E2 C8A099DE 41D8CC7A 31429E8C 8C8880E3


temp =
```

```
                        8FDEC9E6 189636F0 A5CE53E8 1C13AC93
        84FAFBA0 EE50C1E2 C8A099DE 41D8CC7A 31429E8C 8C8880E3


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                                          030000
        01B801D0 8FB441F2 F4CB37CF 6C2420A8 2C7427AC F7FCFD79
        90143834 A5C256AB 2839366D 96348CFE 8C97AB67 67B05E83
        A980406D 94BEE33C BB898081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                 B45D89DB 612CD9D2 8A55C0F0 D1F8F98B 1791FF77


    temp =
                                            8FDEC9 E6189636
        F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
        7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


  V is
                                            8FDEC9 E6189636
        F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
        7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                          008FDEC9 E6189636
        F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
        7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
```

```
                           01 000001B8 008FDEC9 E6189636
    F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
    7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


Hash(counter||no_of_bits_to_return||input_string) is
             97D07631 B22F7C95 7F19F844 F4DC2AFA 6FF97C35


temp =
             97D07631 B22F7C95 7F19F844 F4DC2AFA 6FF97C35


------------

i = 2

counter||no_of_bits_to_return||input_string is
                           02 000001B8 008FDEC9 E6189636
    F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
    7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


Hash(counter||no_of_bits_to_return||input_string) is
             66189821 6991D15B DA75BBD0 5EDF8A0F A80CCAB9


temp =
                      97D07631 B22F7C95 7F19F844 F4DC2AFA
    6FF97C35 66189821 6991D15B DA75BBD0 5EDF8A0F A80CCAB9


------------

i = 3

counter||no_of_bits_to_return||input_string is
                           03 000001B8 008FDEC9 E6189636
    F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
    7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


Hash(counter||no_of_bits_to_return||input_string) is
             5195F479 CD762022 35102EF6 27291945 8BCA75D5


temp =
                                          97D076 31B22F7C
    957F19F8 44F4DC2A FA6FF97C 35661898 216991D1 5BDA75BB
    D05EDF8A 0FA80CCA B95195F4 79CD7620 2235102E F6272919
```

```
  C is
                                                97D076 31B22F7C
        957F19F8 44F4DC2A FA6FF97C 35661898 216991D1 5BDA75BB
        D05EDF8A 0FA80CCA B95195F4 79CD7620 2235102E F6272919


****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                8FDEC9 E6189636
        F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
        7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


    w_i is
                183C242A 1430E46C 4ED70B4D BE1BF9AB 0AB8721C


    W is
                183C242A 1430E46C 4ED70B4D BE1BF9AB 0AB8721C


    ------------

    i = 2

    data is
                                                8FDEC9 E6189636
        F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
        7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8FA


    w_i is
                DCA2A2D1 820AD6F6 C9568585 43B2AA19 1D8D1287
```

```
    W is
                          183C242A 1430E46C 4ED70B4D BE1BF9AB
         0AB8721C DCA2A2D1 820AD6F6 C9568585 43B2AA19 1D8D1287


  returned_bits is
                          183C242A 1430E46C 4ED70B4D BE1BF9AB
         0AB8721C DCA2A2D1 820AD6F6 C9568585 43B2AA19 1D8D1287


---------------------------

  Update V

    0x03||V is
                                              038FDEC9 E6189636
         F0A5CE53 E81C13AC 9384FAFB A0EE50C1 E2C8A099 DE41D8CC
         7A31429E 8C8C8880 E3B45D89 DB612CD9 D28A55C0 F0D1F8F9


    H is
                 4C6A1544 99C73778 B037DE2C 2EB36123 8ADB312A


  Updated values

  V is
                                                27AF40 17CAC5B3
         8624E84C 2D10EFD7 8DF4F477 D654695A 0432326B 3A1C4E88
         4A902228 E89EAA90 36CD2AF7 05668126 2372C713 71D4533D


  reseed_counter is
                                                  0000 00000002


rnd_val is
                          183C242A 1430E46C 4ED70B4D BE1BF9AB
         0AB8721C DCA2A2D1 820AD6F6 C9568585 43B2AA19 1D8D1287


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
```

```
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0127 AF4017CA C5B38624 E84C2D10 EFD78DF4 F477D654
        695A0432 326B3A1C 4E884A90 2228E89E AA9036CD 2AF70566
        81262372 C71371D4 533DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        01B80127 AF4017CA C5B38624 E84C2D10 EFD78DF4 F477D654
        695A0432 326B3A1C 4E884A90 2228E89E AA9036CD 2AF70566
        81262372 C71371D4 533DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
Hash(counter||no_of_bits_to_return||input_string) is
             2C9C0D80 03E34023 BE5B63FD B9D224B4 250CC815


temp =
             2C9C0D80 03E34023 BE5B63FD B9D224B4 250CC815


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    01B80127 AF4017CA C5B38624 E84C2D10 EFD78DF4 F477D654
    695A0432 326B3A1C 4E884A90 2228E89E AA9036CD 2AF70566
    81262372 C71371D4 533DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Hash(counter||no_of_bits_to_return||input_string) is
             5BD1EED8 E55D9106 2FDD2764 B8AEA9C8 2F847E09


temp =
                      2C9C0D80 03E34023 BE5B63FD B9D224B4
    250CC815 5BD1EED8 E55D9106 2FDD2764 B8AEA9C8 2F847E09


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                                      030000
    01B80127 AF4017CA C5B38624 E84C2D10 EFD78DF4 F477D654
    695A0432 326B3A1C 4E884A90 2228E89E AA9036CD 2AF70566
    81262372 C71371D4 533DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Hash(counter||no_of_bits_to_return||input_string) is
             A3FEA1C7 117D6F7D D2EF777D 7CF3EBAC 38E03050
```

```
    temp =
                                                2C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


  V is
                                                2C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                             002C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 002C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


    Hash(counter||no_of_bits_to_return||input_string) is
                 7E8AA493 4272F2A2 8BBFD7AF CC88CE1C 806A38EA


    temp =
                 7E8AA493 4272F2A2 8BBFD7AF CC88CE1C 806A38EA


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 002C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                 7B8945C8 D1B6F175 0378546A B1A29600 D644EC52


    temp =
                          7E8AA493 4272F2A2 8BBFD7AF CC88CE1C
        806A38EA 7B8945C8 D1B6F175 0378546A B1A29600 D644EC52


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                03 000001B8 002C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


    Hash(counter||no_of_bits_to_return||input_string) is
                 0E8BFFF6 0CB77FA5 4BB11A83 31CB24BD 9A5B8B7F


    temp =
                                              7E8AA4 934272F2
        A28BBFD7 AFCC88CE 1C806A38 EA7B8945 C8D1B6F1 75037854
        6AB1A296 00D644EC 520E8BFF F60CB77F A54BB11A 8331CB24


  C is
                                              7E8AA4 934272F2
        A28BBFD7 AFCC88CE 1C806A38 EA7B8945 C8D1B6F1 75037854
        6AB1A296 00D644EC 520E8BFF F60CB77F A54BB11A 8331CB24


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1
```

```
    data is
                                                2C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


    w_i is
                 F196F9BD 021C745C BD5AC7BF CE48EAAF 0D0E7C09


    W is
                 F196F9BD 021C745C BD5AC7BF CE48EAAF 0D0E7C09


    ------------

    i = 2

    data is
                                                2C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EC


    w_i is
                 1FBF4369 40E63A19 8EE770D9 A4F07186 69AF2BC9


    W is
                          F196F9BD 021C745C BD5AC7BF CE48EAAF
        0D0E7C09 1FBF4369 40E63A19 8EE770D9 A4F07186 69AF2BC9


  returned_bits is
                          F196F9BD 021C745C BD5AC7BF CE48EAAF
        0D0E7C09 1FBF4369 40E63A19 8EE770D9 A4F07186 69AF2BC9


---------------------------

  Update V

    0x03||V is
                                             032C9C0D 8003E340
        23BE5B63 FDB9D224 B4250CC8 155BD1EE D8E55D91 062FDD27
        64B8AEA9 C82F847E 09A3FEA1 C7117D6F 7DD2EF77 7D7CF3EB


    H is
                 6B77061B ED13DFBC 0226822E F02EB752 A7561855
```

```
  Updated values

  V is
                                                AB26B2 13465632
        C64A1B3B AD865AF2 D0A57700 FFD75B34 A1B71482 7B33557B
        CF6A5140 347CCF86 48C66A5D BF44B71E 134D57E4 A804D765


  reseed_counter is
                                                  0000 00000002


rnd_val is
                          F196F9BD 021C745C BD5AC7BF CE48EAAF
        0D0E7C09 1FBF4369 40E63A19 8EE770D9 A4F07186 69AF2BC9


################################################################

Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  20 21222324


    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
```

```
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

############################################################

************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                20 21222324


    personal_str is
                                              404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                  000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
        01000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
```

```
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
             99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


temp =
             99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


------------

i = 2

counter||no_of_bits_to_return||input_string is
    02000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
    13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
    2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
             EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


temp =
                      99B9537B 8427B8CE 23219A61 1CBE6106
    44CF8503 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


------------

i = 3

counter||no_of_bits_to_return||input_string is
    03000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
    13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
    2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
             E02E85A2 314CE3D7 4A93324B 27BDE85F 5498B7AC


temp =
                                          99B953 7B8427B8
    CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
    8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8
```

```
  V is
                                                99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    Hash(counter||no_of_bits_to_return||input_string) is
                 A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


    temp =
                 A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    Hash(counter||no_of_bits_to_return||input_string) is
                 D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A
```

```
    temp =
                         A70266F7 F91EC4D2 88731479 34CEAF2A
        2CC35A0F D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                03 000001B8 0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    Hash(counter||no_of_bits_to_return||input_string) is
                 F485DA6C BF0416DC DC5FB8BC 9C94B6BC 511E0813


    temp =
                                               A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


  C is
                                               A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


-------------------------------------------------------------

First call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                               808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            0199B9 537B8427 B8CE2321 9A611CBE
        610644CF 8503EEC5 BA22DE1A B212C3D0 858E9E3B 9026D4E7
        7D58E02E 85A2314C E3D74A93 324B27BD E8808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                01000001 B80199B9 537B8427 B8CE2321 9A611CBE
        610644CF 8503EEC5 BA22DE1A B212C3D0 858E9E3B 9026D4E7
        7D58E02E 85A2314C E3D74A93 324B27BD E8808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                E5043D1B 954B34BA 60D248E8 83EF498C 5C5236B8


    temp =
                E5043D1B 954B34BA 60D248E8 83EF498C 5C5236B8


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                02000001 B80199B9 537B8427 B8CE2321 9A611CBE
        610644CF 8503EEC5 BA22DE1A B212C3D0 858E9E3B 9026D4E7
        7D58E02E 85A2314C E3D74A93 324B27BD E8808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                260E238E 02C8D4FC 5FFE90FA 40134470 75BB543E
```

```
    temp =
                          E5043D1B 954B34BA 60D248E8 83EF498C
        5C5236B8 260E238E 02C8D4FC 5FFE90FA 40134470 75BB543E


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                03000001 B80199B9 537B8427 B8CE2321 9A611CBE
        610644CF 8503EEC5 BA22DE1A B212C3D0 858E9E3B 9026D4E7
        7D58E02E 85A2314C E3D74A93 324B27BD E8808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    Hash(counter||no_of_bits_to_return||input_string) is
                F00C3BDA 596B1088 61F06BF9 1B45D683 A8FCA873


    temp =
                                               E5043D 1B954B34
        BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
        FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


  V is
                                               E5043D 1B954B34
        BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
        FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                             00E5043D 1B954B34
        BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
        FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
```

```
                           01 000001B8 00E5043D 1B954B34
    BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
    FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


Hash(counter||no_of_bits_to_return||input_string) is
             1F3F6310 ED10FC9F 938C4322 61AF42E9 E9175F08


temp =
             1F3F6310 ED10FC9F 938C4322 61AF42E9 E9175F08


------------

i = 2

counter||no_of_bits_to_return||input_string is
                           02 000001B8 00E5043D 1B954B34
    BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
    FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


Hash(counter||no_of_bits_to_return||input_string) is
             0F3222DC 118BA7CF 888CDC3F 360DD28F 5ECB7C80


temp =
                      1F3F6310 ED10FC9F 938C4322 61AF42E9
    E9175F08 0F3222DC 118BA7CF 888CDC3F 360DD28F 5ECB7C80


------------

i = 3

counter||no_of_bits_to_return||input_string is
                           03 000001B8 00E5043D 1B954B34
    BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
    FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


Hash(counter||no_of_bits_to_return||input_string) is
             A6BCFCFC 0F51FE2F 77C1C99D F0A2099F 44A616E7


temp =
                                          1F3F63 10ED10FC
    9F938C43 2261AF42 E9E9175F 080F3222 DC118BA7 CF888CDC
    3F360DD2 8F5ECB7C 80A6BCFC FC0F51FE 2F77C1C9 9DF0A209
```

```
  C is
                                                1F3F63 10ED10FC
        9F938C43 2261AF42 E9E9175F 080F3222 DC118BA7 CF888CDC
        3F360DD2 8F5ECB7C 80A6BCFC FC0F51FE 2F77C1C9 9DF0A209


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                E5043D 1B954B34
        BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
        FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


    w_i is
                 532CA116 5DCFF21C 55592687 639884AF 4BC4B057


    W is
                 532CA116 5DCFF21C 55592687 639884AF 4BC4B057


    ------------

    i = 2

    data is
                                                E5043D 1B954B34
        BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
        FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D7


    w_i is
                 DF8F41DE 653AB44E 2ADEC7C9 303E75AB E277EDBF
```

```
    W is
                          532CA116 5DCFF21C 55592687 639884AF
         4BC4B057 DF8F41DE 653AB44E 2ADEC7C9 303E75AB E277EDBF


  returned_bits is
                          532CA116 5DCFF21C 55592687 639884AF
         4BC4B057 DF8F41DE 653AB44E 2ADEC7C9 303E75AB E277EDBF


---------------------------

  Update V

    0x03||V is
                                             03E5043D 1B954B34
         BA60D248 E883EF49 8C5C5236 B8260E23 8E02C8D4 FC5FFE90
         FA401344 7075BB54 3EF00C3B DA596B10 8861F06B F91B45D6


    H is
                 32AFEC24 6BED8E21 D97FCE1E 66769CEC 55424955


  Updated values

  V is
                                               0443A0 2C825C31
         59F45E8C 0AE59E8C 76456995 C0354046 6A14547C CBE88B6D
         39762117 328472F5 2B84575A AFE88B2D 1E504F21 EC4E3135


  reseed_counter is
                                                 0000 00000002


rnd_val is
                          532CA116 5DCFF21C 55592687 639884AF
         4BC4B057 DF8F41DE 653AB44E 2ADEC7C9 303E75AB E277EDBF


-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>
```

```
Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            010443 A02C825C 3159F45E 8C0AE59E
        8C764569 95C03540 466A1454 7CCBE88B 6D397621 17328472
        F52B8457 5AAFE88B 2D1E504F 21EC4E31 35C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                01000001 B8010443 A02C825C 3159F45E 8C0AE59E
        8C764569 95C03540 466A1454 7CCBE88B 6D397621 17328472
        F52B8457 5AAFE88B 2D1E504F 21EC4E31 35C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                9DC35208 EE2B8C58 1EA30BAA CB5D7431 7A879454


    temp =
                9DC35208 EE2B8C58 1EA30BAA CB5D7431 7A879454


    ------------

    i = 2
```

```
    counter||no_of_bits_to_return||input_string is
                02000001 B8010443 A02C825C 3159F45E 8C0AE59E
        8C764569 95C03540 466A1454 7CCBE88B 6D397621 17328472
        F52B8457 5AAFE88B 2D1E504F 21EC4E31 35C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                10717E58 D3705FBD C760BE0C C90ED1CC BB897D47


    temp =
                          9DC35208 EE2B8C58 1EA30BAA CB5D7431
        7A879454 10717E58 D3705FBD C760BE0C C90ED1CC BB897D47


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                03000001 B8010443 A02C825C 3159F45E 8C0AE59E
        8C764569 95C03540 466A1454 7CCBE88B 6D397621 17328472
        F52B8457 5AAFE88B 2D1E504F 21EC4E31 35C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                D27E2B2E 422B32B9 7F050D1B D2B49080 823932BF


    temp =
                                              9DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
        0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


  V is
                                              9DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
        0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            009DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
```

```
    0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 009DC352 08EE2B8C
    581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
    0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


Hash(counter||no_of_bits_to_return||input_string) is
             1A5AD6CE A3D15DA5 FB474213 1309F0ED 88CF4C90


temp =
             1A5AD6CE A3D15DA5 FB474213 1309F0ED 88CF4C90


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 009DC352 08EE2B8C
    581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
    0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


Hash(counter||no_of_bits_to_return||input_string) is
             A6C1CCEE 35A876EB FCCC8267 29B6639F 811965B0


temp =
                      1A5AD6CE A3D15DA5 FB474213 1309F0ED
    88CF4C90 A6C1CCEE 35A876EB FCCC8267 29B6639F 811965B0


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 009DC352 08EE2B8C
    581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
    0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                EF8576E7 5CB3CFE8 220768B2 6CE77ACE CD58370F


    temp =
                                              1A5AD6 CEA3D15D
        A5FB4742 131309F0 ED88CF4C 90A6C1CC EE35A876 EBFCCC82
        6729B663 9F811965 B0EF8576 E75CB3CF E8220768 B26CE77A


  C is
                                              1A5AD6 CEA3D15D
        A5FB4742 131309F0 ED88CF4C 90A6C1CC EE35A876 EBFCCC82
        6729B663 9F811965 B0EF8576 E75CB3CF E8220768 B26CE77A


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                              9DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
        0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


    w_i is
                73C2C67C 696D686D 0C4DBCEB 5C2AF7DD F6F020B6


    W is
                73C2C67C 696D686D 0C4DBCEB 5C2AF7DD F6F020B6


    ------------

    i = 2
```

```
    data is
                                                9DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
        0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B491


    w_i is
                874FAE43 90F10211 7ECAAFF5 4418529A 367005A0


    W is
                         73C2C67C 696D686D 0C4DBCEB 5C2AF7DD
        F6F020B6 874FAE43 90F10211 7ECAAFF5 4418529A 367005A0


  returned_bits is
                         73C2C67C 696D686D 0C4DBCEB 5C2AF7DD
        F6F020B6 874FAE43 90F10211 7ECAAFF5 4418529A 367005A0


---------------------------

  Update V

    0x03||V is
                                              039DC352 08EE2B8C
        581EA30B AACB5D74 317A8794 5410717E 58D3705F BDC760BE
        0CC90ED1 CCBB897D 47D27E2B 2E422B32 B97F050D 1BD2B490


    H is
                03287CD5 69C9D511 E2E69645 0A15C4BA DAA6BB53


  Updated values

  V is
                                                B81E28 D791FCE9
        FE19EA4D BDDE6765 1F0356E0 E4B7334B 470918D6 A9C42D40
        73F2C535 6F651FB8 628BD8B3 F8857547 ABB6D130 A8E6575E


  reseed_counter is
                                                  0000 00000002


rnd_val is
                         73C2C67C 696D686D 0C4DBCEB 5C2AF7DD
        F6F020B6 874FAE43 90F10211 7ECAAFF5 4418529A 367005A0


################################################################
```

```
Hash_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                     20 21222324


    PersonalizationString =
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                 606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************
```

```
Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                   000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
        01000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503


    temp =
                 99B9537B 8427B8CE 23219A61 1CBE6106 44CF8503
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
        02000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    temp =
                          99B9537B 8427B8CE 23219A61 1CBE6106
        44CF8503 EEC5BA22 DE1AB212 C3D0858E 9E3B9026 D4E77D58


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
        03000001 B8000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                 E02E85A2 314CE3D7 4A93324B 27BDE85F 5498B7AC


    temp =
                                              99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  V is
                                              99B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


---------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                                          0099B953 7B8427B8
      CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
      8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                             01 000001B8 0099B953 7B8427B8
      CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
      8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  Hash(counter||no_of_bits_to_return||input_string) is
               A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


  temp =
               A70266F7 F91EC4D2 88731479 34CEAF2A 2CC35A0F


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                             02 000001B8 0099B953 7B8427B8
      CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
      8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


  Hash(counter||no_of_bits_to_return||input_string) is
               D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


  temp =
                        A70266F7 F91EC4D2 88731479 34CEAF2A
      2CC35A0F D5E00ABA E79DC660 5FABD6F5 F928E18C 63268E1A


  ------------

  i = 3
```

```
    counter||no_of_bits_to_return||input_string is
                                03 000001B8 0099B953 7B8427B8
        CE23219A 611CBE61 0644CF85 03EEC5BA 22DE1AB2 12C3D085
        8E9E3B90 26D4E77D 58E02E85 A2314CE3 D74A9332 4B27BDE8


    Hash(counter||no_of_bits_to_return||input_string) is
                 F485DA6C BF0416DC DC5FB8BC 9C94B6BC 511E0813


    temp =
                                               A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


  C is
                                               A70266 F7F91EC4
        D2887314 7934CEAF 2A2CC35A 0FD5E00A BAE79DC6 605FABD6
        F5F928E1 8C63268E 1AF485DA 6CBF0416 DCDC5FB8 BC9C94B6


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                               606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                               808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                               606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0199 B9537B84 27B8CE23 219A611C BE610644 CF8503EE
        C5BA22DE 1AB212C3 D0858E9E 3B9026D4 E77D58E0 2E85A231
        4CE3D74A 93324B27 BDE88081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        01B80199 B9537B84 27B8CE23 219A611C BE610644 CF8503EE
        C5BA22DE 1AB212C3 D0858E9E 3B9026D4 E77D58E0 2E85A231
        4CE3D74A 93324B27 BDE88081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                563A5D20 7D37707B F5F24D0B D4935DC3 8DBE0436


    temp =
                563A5D20 7D37707B F5F24D0B D4935DC3 8DBE0436


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                        020000
        01B80199 B9537B84 27B8CE23 219A611C BE610644 CF8503EE
        C5BA22DE 1AB212C3 D0858E9E 3B9026D4 E77D58E0 2E85A231
        4CE3D74A 93324B27 BDE88081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
```

```
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                 37B3FF8A B68CFCE2 F290D169 95205524 190FD291


    temp =
                         563A5D20 7D37707B F5F24D0B D4935DC3
        8DBE0436 37B3FF8A B68CFCE2 F290D169 95205524 190FD291


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                                        030000
        01B80199 B9537B84 27B8CE23 219A611C BE610644 CF8503EE
        C5BA22DE 1AB212C3 D0858E9E 3B9026D4 E77D58E0 2E85A231
        4CE3D74A 93324B27 BDE88081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                 AA8A6E6B 8E6D56A4 31333B40 8E6FA812 0AE2B77C


    temp =
                                              563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
        69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


  V is
                                              563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
        69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
```

```
    69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00563A5D 207D3770
    7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
    69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


Hash(counter||no_of_bits_to_return||input_string) is
             C5D3E955 1E00E4EE 32B2116F AF4DEFF4 D4CFAD2B


temp =
             C5D3E955 1E00E4EE 32B2116F AF4DEFF4 D4CFAD2B


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00563A5D 207D3770
    7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
    69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


Hash(counter||no_of_bits_to_return||input_string) is
             DC2DBAA2 E0E7F9DD B9D81EED 45E0A50D A5AFD5C1


temp =
                      C5D3E955 1E00E4EE 32B2116F AF4DEFF4
    D4CFAD2B DC2DBAA2 E0E7F9DD B9D81EED 45E0A50D A5AFD5C1


------------

i = 3

counter||no_of_bits_to_return||input_string is
                            03 000001B8 00563A5D 207D3770
    7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
    69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                F6BCDAF8 1D289CF4 BD3C91B7 005C1833 EBD4CAAB


    temp =
                                              C5D3E9 551E00E4
        EE32B211 6FAF4DEF F4D4CFAD 2BDC2DBA A2E0E7F9 DDB9D81E
        ED45E0A5 0DA5AFD5 C1F6BCDA F81D289C F4BD3C91 B7005C18


  C is
                                              C5D3E9 551E00E4
        EE32B211 6FAF4DEF F4D4CFAD 2BDC2DBA A2E0E7F9 DDB9D81E
        ED45E0A5 0DA5AFD5 C1F6BCDA F81D289C F4BD3C91 B7005C18


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                              563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
        69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


    w_i is
                F2F76CE3D 13BE866F EB390DB5 7591CD12 09E4FE0F


    W is
                F2F76CE3D 13BE866F EB390DB5 7591CD12 09E4FE0F


    ------------

    i = 2
```

```
    data is
                                                563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
        69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA9


    w_i is
                90794C97 218A6482 5D8E4097 CB15D30E D958BC18


    W is
                         2F76CE3D 13BE866F EB390DB5 7591CD12
        09E4FE0F 90794C97 218A6482 5D8E4097 CB15D30E D958BC18


  returned_bits is
                         2F76CE3D 13BE866F EB390DB5 7591CD12
        09E4FE0F 90794C97 218A6482 5D8E4097 CB15D30E D958BC18


---------------------------

  Update V

    0x03||V is
                                               03563A5D 207D3770
        7BF5F24D 0BD4935D C38DBE04 3637B3FF 8AB68CFC E2F290D1
        69952055 24190FD2 91AA8A6E 6B8E6D56 A431333B 408E6FA8


    H is
                E1229C4C 8AF4096D CF7297C9 CD5DCAEA 7F595990


  Updated values

  V is
                                                 1C0E46 759B3855
        6A28A45E 7B83E14D B8628DB1 6213E1BA 2D9774F6 C0AC68F0
        56DB00FB 12E15BF4 DE9550B7 331E2DBD 664C3AB7 76E82551


  reseed_counter is
                                                   0000 00000002


rnd_val is
                         2F76CE3D 13BE866F EB390DB5 7591CD12
        09E4FE0F 90794C97 218A6482 5D8E4097 CB15D30E D958BC18


---------------------------------------------------------------
```

```
Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input
                                              A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                              C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                              A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            011C 0E46759B 38556A28 A45E7B83 E14DB862 8DB16213
        E1BA2D97 74F6C0AC 68F056DB 00FB12E1 5BF4DE95 50B7331E
        2DBD664C 3AB776E8 2551C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
                                                        010000
    01B8011C 0E46759B 38556A28 A45E7B83 E14DB862 8DB16213
    E1BA2D97 74F6C0AC 68F056DB 00FB12E1 5BF4DE95 50B7331E
    2DBD664C 3AB776E8 2551C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Hash(counter||no_of_bits_to_return||input_string) is
             600193C8 F6031A2D 49372A8B 0F60F68C 1DFDACD4


temp =
             600193C8 F6031A2D 49372A8B 0F60F68C 1DFDACD4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    01B8011C 0E46759B 38556A28 A45E7B83 E14DB862 8DB16213
    E1BA2D97 74F6C0AC 68F056DB 00FB12E1 5BF4DE95 50B7331E
    2DBD664C 3AB776E8 2551C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Hash(counter||no_of_bits_to_return||input_string) is
             F8EA0137 47D71482 333DF525 2E95B822 57391BF1


temp =
                      600193C8 F6031A2D 49372A8B 0F60F68C
    1DFDACD4 F8EA0137 47D71482 333DF525 2E95B822 57391BF1


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                                        030000
    01B8011C 0E46759B 38556A28 A45E7B83 E14DB862 8DB16213
    E1BA2D97 74F6C0AC 68F056DB 00FB12E1 5BF4DE95 50B7331E
    2DBD664C 3AB776E8 2551C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
```

```
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                 0AB07D12 08B6BD66 5B300AA4 DB9C3EF0 70322C9B


    temp =
                                              600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


  V is
                                              600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    Hash(counter||no_of_bits_to_return||input_string) is
                 6B71823B 18200771 CAAE5D12 55C1403E DFE38B4D


    temp =
                 6B71823B 18200771 CAAE5D12 55C1403E DFE38B4D
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    Hash(counter||no_of_bits_to_return||input_string) is
                18C787BB 44CD1718 6152EFEA D6FDC4B8 94F92002


    temp =
                          6B71823B 18200771 CAAE5D12 55C1403E
        DFE38B4D 18C787BB 44CD1718 6152EFEA D6FDC4B8 94F92002


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                03 000001B8 00600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    Hash(counter||no_of_bits_to_return||input_string) is
                C0720955 5D7E3554 F9D12FC5 597F22F4 44AAC5B9


    temp =
                                              6B7182 3B182007
        71CAAE5D 1255C140 3EDFE38B 4D18C787 BB44CD17 186152EF
        EAD6FDC4 B894F920 02C07209 555D7E35 54F9D12F C5597F22


  C is
                                              6B7182 3B182007
        71CAAE5D 1255C140 3EDFE38B 4D18C787 BB44CD17 186152EF
        EAD6FDC4 B894F920 02C07209 555D7E35 54F9D12F C5597F22


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 320

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 320

    ------------

    i = 1

    data is
                                                600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    w_i is
                79CE5A7D 09EBB2FF 600EDB53 1C8A212F F3EA267C


    W is
                79CE5A7D 09EBB2FF 600EDB53 1C8A212F F3EA267C


    ------------

    i = 2

    data is
                                                600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3F


    w_i is
                1C5487E5 83592A0A BFEAFC4E 13045EA9 3666DB85


    W is
                         79CE5A7D 09EBB2FF 600EDB53 1C8A212F
        F3EA267C 1C5487E5 83592A0A BFEAFC4E 13045EA9 3666DB85


  returned_bits is
                         79CE5A7D 09EBB2FF 600EDB53 1C8A212F
        F3EA267C 1C5487E5 83592A0A BFEAFC4E 13045EA9 3666DB85


---------------------------

  Update V
```

```
    0x03||V is
                                                03600193 C8F6031A
        2D49372A 8B0F60F6 8C1DFDAC D4F8EA01 3747D714 82333DF5
        252E95B8 2257391B F10AB07D 1208B6BD 665B300A A4DB9C3E


    H is
                 EB7068BD AD62FFEA 6E358C7A 1FC2427D DC635B99


  Updated values

  V is
                                                  CB7316 040E2321
        9F13E587 9D652236 CAFDE138 2211B188 F28CA42B 9A9490E5
        1005937D C65C9AF9 A12E2270 D59BC16C DB1743B8 469876FA


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          79CE5A7D 09EBB2FF 600EDB53 1C8A212F
        F3EA267C 1C5487E5 83592A0A BFEAFC4E 13045EA9 3666DB85
```

```
################################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                   010000 01B80001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


    temp =
                                                        0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
```

020000 01B80001 02030405 06070809 0A0B0C0D
0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526

Hash(counter||no_of_bits_to_return||input_string) is
33D18070
2841C3D3 7CA40F35 645ECB1A A6548550 7F577CA9 8F418A0E

temp =
0BB6E5 3D916573
A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A

V is
0BB6E5 3D916573
A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A

Hash_df - Generate C - Step 4

0x00||V is
000BB6E5 3D916573
A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A

no_of_bits_to_return = 440

---

i = 1

counter||no_of_bits_to_return||input_string is
01 000001B8 000BB6E5 3D916573
A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A

Hash(counter||no_of_bits_to_return||input_string) is
E5B7AE6C

```
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    temp =
                                                        E5B7AE6C
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        11F35DAE
        12883480 7F41DD3A A952DE09 0AB3C78C C4D38F67 F13F7896


    temp =
                                                  E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


  C is
                                                  E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                                0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    w_i is
                                                        5E68BDE0
        9AAA08BC 11B32790 2C82F011 4CBA0F9C CCA6203B A3940091


    W is
                                                        5E68BDE0
        9AAA08BC 11B32790 2C82F011 4CBA0F9C CCA6203B A3940091


    ------------

    i = 2

    data is
                                                0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418B


    w_i is
                                                        3ECD3671
        A5B60EF9 22999D90 FCEEEC5C 227E5D25 C56921EE 572ED472


    W is
                                               5E68BDE0 9AAA08BC
        11B32790 2C82F011 4CBA0F9C CCA6203B A3940091 3ECD3671
        A5B60EF9 22999D90 FCEEEC5C 227E5D25 C56921EE 572ED472
```

```
  returned_bits is
                                                5E68BDE0 9AAA08BC
        11B32790 2C82F011 4CBA0F9C CCA6203B A3940091 3ECD3671
        A5B60EF9 22999D90 FCEEEC5C 227E5D25 C56921EE 572ED472


---------------------------

  Update V

    0x03||V is
                                                030BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    H is
                                                        F4F9E387
        8DAC8089 5CE1C1DD E67CBEAD 36B59C8F 3767955D 3623164F


  Updated values

  V is
                                                  F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 3F3FA865
        ABE74A81 B0DDA7CA 568A7056 5A66A4DC 14ABC069 47A39752


  reseed_counter is
                                                    0000 00000002


rnd_val is
                                                5E68BDE0 9AAA08BC
        11B32790 2C82F011 4CBA0F9C CCA6203B A3940091 3ECD3671
        A5B60EF9 22999D90 FCEEEC5C 227E5D25 C56921EE 572ED472


-------------------------------------------------------------

Second call to Generate

*************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                                F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 3F3FA865
        ABE74A81 B0DDA7CA 568A7056 5A66A4DC 14ABC069 47A39752


    w_i is
                                                        DC056FCB
        35FF51D7 D9FB72FD 4FD1B1D2 46451DB5 6CD4F889 E432E327


    W is
                                                        DC056FCB
        35FF51D7 D9FB72FD 4FD1B1D2 46451DB5 6CD4F889 E432E327


    ------------

    i = 2

    data is
                                                F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 3F3FA865
        ABE74A81 B0DDA7CA 568A7056 5A66A4DC 14ABC069 47A39753


    w_i is
                                                        3F9ED82D
        E3EF7CD2 8B6A9C0F 4D78E5C8 451D3634 0A2BD7E6 9FAB32EB
```

```
    W is
                                                DC056FCB 35FF51D7
        D9FB72FD 4FD1B1D2 46451DB5 6CD4F889 E432E327 3F9ED82D
        E3EF7CD2 8B6A9C0F 4D78E5C8 451D3634 0A2BD7E6 9FAB32EB


  returned_bits is
                                                DC056FCB 35FF51D7
        D9FB72FD 4FD1B1D2 46451DB5 6CD4F889 E432E327 3F9ED82D
        E3EF7CD2 8B6A9C0F 4D78E5C8 451D3634 0A2BD7E6 9FAB32EB


---------------------------

  Update V

    0x03||V is
                                                03F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 3F3FA865
        ABE74A81 B0DDA7CA 568A7056 5A66A4DC 14ABC069 47A39752


    H is
                                                        06BFA186
        BFC4A213 5AA645D7 D2E29A3B E15BA781 7EEC5A90 E0536E52


  Updated values

  V is
                                                  D72642 169D7456
        5D9A1305 6D179B58 06F58DDA 47761ABD C47343B2 06113D4A
        19BE74C9 8C032F7F 64165D70 44CD0025 205CEE89 8FE8451E


  reseed_counter is
                                                    0000 00000003


rnd_val is
                                                DC056FCB 35FF51D7
        D9FB72FD 4FD1B1D2 46451DB5 6CD4F889 E432E327 3F9ED82D
        E3EF7CD2 8B6A9C0F 4D78E5C8 451D3634 0A2BD7E6 9FAB32EB
```

```
################################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                    010000 01B80001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A
```

```
    temp =
                                                          0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                  020000 01B80001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    Hash(counter||no_of_bits_to_return||input_string) is
                                                          33D18070
        2841C3D3 7CA40F35 645ECB1A A6548550 7F577CA9 8F418A0E


    temp =
                                                 0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


  V is
                                                 0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    no_of_bits_to_return = 440

    ------------
```

```
  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 000BB6E5 3D916573
      A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
      702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    E5B7AE6C
      8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


  temp =
                                                    E5B7AE6C
      8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 000BB6E5 3D916573
      A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
      702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    11F35DAE
      12883480 7F41DD3A A952DE09 0AB3C78C C4D38F67 F13F7896


  temp =
                                                E5B7AE 6C860771
      5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
      AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


C is
                                                E5B7AE 6C860771
      5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
      AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78
```

```
---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           020BB6 E53D9165 73A7AC79 6702CA6D
        D2E30D13 B8A3ACFD 7E23905D 6F8A33D1 80702841 C3D37CA4
        0F35645E CB1AA654 85507F57 7CA98F41 8A606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    w=Hash(0x02||V||additional_input) is
                                                        4287889E
        AD10CE0F D67794A8 CCE65303 02F18AEC 557970F0 CA5195D5


    V is
                                                0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F CCBB5A1F
        1D390FD3 A9F438B8 024AB1CE 1D97DF71 A5F8C86D 73E0D75F


---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------
```

```
  i = 1

  data is
                                                0BB6E5 3D916573
      A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F CCBB5A1F
      1D390FD3 A9F438B8 024AB1CE 1D97DF71 A5F8C86D 73E0D75F


  w_i is
                                                      B15DEC1B
      266433D9 7E587C87 1D15717A E15CA7B7 E616CFE1 0120523A


  W is
                                                      B15DEC1B
      266433D9 7E587C87 1D15717A E15CA7B7 E616CFE1 0120523A


  ------------

  i = 2

  data is
                                                0BB6E5 3D916573
      A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F CCBB5A1F
      1D390FD3 A9F438B8 024AB1CE 1D97DF71 A5F8C86D 73E0D760


  w_i is
                                                      E9504D80
      4E102D1C AFAFD3FF 677BEBBD 0C435952 505F8723 1D9EA679


  W is
                                              B15DEC1B 266433D9
      7E587C87 1D15717A E15CA7B7 E616CFE1 0120523A E9504D80
      4E102D1C AFAFD3FF 677BEBBD 0C435952 505F8723 1D9EA679


returned_bits is
                                              B15DEC1B 266433D9
      7E587C87 1D15717A E15CA7B7 E616CFE1 0120523A E9504D80
      4E102D1C AFAFD3FF 677BEBBD 0C435952 505F8723 1D9EA679
```

```
--------------------------

  Update V

    0x03||V is
                                              030BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F CCBB5A1F
        1D390FD3 A9F438B8 024AB1CE 1D97DF71 A5F8C86D 73E0D75F


    H is
                                                      9C1A49BE
        0F0F864F B744F3E4 59836BE7 F8D4F8EE 59534561 7F265D00


  Updated values

  V is
                                                F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 28E7973A
        DA5B1E57 E1B86E79 96777094 1F778C27 8C10E15E 5AF873D8


  reseed_counter is
                                                   0000 00000002


rnd_val is
                                              B15DEC1B 266433D9
        7E587C87 1D15717A E15CA7B7 E616CFE1 0120523A E9504D80
        4E102D1C AFAFD3FF 677BEBBD 0C435952 505F8723 1D9EA679


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
```

```
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           02F16E 93AA176C E502A346 3637F104
        95750150 C975918C 1DF401D0 9128E797 3ADA5B1E 57E1B86E
        79967770 941F778C 278C10E1 5E5AF873 D8A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                                                    6B2A78EE
        40118B02 0EBD27A2 812B5A04 4490BA01 A292FEC7 6FB262E6


    V is
                                              F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 94121029
        1A6CA959 F075961C 17A2CA98 64084629 2EA3E025 CAAAD6BE


---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                              F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 94121029
        1A6CA959 F075961C 17A2CA98 64084629 2EA3E025 CAAAD6BE


    w_i is
                                                    8E428812
        257FB69B 1A8C6712 88F702B0 A82574AF D2BA8868 F4124A7D
```

```
    W is
                                                        8E428812
        257FB69B 1A8C6712 88F702B0 A82574AF D2BA8868 F4124A7D


    ------------

    i = 2

    data is
                                              F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 94121029
        1A6CA959 F075961C 17A2CA98 64084629 2EA3E025 CAAAD6BF


    w_i is
                                                        5A8EA256
        43141DA9 4042D1C7 170CB6B5 412F9178 84C5CA8D 6CD275F3


    W is
                                              8E428812 257FB69B
        1A8C6712 88F702B0 A82574AF D2BA8868 F4124A7D 5A8EA256
        43141DA9 4042D1C7 170CB6B5 412F9178 84C5CA8D 6CD275F3


  returned_bits is
                                              8E428812 257FB69B
        1A8C6712 88F702B0 A82574AF D2BA8868 F4124A7D 5A8EA256
        43141DA9 4042D1C7 170CB6B5 412F9178 84C5CA8D 6CD275F3


--------------------------

  Update V

    0x03||V is
                                              03F16E93 AA176CE5
        02A34636 37F10495 750150C9 75918C1D F401D091 94121029
        1A6CA959 F075961C 17A2CA98 64084629 2EA3E025 CAAAD6BE


    H is
                                                        41408548
        633CC968 D38560B6 AE43BB48 B6C6D1D9 A0E13F94 42BF565D
```

```
  Updated values

  V is
                                                 D72642 169D7456
        5D9A1305 6D179B58 06F58DDA 47761ABD C47343B2 956488CF
        2BBBFAF7 447A38B0 008FD8BF 23D9CBCA 5C49F349 755B6C95


  reseed_counter is
                                                   0000 00000003


rnd_val is
                                               8E428812 257FB69B
        1A8C6712 88F702B0 A82574AF D2BA8868 F4124A7D 5A8EA256
        43141DA9 4042D1C7 170CB6B5 412F9178 84C5CA8D 6CD275F3


################################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
    Nonce =
                                                202122 23242526


    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                202122 23242526


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
```

```
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                        0100
    0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
    15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
    2D2E2F30 31323334 35362021 22232425 26404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
                                                    E2524D0E
    2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


temp =
                                                    E2524D0E
    2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                        0200
    0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
    15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
    2D2E2F30 31323334 35362021 22232425 26404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
                                                    5FEA7A53
    F4A6C635 DC5FED69 1F36A168 A07266E7 75A7FB60 7BE9D680
```

```
    temp =
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  V is
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                    FADECBC8
        A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


    temp =
                                                    FADECBC8
        A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


    ------------
```

```
    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        90A2F07A
        9E31D50D 5B7DE500 5AD7C1E8 9A3E1AFE D62C331D 6A561403


    temp =
                                              FADECB C8A4B733
        F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
        7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614


  C is
                                              FADECB C8A4B733
        F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
        7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1
```

```
    data is
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


    w_i is
                                                        A13548D9
        029814B7 F142E991 5742B984 4EC5C386 E648CDA9 4BCDCE22


    W is
                                                        A13548D9
        029814B7 F142E991 5742B984 4EC5C386 E648CDA9 4BCDCE22


    ------------

    i = 2

    data is
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D7


    w_i is
                                                        60E79C86
        C06B5597 81E8DFEB BB978C76 0D04DAB9 56E79E7E D0065638


    W is
                                            A13548D9 029814B7
        F142E991 5742B984 4EC5C386 E648CDA9 4BCDCE22 60E79C86
        C06B5597 81E8DFEB BB978C76 0D04DAB9 56E79E7E D0065638


  returned_bits is
                                            A13548D9 029814B7
        F142E991 5742B984 4EC5C386 E648CDA9 4BCDCE22 60E79C86
        C06B5597 81E8DFEB BB978C76 0D04DAB9 56E79E7E D0065638


---------------------------
```

```
  Update V

    0x03||V is
                                                03E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


    H is
                                                            DAFAC71D
        EAFCE300 C98C6196 BB1AF5C8 F7FA2169 81211536 599E3665


  Updated values

  V is
                                                  DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB8 17EB5488
        B98FBB9C 0CC43F69 2495042C 4934D1EB 676CE964 D7847650


  reseed_counter is
                                                     0000 00000002


rnd_val is
                                                A13548D9 029814B7
        F142E991 5742B984 4EC5C386 E648CDA9 4BCDCE22 60E79C86
        C06B5597 81E8DFEB BB978C76 0D04DAB9 56E79E7E D0065638


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen
```

```
  requested_no_of_bits  = 448

  ------------

  i = 1

  data is
                                                DD3118 D6D22089
      FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB8 17EB5488
      B98FBB9C 0CC43F69 2495042C 4934D1EB 676CE964 D7847650


  w_i is
                                                        A2B1DC82
      42469DEC 61E738D1 2B3685FA D4D640B4 1C0D4343 03E6A185


  W is
                                                        A2B1DC82
      42469DEC 61E738D1 2B3685FA D4D640B4 1C0D4343 03E6A185


  ------------

  i = 2

  data is
                                                DD3118 D6D22089
      FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB8 17EB5488
      B98FBB9C 0CC43F69 2495042C 4934D1EB 676CE964 D7847651


  w_i is
                                                        17CFF39A
      3C1FBF1B CBEF2B69 EB2C9A9D A76F5F49 D1BF3825 130A30D3


  W is
                                              A2B1DC82 42469DEC
      61E738D1 2B3685FA D4D640B4 1C0D4343 03E6A185 17CFF39A
      3C1FBF1B CBEF2B69 EB2C9A9D A76F5F49 D1BF3825 130A30D3


returned_bits is
                                              A2B1DC82 42469DEC
```

```
        61E738D1 2B3685FA D4D640B4 1C0D4343 03E6A185 17CFF39A
        3C1FBF1B CBEF2B69 EB2C9A9D A76F5F49 D1BF3825 130A30D3


---------------------------

  Update V

    0x03||V is
                                              03DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB8 17EB5488
        B98FBB9C 0CC43F69 2495042C 4934D1EB 676CE964 D7847650


    H is
                                                    6FD91259
        78571F75 B50237AB EC52277E 95C7D59F A5CCB232 F080A043


  Updated values

  V is
                                                D80FE4 9F76D7BD
        F9860BC0 A72DBCAB 7905CEB9 99963951 E5E0A90C EB5509D2
        AC850CE6 CF21F4FA 1142036C C796E5A6 0C0FC7CA E56F6CA9


  reseed_counter is
                                                  0000 00000003


rnd_val is
                                              A2B1DC82 42469DEC
        61E738D1 2B3685FA D4D640B4 1C0D4343 03E6A185 17CFF39A
        3C1FBF1B CBEF2B69 EB2C9A9D A76F5F49 D1BF3825 130A30D3


###############################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
```

```
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                             0100
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    temp =
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                            0200
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        5FEA7A53
        F4A6C635 DC5FED69 1F36A168 A07266E7 75A7FB60 7BE9D680


    temp =
                                              E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  V is
                                              E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
```

```
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00E2524D 0E2D6956
    063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


Hash(counter||no_of_bits_to_return||input_string) is
                                                    FADECBC8
    A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


temp =
                                                    FADECBC8
    A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00E2524D 0E2D6956
    063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


Hash(counter||no_of_bits_to_return||input_string) is
                                                    90A2F07A
    9E31D50D 5B7DE500 5AD7C1E8 9A3E1AFE D62C331D 6A561403


temp =
                                              FADECB C8A4B733
    F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
    7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614
```

C is
                                                FADECB C8A4B733
      F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
      7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614

First call to Generate

****

Hash_DRBG_Generate_algorithm

requested_number_of_bits = 448

additional_input
                                                606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

Process additional_input

0x02||V||additional_input is
                          02E252 4D0E2D69 56063403 E1373C2A
      03105C27 C33EFD4B E0E0CB74 62D95FEA 7A53F4A6 C635DC5F
      ED691F36 A168A072 66E775A7 FB607BE9 D6606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

w=Hash(0x02||V||additional_input) is
                                                      FC650A81
      245264C9 C4784731 6CC37582 91DDA47F 4276B81A 036889B5

V is
                                                E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7463 D5C4F4FB
      78470B8F FA54A71E D5E2AC23 FA7E16E6 29EC6015 63E4738B

```
Hashgen

  requested_no_of_bits  = 448

  ------------

  i = 1

  data is
                                                E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7463 D5C4F4FB
      78470B8F FA54A71E D5E2AC23 FA7E16E6 29EC6015 63E4738B


  w_i is
                                                       AE2E703E
      D178DC74 31D2B9C3 09C52AE4 AE5742AF C119A0FB 8F500FDD


  W is
                                                       AE2E703E
      D178DC74 31D2B9C3 09C52AE4 AE5742AF C119A0FB 8F500FDD


  ------------

  i = 2

  data is
                                                E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7463 D5C4F4FB
      78470B8F FA54A71E D5E2AC23 FA7E16E6 29EC6015 63E4738C


  w_i is
                                                       83F17226
      1AD9FA6D 6203E549 33B07E9C B635CEA8 3F1F80FB 7A7153A1


  W is
                                             AE2E703E D178DC74
      31D2B9C3 09C52AE4 AE5742AF C119A0FB 8F500FDD 83F17226
      1AD9FA6D 6203E549 33B07E9C B635CEA8 3F1F80FB 7A7153A1
```

```
  returned_bits is
                                                AE2E703E D178DC74
        31D2B9C3 09C52AE4 AE5742AF C119A0FB 8F500FDD 83F17226
        1AD9FA6D 6203E549 33B07E9C B635CEA8 3F1F80FB 7A7153A1


--------------------------

  Update V

    0x03||V is
                                                03E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7463 D5C4F4FB
        78470B8F FA54A71E D5E2AC23 FA7E16E6 29EC6015 63E4738B


    H is
                                                            DA5B71E5
        F0C9872F A4BB580D ED2D80A5 7DB2582B FE2FB539 8C52A5F7


  Updated values

  V is
                                                  DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB9 13B109D1
        E3AEC494 AC6B7D11 C36B048B 60CAAD2D 26F24182 0DA16F97


  reseed_counter is
                                                     0000 00000002


rnd_val is
                                                AE2E703E D178DC74
        31D2B9C3 09C52AE4 AE5742AF C119A0FB 8F500FDD 83F17226
        1AD9FA6D 6203E549 33B07E9C B635CEA8 3F1F80FB 7A7153A1


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 448

  additional_input
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           02DD31 18D6D220 89FFDD07 D0EF34F3
        5744B0FB 3E6C49C2 9963560E B913B109 D1E3AEC4 94AC6B7D
        11C36B04 8B60CAAD 2D26F241 820DA16F 97A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                                                      B90A7495
        AA5FCC34 49236DF0 7084B861 AE7B5FC3 50839FFE DB6589CC


    V is
                                                DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB9 CCBB7E67
        8E0E90C8 F58EEB02 33EFBCED 0F460CF0 7775E180 E906F963


---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                                DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB9 CCBB7E67
        8E0E90C8 F58EEB02 33EFBCED 0F460CF0 7775E180 E906F963
```

```
    w_i is
                                                          E3C91764
        215E04D2 9751C152 8D7CBBF8 4E7CC370 2ADA3A1F 79F87DBB


    W is
                                                          E3C91764
        215E04D2 9751C152 8D7CBBF8 4E7CC370 2ADA3A1F 79F87DBB


    ------------

    i = 2

    data is
                                                DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB9 CCBB7E67
        8E0E90C8 F58EEB02 33EFBCED 0F460CF0 7775E180 E906F964


    w_i is
                                                          6043202F
        F7450A58 A73B95E3 2E4C0513 D0B6118A 677592EB ACC49FBE


    W is
                                              E3C91764 215E04D2
        9751C152 8D7CBBF8 4E7CC370 2ADA3A1F 79F87DBB 6043202F
        F7450A58 A73B95E3 2E4C0513 D0B6118A 677592EB ACC49FBE


  returned_bits is
                                              E3C91764 215E04D2
        9751C152 8D7CBBF8 4E7CC370 2ADA3A1F 79F87DBB 6043202F
        F7450A58 A73B95E3 2E4C0513 D0B6118A 677592EB ACC49FBE


--------------------------

  Update V

    0x03||V is
                                              03DD3118 D6D22089
        FFDD07D0 EF34F357 44B0FB3E 6C49C299 63560EB9 CCBB7E67
```

```
        8E0E90C8 F58EEB02 33EFBCED 0F460CF0 7775E180 E906F963


    H is
                                                        0C16F778
        4D6335D4 B4509A6E 9F6A44F5 364BC454 8A6582C2 C20D1FCB


  Updated values

  V is
                                                  D80FE4 9F76D7BD
        F9860BC0 A72DBCAB 7905CEB9 99963951 E5E0A90E 3C6318D0
        560FF872 B73B0355 D3B4D9A4 2E2C0F60 00B19076 C87E6F44


  reseed_counter is
                                                     0000 00000003


rnd_val is
                                               E3C91764 215E04D2
        9751C152 8D7CBBF8 4E7CC370 2ADA3A1F 79F87DBB 6043202F
        F7450A58 A73B95E3 2E4C0513 D0B6118A 677592EB ACC49FBE


###############################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    no_of_bits_to_return = 440
```

```
   ------------

   i = 1

   counter||no_of_bits_to_return||input_string is
                  010000 01B80001 02030405 06070809 0A0B0C0D
       0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
       26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


   Hash(counter||no_of_bits_to_return||input_string) is
                                                      0BB6E53D
       916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


   temp =
                                                      0BB6E53D
       916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


   ------------

   i = 2

   counter||no_of_bits_to_return||input_string is
                  020000 01B80001 02030405 06070809 0A0B0C0D
       0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
       26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


   Hash(counter||no_of_bits_to_return||input_string) is
                                                      33D18070
       2841C3D3 7CA40F35 645ECB1A A6548550 7F577CA9 8F418A0E


   temp =
                                                0BB6E5 3D916573
       A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
       702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


V is
                                                0BB6E5 3D916573
       A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
       702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                       E5B7AE6C
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    temp =
                                                       E5B7AE6C
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                       11F35DAE
```

```
        12883480 7F41DD3A A952DE09 0AB3C78C C4D38F67 F13F7896


    temp =
                                                E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


  C is
                                                E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                             010BB6 E53D9165 73A7AC79 6702CA6D
```

```
    D2E30D13 B8A3ACFD 7E23905D 6F8A33D1 80702841 C3D37CA4
    0F35645E CB1AA654 85507F57 7CA98F41 8A808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
             01000001 B8010BB6 E53D9165 73A7AC79 6702CA6D
    D2E30D13 B8A3ACFD 7E23905D 6F8A33D1 80702841 C3D37CA4
    0F35645E CB1AA654 85507F57 7CA98F41 8A808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                                 61745177
    968386F7 F279CA4A 2434BF94 97B5DF91 29D19843 184B652B


temp =
                                                 61745177
    968386F7 F279CA4A 2434BF94 97B5DF91 29D19843 184B652B


------------

i = 2

counter||no_of_bits_to_return||input_string is
             02000001 B8010BB6 E53D9165 73A7AC79 6702CA6D
    D2E30D13 B8A3ACFD 7E23905D 6F8A33D1 80702841 C3D37CA4
    0F35645E CB1AA654 85507F57 7CA98F41 8A808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                                 EF41D39F
    DC19F1E4 C54298AD 29F596FA 8D4F47CD 0081697F AFB07A4B
```

```
    temp =
                                                 617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


  V is
                                                 617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               00617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                     E5912949
        19DD3D92 743988D8 6C7927A6 94A6D90C 502FA7AA 5414F501


    temp =
                                                     E5912949
        19DD3D92 743988D8 6C7927A6 94A6D90C 502FA7AA 5414F501


    ------------
```

```
    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        0A2967F3
        30B7C64E 191BDC23 0C6CF679 4031D63D 1E92E4D9 151FF346


    temp =
                                              E59129 4919DD3D
        92743988 D86C7927 A694A6D9 0C502FA7 AA5414F5 010A2967
        F330B7C6 4E191BDC 230C6CF6 794031D6 3D1E92E4 D9151FF3


  C is
                                              E59129 4919DD3D
        92743988 D86C7927 A694A6D9 0C502FA7 AA5414F5 010A2967
        F330B7C6 4E191BDC 230C6CF6 794031D6 3D1E92E4 D9151FF3


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                              617451 77968386
```

```
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


    w_i is
                                                        3FE2AD85
        24CE60E7 C21C38A1 DAB02F3C 20501182 F389EE69 9F03FD87


    W is
                                                        3FE2AD85
        24CE60E7 C21C38A1 DAB02F3C 20501182 F389EE69 9F03FD87


    ------------

    i = 2

    data is
                                              617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07B


    w_i is
                                                        79ED17C6
        5B87ACEE EBF1D146 E7EE106C EC8955EE AFC18ABB C562A566


    W is
                                              3FE2AD85 24CE60E7
        C21C38A1 DAB02F3C 20501182 F389EE69 9F03FD87 79ED17C6
        5B87ACEE EBF1D146 E7EE106C EC8955EE AFC18ABB C562A566


  returned_bits is
                                              3FE2AD85 24CE60E7
        C21C38A1 DAB02F3C 20501182 F389EE69 9F03FD87 79ED17C6
        5B87ACEE EBF1D146 E7EE106C EC8955EE AFC18ABB C562A566


---------------------------

  Update V

    0x03||V is
```

```
                                                03617451 77968386
        F7F279CA 4A2434BF 9497B5DF 9129D198 43184B65 2BEF41D3
        9FDC19F1 E4C54298 AD29F596 FA8D4F47 CD008169 7FAFB07A


    H is
                                                          8F7D2138
        AD260EA2 51ECF405 9CFBA902 98790557 49981439 47C7CE66


  Updated values

  V is
                                                  47057A C0B060C4
        8A66B353 2290ADE7 3B2C5CB8 9D7A013F ED6C605A BC768C74
        4032E05A 84CB527A 6D320B90 0C468675 53B72887 A08C9ED4


  reseed_counter is
                                                     0000 00000002


rnd_val is
                                                3FE2AD85 24CE60E7
        C21C38A1 DAB02F3C 20501182 F389EE69 9F03FD87 79ED17C6
        5B87ACEE EBF1D146 E7EE106C EC8955EE AFC18ABB C562A566


-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
```

```
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input <empty>

----------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                           014705 7AC0B060 C48A66B3 532290AD
        E73B2C5C B89D7A01 3FED6C60 5ABC768C 744032E0 5A84CB52
        7A6D320B 900C4686 7553B728 87A08C9E D4C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B8014705 7AC0B060 C48A66B3 532290AD
        E73B2C5C B89D7A01 3FED6C60 5ABC768C 744032E0 5A84CB52
        7A6D320B 900C4686 7553B728 87A08C9E D4C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                      D061978A
        A8FA51B3 48ADD35F 9590A3E0 60826012 749A8AF8 3051C0B1


    temp =
                                                      D061978A
        A8FA51B3 48ADD35F 9590A3E0 60826012 749A8AF8 3051C0B1


    ------------

    i = 2
```

```
    counter||no_of_bits_to_return||input_string is
                02000001 B8014705 7AC0B060 C48A66B3 532290AD
        E73B2C5C B89D7A01 3FED6C60 5ABC768C 744032E0 5A84CB52
        7A6D320B 900C4686 7553B728 87A08C9E D4C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        5D22F7FD
        6C4BABE0 85D0232C 4AABF0AD C434722F B2B4DCBB 85E16C2D


    temp =
                                              D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


  V is
                                              D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                                                        708724BF
        4E161788 2C0EEF91 2F98DE09 CFD9B773 AE93E33E 3AD3F48A


    temp =
                                                        708724BF
        4E161788 2C0EEF91 2F98DE09 CFD9B773 AE93E33E 3AD3F48A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        91813DC5
        88497C56 9AAEDFB8 591AF62E E6679F0E 5F696843 D5664DCF


    temp =
                                                708724 BF4E1617
        882C0EEF 912F98DE 09CFD9B7 73AE93E3 3E3AD3F4 8A91813D
        C588497C 569AAEDF B8591AF6 2EE6679F 0E5F6968 43D5664D


  C is
                                                708724 BF4E1617
        882C0EEF 912F98DE 09CFD9B7 73AE93E3 3E3AD3F4 8A91813D
        C588497C 569AAEDF B8591AF6 2EE6679F 0E5F6968 43D5664D


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                                D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


    w_i is
                                                       8BB49B0B
        9C2FC701 89B24E02 73595458 CD780FBF A5F21612 2421B80B


    W is
                                                       8BB49B0B
        9C2FC701 89B24E02 73595458 CD780FBF A5F21612 2421B80B


    ------------

    i = 2

    data is
                                                D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16D


    w_i is
                                                       F773D736
        E6E11DEB B42477D6 9668D2F9 40C660F6 A2C1C9B4 179592E0


    W is
                                               8BB49B0B 9C2FC701
        89B24E02 73595458 CD780FBF A5F21612 2421B80B F773D736
        E6E11DEB B42477D6 9668D2F9 40C660F6 A2C1C9B4 179592E0
```

```
  returned_bits is
                                                  8BB49B0B 9C2FC701
        89B24E02 73595458 CD780FBF A5F21612 2421B80B F773D736
        E6E11DEB B42477D6 9668D2F9 40C660F6 A2C1C9B4 179592E0


---------------------------

  Update V

    0x03||V is
                                                  03D06197 8AA8FA51
        B348ADD3 5F9590A3 E0608260 12749A8A F83051C0 B15D22F7
        FD6C4BAB E085D023 2C4AABF0 ADC43472 2FB2B4DC BB85E16C


    H is
                                                              D187B76F
        837D624C C97B272F 04F68758 518D0E71 481D8A26 B15F5374


  Updated values

  V is
                                                    40E8BC 49F71069
        3B74BCC2 F0C52981 EA305C17 86232E6E 366B25B6 0D765BA5
        4671F775 009BA631 E99A4E3F 2E37AA82 862FA86B B0BA9B2E


  reseed_counter is
                                                      0000 00000002


rnd_val is
                                                  8BB49B0B 9C2FC701
        89B24E02 73595458 CD780FBF A5F21612 2421B80B F773D736
        E6E11DEB B42477D6 9668D2F9 40C660F6 A2C1C9B4 179592E0


##############################################################

Hash_DRBG

    Requested Security Strength = 112
```

```
    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                    010000 01B80001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A


    temp =
                                                        0BB6E53D
        916573A7 AC796702 CA6DD2E3 0D13B8A3 ACFD7E23 905D6F8A
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                  020000 01B80001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    Hash(counter||no_of_bits_to_return||input_string) is
                                                       33D18070
        2841C3D3 7CA40F35 645ECB1A A6548550 7F577CA9 8F418A0E


    temp =
                                              0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


  V is
                                              0BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                           000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
```

```
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        E5B7AE6C
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    temp =
                                                        E5B7AE6C
        8607715A F6CCCF35 2696C291 F43D10D1 E48E9FD0 717320C0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 000BB6E5 3D916573
        A7AC7967 02CA6DD2 E30D13B8 A3ACFD7E 23905D6F 8A33D180
        702841C3 D37CA40F 35645ECB 1AA65485 507F577C A98F418A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        11F35DAE
        12883480 7F41DD3A A952DE09 0AB3C78C C4D38F67 F13F7896


    temp =
                                                  E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


  C is
                                                  E5B7AE 6C860771
        5AF6CCCF 352696C2 91F43D10 D1E48E9F D0717320 C011F35D
        AE128834 807F41DD 3AA952DE 090AB3C7 8CC4D38F 67F13F78


----------------------------------------------------------------

First call to Generate

****************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            010B B6E53D91 6573A7AC 796702CA 6DD2E30D 13B8A3AC
        FD7E2390 5D6F8A33 D1807028 41C3D37C A40F3564 5ECB1AA6
        5485507F 577CA98F 418A8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    no_of_bits_to_return = 440

    ------------

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
                                                        010000
    01B8010B B6E53D91 6573A7AC 796702CA 6DD2E30D 13B8A3AC
    FD7E2390 5D6F8A33 D1807028 41C3D37C A40F3564 5ECB1AA6
    5485507F 577CA98F 418A8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                                      FCAB6277
    48788F7F EEF50098 68779B47 3D608D85 D2214B8B 231262E1


temp =
                                                      FCAB6277
    48788F7F EEF50098 68779B47 3D608D85 D2214B8B 231262E1


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    01B8010B B6E53D91 6573A7AC 796702CA 6DD2E30D 13B8A3AC
    FD7E2390 5D6F8A33 D1807028 41C3D37C A40F3564 5ECB1AA6
    5485507F 577CA98F 418A8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                                      20DE6D88
    52E4679D 02FF39FF D6260E0D D59B11E1 22FD190F 2120DE4B


temp =
                                              FCAB62 7748788F
    7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
    8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE
```

```
  V is
                                                 FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               00FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE


    Hash(counter||no_of_bits_to_return||input_string) is
                                                     37284C74
        6B01798D F00645F4 4F45B16F 162E3308 EABE1298 D80B27C8


    temp =
                                                     37284C74
        6B01798D F00645F4 4F45B16F 162E3308 EABE1298 D80B27C8


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 00FCAB62 7748788F
```

```
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        B59DBCB6
        5FE5CD7C 622751F2 14389150 1ED1BFCD 702D7DE5 326A5822


    temp =
                                              37284C 746B0179
        8DF00645 F44F45B1 6F162E33 08EABE12 98D80B27 C8B59DBC
        B65FE5CD 7C622751 F2143891 501ED1BF CD702D7D E5326A58


  C is
                                              37284C 746B0179
        8DF00645 F44F45B1 6F162E33 08EABE12 98D80B27 C8B59DBC
        B65FE5CD 7C622751 F2143891 501ED1BF CD702D7D E5326A58


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                              FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE


    w_i is
```

```
                                                        DE976A14
        41A637C1 B1B12E51 B6D08E77 4F6257D3 4A5D8415 D7334287


    W is
                                                        DE976A14
        41A637C1 B1B12E51 B6D08E77 4F6257D3 4A5D8415 D7334287


    ------------

    i = 2

    data is
                                              FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DF


    w_i is
                                                        EE68606D
        6936A310 A079D934 1BC828B4 D1BB7A94 D0BCB9F9 BDD3C926


    W is
                                              DE976A14 41A637C1
        B1B12E51 B6D08E77 4F6257D3 4A5D8415 D7334287 EE68606D
        6936A310 A079D934 1BC828B4 D1BB7A94 D0BCB9F9 BDD3C926


  returned_bits is
                                              DE976A14 41A637C1
        B1B12E51 B6D08E77 4F6257D3 4A5D8415 D7334287 EE68606D
        6936A310 A079D934 1BC828B4 D1BB7A94 D0BCB9F9 BDD3C926


--------------------------

  Update V

    0x03||V is
                                              03FCAB62 7748788F
        7FEEF500 9868779B 473D608D 85D2214B 8B231262 E120DE6D
        8852E467 9D02FF39 FFD6260E 0DD59B11 E122FD19 0F2120DE
```

```
    H is
                                                          D13D8EA6
        39863AC1 6CE34F4C D36365E0 D1A2EF5B 21314144 A950CAE2


  Updated values

  V is
                                                 33D3AE EBB37A09
        0DDEFB46 8CB7BD4C B6538EC0 8EBCDF5E 23FB1D8B 7B140AD0
        783904F6 864875D8 C54DC480 2F975C2C CFC46BDB 9DA45619


  reseed_counter is
                                                    0000 00000002


rnd_val is
                                               DE976A14 41A637C1
        B1B12E51 B6D08E77 4F6257D3 4A5D8415 D7334287 EE68606D
        6936A310 A079D934 1BC828B4 D1BB7A94 D0BCB9F9 BDD3C926


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
---------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                 C0C1C2 C3C4C5C6
```

```
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0133 D3AEEBB3 7A090DDE FB468CB7 BD4CB653 8EC08EBC
        DF5E23FB 1D8B7B14 0AD07839 04F68648 75D8C54D C4802F97
        5C2CCFC4 6BDB9DA4 5619C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        01B80133 D3AEEBB3 7A090DDE FB468CB7 BD4CB653 8EC08EBC
        DF5E23FB 1D8B7B14 0AD07839 04F68648 75D8C54D C4802F97
        5C2CCFC4 6BDB9DA4 5619C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                      609F2481
        705555CB 3B3FF6E7 70C6115B F69D1239 478D7E77 D862349E
```

```
    temp =
                                                          609F2481
        705555CB 3B3FF6E7 70C6115B F69D1239 478D7E77 D862349E


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                            020000
        01B80133 D3AEEBB3 7A090DDE FB468CB7 BD4CB653 8EC08EBC
        DF5E23FB 1D8B7B14 0AD07839 04F68648 75D8C54D C4802F97
        5C2CCFC4 6BDB9DA4 5619C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                          91A91BD5
        D0043690 034687A4 27F9B505 9AFF2774 B32688BA 9C8675CB


    temp =
                                                609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


  V is
                                                609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               00609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675
```

```
  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 00609F24 81705555
      CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
      D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    C0CCD185
      2BE68FE5 1D3B077B DC14D672 15306286 FAE0F914 4FB4755E


  temp =
                                                    C0CCD185
      2BE68FE5 1D3B077B DC14D672 15306286 FAE0F914 4FB4755E


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 00609F24 81705555
      CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
      D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    7F045F9F
      75650E14 6FDFF3D4 7A492886 14E6C930 990BDB18 349833AB


  temp =
                                            C0CCD1 852BE68F
      E51D3B07 7BDC14D6 72153062 86FAE0F9 144FB475 5E7F045F
      9F75650E 146FDFF3 D47A4928 8614E6C9 30990BDB 18349833


C is
                                            C0CCD1 852BE68F
```

```
        E51D3B07 7BDC14D6 72153062 86FAE0F9 144FB475 5E7F045F
        9F75650E 146FDFF3 D47A4928 8614E6C9 30990BDB 18349833


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                                609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


    w_i is
                                                        E8593358
        63B8A94D 3A2CD1CD 810939EC F9E41B82 74A95724 0324C575


    W is
                                                        E8593358
        63B8A94D 3A2CD1CD 810939EC F9E41B82 74A95724 0324C575


    ------------

    i = 2

    data is
                                                609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8676
```

```
    w_i is
                                                            7737A885
        78F0F807 1B1E5433 8CC81A72 6BC3836F 8941BF64 EC34B884


    W is
                                                E8593358 63B8A94D
        3A2CD1CD 810939EC F9E41B82 74A95724 0324C575 7737A885
        78F0F807 1B1E5433 8CC81A72 6BC3836F 8941BF64 EC34B884


  returned_bits is
                                                E8593358 63B8A94D
        3A2CD1CD 810939EC F9E41B82 74A95724 0324C575 7737A885
        78F0F807 1B1E5433 8CC81A72 6BC3836F 8941BF64 EC34B884


---------------------------

  Update V

    0x03||V is
                                                03609F24 81705555
        CB3B3FF6 E770C611 5BF69D12 39478D7E 77D86234 9E91A91B
        D5D00436 90034687 A427F9B5 059AFF27 74B32688 BA9C8675


    H is
                                                            F2FA7521
        1A83F14A 56A33E25 85992F86 12AD78B7 354FE28A 1D1DFB0D


  Updated values

  V is
                                                  216BF6 069C3BE5
        B0587AFE 634CDAE7 CE0BCD74 C0426E77 8C2816AA F00B229C
        8FC95A8E FB1664A0 FE3B7263 9E5D5EA7 DA9C14ED EFEF19B6


  reseed_counter is
                                                    0000 00000002
```

```
rnd_val is
                                                E8593358 63B8A94D
        3A2CD1CD 810939EC F9E41B82 74A95724 0324C575 7737A885
        78F0F807 1B1E5433 8CC81A72 6BC3836F 8941BF64 EC34B884


##############################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

##############################################################
```

```
**************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                 202122 23242526


    personal_str is
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                           0100
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
```

```
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    temp =
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                              0200
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        5FEA7A53
        F4A6C635 DC5FED69 1F36A168 A07266E7 75A7FB60 7BE9D680


    temp =
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  V is
                                                E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


--------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                                              00E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
      53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 00E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
      53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    FADECBC8
      A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


  temp =
                                                    FADECBC8
      A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 00E2524D 0E2D6956
      063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
      53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  Hash(counter||no_of_bits_to_return||input_string) is
                                                    90A2F07A
      9E31D50D 5B7DE500 5AD7C1E8 9A3E1AFE D62C331D 6A561403


  temp =
```

                                                FADECB C8A4B733
        F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
        7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614

  C is
                                                FADECB C8A4B733
        F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
        7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614

First call to Generate

****

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

Generate FAILED: Reseed is required

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

  additional_input <empty>

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            01E252 4D0E2D69 56063403 E1373C2A
        03105C27 C33EFD4B E0E0CB74 62D95FEA 7A53F4A6 C635DC5F
        ED691F36 A168A072 66E775A7 FB607BE9 D6808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

```
no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
             01000001 B801E252 4D0E2D69 56063403 E1373C2A
    03105C27 C33EFD4B E0E0CB74 62D95FEA 7A53F4A6 C635DC5F
    ED691F36 A168A072 66E775A7 FB607BE9 D6808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                                564A35DB
    8325A793 1214594B CFC4A00D B9F4129E 89BA79BA 5FE29EDC


temp =
                                                564A35DB
    8325A793 1214594B CFC4A00D B9F4129E 89BA79BA 5FE29EDC


------------

i = 2

counter||no_of_bits_to_return||input_string is
             02000001 B801E252 4D0E2D69 56063403 E1373C2A
    03105C27 C33EFD4B E0E0CB74 62D95FEA 7A53F4A6 C635DC5F
    ED691F36 A168A072 66E775A7 FB607BE9 D6808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                                610C0841
    28F1C76C 654FD153 BDCA19F1 C1C076B7 4B8DC995 4767B399


temp =
                                              564A35 DB8325A7
    93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
```

```
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3


  V is
                                                564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                             00564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3


    Hash(counter||no_of_bits_to_return||input_string) is
                                                       4D3FC5A7
        AF736648 D9432578 04E5A34F EE10D86A 1DAE2041 8A14EF1A


    temp =
                                                       4D3FC5A7
        AF736648 D9432578 04E5A34F EE10D86A 1DAE2041 8A14EF1A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
```

```
                                02 000001B8 00564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3


    Hash(counter||no_of_bits_to_return||input_string) is
                                                      56D55D4B
        B3D34A32 385822C3 BDB2BE83 0AAFD635 679F60CE 5790A03E


    temp =
                                               4D3FC5 A7AF7366
        48D94325 7804E5A3 4FEE10D8 6A1DAE20 418A14EF 1A56D55D
        4BB3D34A 32385822 C3BDB2BE 830AAFD6 35679F60 CE5790A0


  C is
                                               4D3FC5 A7AF7366
        48D94325 7804E5A3 4FEE10D8 6A1DAE20 418A14EF 1A56D55D
        4BB3D34A 32385822 C3BDB2BE 830AAFD6 35679F60 CE5790A0


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 448

    ------------

    i = 1

    data is
                                               564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3
```

```
    w_i is
                                                          B390977A
        DEFACF7D 3DF3C5B2 533FCC45 113DAEB1 9366DF1E 0A6EA52B


    W is
                                                          B390977A
        DEFACF7D 3DF3C5B2 533FCC45 113DAEB1 9366DF1E 0A6EA52B


    ------------

    i = 2

    data is
                                                 564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B4


    w_i is
                                                          4D35B60C
        584D75A0 D8E6A31C 6941C885 A7B25EBB 61C220E0 2DDB0426


    W is
                                                 B390977A DEFACF7D
        3DF3C5B2 533FCC45 113DAEB1 9366DF1E 0A6EA52B 4D35B60C
        584D75A0 D8E6A31C 6941C885 A7B25EBB 61C220E0 2DDB0426


  returned_bits is
                                                 B390977A DEFACF7D
        3DF3C5B2 533FCC45 113DAEB1 9366DF1E 0A6EA52B 4D35B60C
        584D75A0 D8E6A31C 6941C885 A7B25EBB 61C220E0 2DDB0426


---------------------------

  Update V

    0x03||V is
                                                 03564A35 DB8325A7
        93121459 4BCFC4A0 0DB9F412 9E89BA79 BA5FE29E DC610C08
        4128F1C7 6C654FD1 53BDCA19 F1C1C076 B74B8DC9 954767B3
```

```
    H is
                                                          380EBE6A
         AFD83737 E58795AC 92561432 F333A595 34DADC6C 94D69945


  Updated values

  V is
                                                  A389FB 8332990D
         DBEB577E C3D4AA43 5DA804EB 08A76899 FBE9F78E 2EC69FD0
         3CB4FC49 84253DA0 A9D1910B 680015E2 218E0996 F8759199


  reseed_counter is
                                                    0000 00000002


rnd_val is
                                                 B390977A DEFACF7D
         3DF3C5B2 533FCC45 113DAEB1 9366DF1E 0A6EA52B 4D35B60C
         584D75A0 D8E6A31C 6941C885 A7B25EBB 61C220E0 2DDB0426


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  C0C1C2 C3C4C5C6
         C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
         DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            01A389 FB833299 0DDBEB57 7EC3D4AA
        435DA804 EB08A768 99FBE9F7 8E2EC69F D03CB4FC 4984253D
        A0A9D191 0B680015 E2218E09 96F87591 99C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B801A389 FB833299 0DDBEB57 7EC3D4AA
        435DA804 EB08A768 99FBE9F7 8E2EC69F D03CB4FC 4984253D
        A0A9D191 0B680015 E2218E09 96F87591 99C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                    C792A300
        9915EAC0 3FE567B3 70AB5B70 D7C8B9FE 1D8BA65B 73054353


    temp =
                                                    C792A300
        9915EAC0 3FE567B3 70AB5B70 D7C8B9FE 1D8BA65B 73054353


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                 02000001 B801A389 FB833299 0DDBEB57 7EC3D4AA
        435DA804 EB08A768 99FBE9F7 8E2EC69F D03CB4FC 4984253D
```

```
        A0A9D191 0B680015 E2218E09 96F87591 99C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        D761BD4D
        04B6964D AC8FC294 83E3E3F0 A584B853 2BB01E0F 18FEE1D1


    temp =
                                              C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


  V is
                                              C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        C9B79D99
```

```
        F0E8F7C2 0325C58E F8DCF907 6255EDF4 820DC35B A1DA01B7


    temp =
                                                        C9B79D99
        F0E8F7C2 0325C58E F8DCF907 6255EDF4 820DC35B A1DA01B7


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        CA142C8D
        58157FD7 76D401A9 55995DB7 08141880 A4F8E118 7C919F17


    temp =
                                              C9B79D 99F0E8F7
        C20325C5 8EF8DCF9 076255ED F4820DC3 5BA1DA01 B7CA142C
        8D58157F D776D401 A955995D B7081418 80A4F8E1 187C919F


  C is
                                              C9B79D 99F0E8F7
        C20325C5 8EF8DCF9 076255ED F4820DC3 5BA1DA01 B7CA142C
        8D58157F D776D401 A955995D B7081418 80A4F8E1 187C919F


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

----------------------------

  Hashgen
```

```
  requested_no_of_bits  = 448

  ------------

  i = 1

  data is
                                              C792A3 009915EA
      C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
      4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


  w_i is
                                                    258437C9
      CF68A286 1F3BE81F 80AC7864 78B65211 3613F79C 6D21C020


  W is
                                                    258437C9
      CF68A286 1F3BE81F 80AC7864 78B65211 3613F79C 6D21C020


  ------------

  i = 2

  data is
                                              C792A3 009915EA
      C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
      4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE2


  w_i is
                                                    B6CA5DFC
      35875873 10777745 B0B49B04 3EC0E4CD E1A31A57 C187E64D


  W is
                                           258437C9 CF68A286
      1F3BE81F 80AC7864 78B65211 3613F79C 6D21C020 B6CA5DFC
      35875873 10777745 B0B49B04 3EC0E4CD E1A31A57 C187E64D


returned_bits is
                                           258437C9 CF68A286
```

```
        1F3BE81F 80AC7864 78B65211 3613F79C 6D21C020 B6CA5DFC
        35875873 10777745 B0B49B04 3EC0E4CD E1A31A57 C187E64D


---------------------------

  Update V

    0x03||V is
                                              03C792A3 009915EA
        C03FE567 B370AB5B 70D7C8B9 FE1D8BA6 5B730543 53D761BD
        4D04B696 4DAC8FC2 9483E3E3 F0A584B8 532BB01E 0F18FEE1


    H is
                                                    6E801A28
        3CFDD3FA 7520BDAF 88C6FE83 2175EA33 567F3946 5F991C69


  Updated values

  V is
                                                914A40 9A89FEE2
        82430B2D 42698854 783A1EA7 F29F9969 B714DF45 7A219012
        175AA010 9A442173 C6A07BC4 C9238304 2A4FE245 872EACEA


  reseed_counter is
                                                  0000 00000002


rnd_val is
                                              258437C9 CF68A286
        1F3BE81F 80AC7864 78B65211 3613F79C 6D21C020 B6CA5DFC
        35875873 10777745 B0B49B04 3EC0E4CD E1A31A57 C187E64D


################################################################

Hash_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
```

```
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                              0100
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    temp =
                                                        E2524D0E
        2D695606 3403E137 3C2A0310 5C27C33E FD4BE0E0 CB7462D9


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                            0200
        0001B800 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        5FEA7A53
        F4A6C635 DC5FED69 1F36A168 A07266E7 75A7FB60 7BE9D680


    temp =
                                              E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


  V is
                                              E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
        53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00E2524D 0E2D6956
        063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
```

```
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00E2524D 0E2D6956
    063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


Hash(counter||no_of_bits_to_return||input_string) is
                                                    FADECBC8
    A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


temp =
                                                    FADECBC8
    A4B733F9 A903EFB7 F8C95434 54D37B2D 4C76B882 8A9A5463


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00E2524D 0E2D6956
    063403E1 373C2A03 105C27C3 3EFD4BE0 E0CB7462 D95FEA7A
    53F4A6C6 35DC5FED 691F36A1 68A07266 E775A7FB 607BE9D6


Hash(counter||no_of_bits_to_return||input_string) is
                                                    90A2F07A
    9E31D50D 5B7DE500 5AD7C1E8 9A3E1AFE D62C331D 6A561403


temp =
                                              FADECB C8A4B733
    F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
    7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614
```

```
  C is
                                                FADECB C8A4B733
        F9A903EF B7F8C954 3454D37B 2D4C76B8 828A9A54 6390A2F0
        7A9E31D5 0D5B7DE5 005AD7C1 E89A3E1A FED62C33 1D6A5614


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01E2 524D0E2D 69560634 03E1373C 2A03105C 27C33EFD
        4BE0E0CB 7462D95F EA7A53F4 A6C635DC 5FED691F 36A168A0
```

```
    7266E775 A7FB607B E9D68081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    01B801E2 524D0E2D 69560634 03E1373C 2A03105C 27C33EFD
    4BE0E0CB 7462D95F EA7A53F4 A6C635DC 5FED691F 36A168A0
    7266E775 A7FB607B E9D68081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                                    96C7FF18
    C18C5000 958F19BD D20537ED A5A01AA0 E0ACBD40 F3E77215


temp =
                                                    96C7FF18
    C18C5000 958F19BD D20537ED A5A01AA0 E0ACBD40 F3E77215


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    01B801E2 524D0E2D 69560634 03E1373C 2A03105C 27C33EFD
    4BE0E0CB 7462D95F EA7A53F4 A6C635DC 5FED691F 36A168A0
    7266E775 A7FB607B E9D68081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        46E4741C
        7BB1E820 3272FFA4 1A565735 65884C04 59569DDA D61A7A9F


    temp =
                                              96C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


  V is
                                              96C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            0096C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 0096C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        3E4105EB
        0DB7617D 06346DA9 3405164C 23FA5247 E549890C 761D7990
```

```
    temp =
                                                        3E4105EB
        0DB7617D 06346DA9 3405164C 23FA5247 E549890C 761D7990


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 0096C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        B06074C0
        564F00E0 010D23D2 DF8FABBC 5CE4A434 14A46EF8 A63C0BDC


    temp =
                                                  3E4105 EB0DB761
        7D06346D A9340516 4C23FA52 47E54989 0C761D79 90B06074
        C0564F00 E0010D23 D2DF8FAB BC5CE4A4 3414A46E F8A63C0B


  C is
                                                  3E4105 EB0DB761
        7D06346D A9340516 4C23FA52 47E54989 0C761D79 90B06074
        C0564F00 E0010D23 D2DF8FAB BC5CE4A4 3414A46E F8A63C0B


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 448
```

```
  ------------

  i = 1

  data is
                                                96C7FF 18C18C50
      00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
      1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


  w_i is
                                                       E41DCEFB
      B418588E 7AB62A63 0D52A955 E55CE37A 79DB568B CFA10A57


  W is
                                                       E41DCEFB
      B418588E 7AB62A63 0D52A955 E55CE37A 79DB568B CFA10A57


  ------------

  i = 2

  data is
                                                96C7FF 18C18C50
      00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
      1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7B


  w_i is
                                                       CD89C490
      447D43A8 83CDF14C F6367FC1 9EA52A46 3A1FE2EB 7DF168F6


  W is
                                             E41DCEFB B418588E
      7AB62A63 0D52A955 E55CE37A 79DB568B CFA10A57 CD89C490
      447D43A8 83CDF14C F6367FC1 9EA52A46 3A1FE2EB 7DF168F6


returned_bits is
                                             E41DCEFB B418588E
      7AB62A63 0D52A955 E55CE37A 79DB568B CFA10A57 CD89C490
      447D43A8 83CDF14C F6367FC1 9EA52A46 3A1FE2EB 7DF168F6
```

```
---------------------------

  Update V

    0x03||V is
                                                0396C7FF 18C18C50
        00958F19 BDD20537 EDA5A01A A0E0ACBD 40F3E772 1546E474
        1C7BB1E8 203272FF A41A5657 3565884C 0459569D DAD61A7A


    H is
                                                          8A397569
        1FBBD432 E574BB4E 64A74C4F 76506178 425EC799 1305F482


  Updated values

  V is
                                                  D50905 03CF43B1
        7D9BC387 67060A4E 39C99A6C E8C5F646 4D6A04EC 3030BA51
        FC8DD51B E5A83B71 DBA13252 6812CE68 7ACCC2A5 E6824B08


  reseed_counter is
                                                     0000 00000002


rnd_val is
                                                E41DCEFB B418588E
        7AB62A63 0D52A955 E55CE37A 79DB568B CFA10A57 CD89C490
        447D43A8 83CDF14C F6367FC1 9EA52A46 3A1FE2EB 7DF168F6


-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input
```

```
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01D5 090503CF 43B17D9B C3876706 0A4E39C9 9A6CE8C5
        F6464D6A 04EC3030 BA51FC8D D51BE5A8 3B71DBA1 32526812
        CE687ACC C2A5E682 4B08C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        01B801D5 090503CF 43B17D9B C3876706 0A4E39C9 9A6CE8C5
        F6464D6A 04EC3030 BA51FC8D D51BE5A8 3B71DBA1 32526812
```

```
        CE687ACC C2A5E682 4B08C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        FCC6C861
        900DDB57 BDC97001 8F6CF691 59C1B68E BA85E4B0 A9E2FDF3


    temp =
                                                        FCC6C861
        900DDB57 BDC97001 8F6CF691 59C1B68E BA85E4B0 A9E2FDF3


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                          020000
        01B801D5 090503CF 43B17D9B C3876706 0A4E39C9 9A6CE8C5
        F6464D6A 04EC3030 BA51FC8D D51BE5A8 3B71DBA1 32526812
        CE687ACC C2A5E682 4B08C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                        CEAB36C7
        DC9BC0A1 4BB7AB98 7481DB03 C014DAE1 3E734896 007224AA


    temp =
                                                FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224


V is
                                                FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
```

```
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224


    Hash(counter||no_of_bits_to_return||input_string) is
                                                    3618B297
        02390319 E360A7FC 627EC87B B6B1DA4A 36D40BB4 2030D850


    temp =
                                                    3618B297
        02390319 E360A7FC 627EC87B B6B1DA4A 36D40BB4 2030D850


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 00FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224


    Hash(counter||no_of_bits_to_return||input_string) is
```

                                                    D6FEBBB0
        BFC783A8 034F3B2F 02F272FD 91507588 6A0F6C44 3DD2FEFD

    temp =
                                                  3618B2 97023903
        19E360A7 FC627EC8 7BB6B1DA 4A36D40B B42030D8 50D6FEBB
        B0BFC783 A8034F3B 2F02F272 FD915075 886A0F6C 443DD2FE

  C is
                                                  3618B2 97023903
        19E360A7 FC627EC8 7BB6B1DA 4A36D40B B42030D8 50D6FEBB
        B0BFC783 A8034F3B 2F02F272 FD915075 886A0F6C 443DD2FE

****

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 448

  additional_input <empty>

  Hashgen

    requested_no_of_bits = 448

    ----

    i = 1

    data is
                                                  FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224

    w_i is
                                                    098BD7FB
        3E7B0673 F319E2ED A9240C9F 7A657200 C0F5482E BEE4EEC1

    W is

                                                    098BD7FB
        3E7B0673 F319E2ED A9240C9F 7A657200 C0F5482E BEE4EEC1

    ----

    i = 2

    data is
                                                  FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007225

    w_i is
                                                    C6395339
        E48B0B7A 01456745 BE894FC1 8A98B252 258DAEC4 D878C086

    W is
                                            098BD7FB 3E7B0673
        F319E2ED A9240C9F 7A657200 C0F5482E BEE4EEC1 C6395339
        E48B0B7A 01456745 BE894FC1 8A98B252 258DAEC4 D878C086

  returned_bits is
                                            098BD7FB 3E7B0673
        F319E2ED A9240C9F 7A657200 C0F5482E BEE4EEC1 C6395339
        E48B0B7A 01456745 BE894FC1 8A98B252 258DAEC4 D878C086

  Update V

    0x03||V is
                                            03FCC6C8 61900DDB
        57BDC970 018F6CF6 9159C1B6 8EBA85E4 B0A9E2FD F3CEAB36
        C7DC9BC0 A14BB7AB 987481DB 03C014DA E13E7348 96007224

    H is
                                                    CAED9D58
        9C88C301 C7611C02 E83ABC6F D76797DC CCCA8788 D91A3DB6

Updated values

V is

32DF7A F89246DE
71A12A17 FDF1EBBF 0D107390 D8F159F0 64CA13D7 0F93474B
15252646 10B022E9 AFB230BD D8B8FD2D 36730A3D B35882D9

reseed_counter is

0000 00000002

rnd_val is

098BD7FB 3E7B0673
F319E2ED A9240C9F 7A657200 C0F5482E BEE4EEC1 C6395339
E48B0B7A 01456745 BE894FC1 8A98B252 258DAEC4 D878C086

```
################################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                 20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                               AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


    temp =
                                               AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
```

```
                02000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                              167D84AF 64128C0D
        71F4D5B8 C0EDFBBE 3DF40448 D2D8E12F A91BA8B0 97969506


    temp =
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


  V is
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              E15DE4A8 E3B1419B
```

```
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    temp =
                                              E15DE4A8 E3B1419B
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              CFAAFDDC 90195902
        E979F79B 65357FEA 85998E4E 37D2C1D4 FD0F0D66 3A829565


    temp =
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


  C is
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    w_i is
                                               77E05A0E 7DC78AB5
        D8934D5E 93E82C06 A07C04CE E6C9C530 45EEB485 872777CF


    W is
                                               77E05A0E 7DC78AB5
        D8934D5E 93E82C06 A07C04CE E6C9C530 45EEB485 872777CF


    ------------

    i = 2

    data is
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E2


    w_i is
                                               3B3E35C4 74F976B8
        94BF301A 86FA651F 463970E8 9D4A0534 B2ECAD29 EC044E7E


    W is
                           77E05A0E 7DC78AB5 D8934D5E 93E82C06
        A07C04CE E6C9C530 45EEB485 872777CF 3B3E35C4 74F976B8
        94BF301A 86FA651F 463970E8 9D4A0534 B2ECAD29 EC044E7E
```

```
  returned_bits is
                          77E05A0E 7DC78AB5 D8934D5E 93E82C06
        A07C04CE E6C9C530 45EEB485 872777CF 3B3E35C4 74F976B8
        94BF301A 86FA651F 463970E8 9D4A0534 B2ECAD29 EC044E7E


---------------------------

  Update V

    0x03||V is
                                               03AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    H is
                                               FC0D84A6 B4556DFF
        3915BE7E 63044692 5ABC4032 81175379 3AFAD856 3240C4EC


  Updated values

  V is
                                                 8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 144E7579 368E9955
        BEFBE700 EEF87277 6B17AEFF D53D76F4 E3BE65E8 C94B708F


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          77E05A0E 7DC78AB5 D8934D5E 93E82C06
        A07C04CE E6C9C530 45EEB485 872777CF 3B3E35C4 74F976B8
        94BF301A 86FA651F 463970E8 9D4A0534 B2ECAD29 EC044E7E


-------------------------------------------------------------

Second call to Generate

*************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 144E7579 368E9955
        BEFBE700 EEF87277 6B17AEFF D53D76F4 E3BE65E8 C94B708F


    w_i is
                                               5FF4BA49 3C40CFFF
        3B01E472 C575668C CE3880B9 290B05BF EDE5EC96 ED5E9B28


    W is
                                               5FF4BA49 3C40CFFF
        3B01E472 C575668C CE3880B9 290B05BF EDE5EC96 ED5E9B28


    ------------

    i = 2

    data is
                                                8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 144E7579 368E9955
        BEFBE700 EEF87277 6B17AEFF D53D76F4 E3BE65E8 C94B7090


    w_i is
                                               98508B09 BC800EEE
        099A3C90 602ABD4B 1D4F343D 497C6055 C87BB956 D53BF351
```

```
    W is
                          5FF4BA49 3C40CFFF 3B01E472 C575668C
        CE3880B9 290B05BF EDE5EC96 ED5E9B28 98508B09 BC800EEE
        099A3C90 602ABD4B 1D4F343D 497C6055 C87BB956 D53BF351


  returned_bits is
                          5FF4BA49 3C40CFFF 3B01E472 C575668C
        CE3880B9 290B05BF EDE5EC96 ED5E9B28 98508B09 BC800EEE
        099A3C90 602ABD4B 1D4F343D 497C6055 C87BB956 D53BF351


---------------------------

  Update V

    0x03||V is
                                               038C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 144E7579 368E9955
        BEFBE700 EEF87277 6B17AEFF D53D76F4 E3BE65E8 C94B708F


    H is
                                               15D2C146 0EDF2565
        20C61E8A E5EEBBC5 6D12F9B0 FBF299BF B232B53F 0A43EC3F


  Updated values

  V is
                                                 6DFD97 35FF0E0E
        3FE0522F 58188B53 ED3FF670 05465290 44B62BE1 7D1B1C21
        D091B089 B1774795 DB1422A8 6C954634 8076B4B6 21C72F91


  reseed_counter is
                                                   0000 00000003


rnd_val is
                          5FF4BA49 3C40CFFF 3B01E472 C575668C
        CE3880B9 290B05BF EDE5EC96 ED5E9B28 98508B09 BC800EEE
        099A3C90 602ABD4B 1D4F343D 497C6055 C87BB956 D53BF351
```

```
################################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                               20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                               AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95
```

```
    temp =
                                                AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                 02000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                                167D84AF 64128C0D
        71F4D5B8 C0EDFBBE 3DF40448 D2D8E12F A91BA8B0 97969506


    temp =
                                                  AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


  V is
                                                  AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    no_of_bits_to_return = 440

    ------------
```

```
  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 00AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
      95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


  Hash(counter||no_of_bits_to_return||input_string) is
                                          E15DE4A8 E3B1419B
      61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


  temp =
                                          E15DE4A8 E3B1419B
      61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 00AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
      95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


  Hash(counter||no_of_bits_to_return||input_string) is
                                          CFAAFDDC 90195902
      E979F79B 65357FEA 85998E4E 37D2C1D4 FD0F0D66 3A829565


  temp =
                                            E15DE4 A8E3B141
      9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
      F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


C is
                                            E15DE4 A8E3B141
      9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
      F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1
```

```
-------------------------------------------------------------

First call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           02AB41 CDE437AB 8B091CA7 C5755D10
        F0110C1D BD462F22 6CFDABFB B04A8BCD EF95167D 84AF6412
        8C0D71F4 D5B8C0ED FBBE3DF4 0448D2D8 E1606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    w=Hash(0x02||V||additional_input) is
                                               5A0FEBC5 0A3DBB70
        91C99849 CCF32413 F39B9382 05D3ECF0 F67DBFF3 49CE00B9


    V is
                                                 AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226D 57BBE775 54C98960
        26E015CE 7C5736A0 010D8857 BE94DAEC B4BBB3F7 92A0D99A


---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------
```

```
  i = 1

  data is
                                                AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226D 57BBE775 54C98960
      26E015CE 7C5736A0 010D8857 BE94DAEC B4BBB3F7 92A0D99A


  w_i is
                                              510724B9 3AE9A182
      70E48473 711D8824 631BAA7F 1D9AC928 4E7EC8F3 637F7A74


  W is
                                              510724B9 3AE9A182
      70E48473 711D8824 631BAA7F 1D9AC928 4E7EC8F3 637F7A74


  ------------

  i = 2

  data is
                                                AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226D 57BBE775 54C98960
      26E015CE 7C5736A0 010D8857 BE94DAEC B4BBB3F7 92A0D99B


  w_i is
                                              3B3644EB 96C98627
      C8FD405A 7A4603F3 8CFF7C89 E9C133F5 851F40E9 2030FEA2


  W is
                        510724B9 3AE9A182 70E48473 711D8824
      631BAA7F 1D9AC928 4E7EC8F3 637F7A74 3B3644EB 96C98627
      C8FD405A 7A4603F3 8CFF7C89 E9C133F5 851F40E9 2030FEA2


returned_bits is
                        510724B9 3AE9A182 70E48473 711D8824
      631BAA7F 1D9AC928 4E7EC8F3 637F7A74 3B3644EB 96C98627
      C8FD405A 7A4603F3 8CFF7C89 E9C133F5 851F40E9 2030FEA2
```

```
--------------------------

  Update V

    0x03||V is
                                                03AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226D 57BBE775 54C98960
        26E015CE 7C5736A0 010D8857 BE94DAEC B4BBB3F7 92A0D99A


    H is
                                                AD825E98 ED18CBD2
        F80AA598 A9962F17 547ABD64 E6E5AE71 E28EFF9C FF1EDD85


  Updated values

  V is
                                                  8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 1FD33B30 798FB29A
        0FBA6665 027D7F10 5871BFB4 40DFBEDE 81D04D22 DFF789E1


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          510724B9 3AE9A182 70E48473 711D8824
        631BAA7F 1D9AC928 4E7EC8F3 637F7A74 3B3644EB 96C98627
        C8FD405A 7A4603F3 8CFF7C89 E9C133F5 851F40E9 2030FEA2


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
```

```
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           028C9F B28D1B5C CCA47E7C FA66BACE
        21FF260A 16A5BABA 7F1FD33B 30798FB2 9A0FBA66 65027D7F
        105871BF B440DFBE DE81D04D 22DFF789 E1A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                                              2E5668C1 70F5B45B
        F61C9814 6C3D84D7 B3A218D1 4FA4D6F7 6BE092AC E9905ADD


    V is
                                                8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 4E29A3F1 EA8566F6
        05D6FE79 6EBB03E8 0C13D885 908495D5 EDB0DFCF C987E4BE


---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 4E29A3F1 EA8566F6
        05D6FE79 6EBB03E8 0C13D885 908495D5 EDB0DFCF C987E4BE


    w_i is
                                              6253DA3A AE8B88A3
        B746E4C8 B2635C54 0F6E9EA7 157EE69D D71EFB2E 8FF7BBE1
```

```
    W is
                                              6253DA3A AE8B88A3
        B746E4C8 B2635C54 0F6E9EA7 157EE69D D71EFB2E 8FF7BBE1


    ------------

    i = 2

    data is
                                                8C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 4E29A3F1 EA8566F6
        05D6FE79 6EBB03E8 0C13D885 908495D5 EDB0DFCF C987E4BF


    w_i is
                                              E3336888 38DD7DE4
        9CC88990 309C96CD B2AB9295 7436BF83 D1BD8308 19C748CA


    W is
                           6253DA3A AE8B88A3 B746E4C8 B2635C54
        0F6E9EA7 157EE69D D71EFB2E 8FF7BBE1 E3336888 38DD7DE4
        9CC88990 309C96CD B2AB9295 7436BF83 D1BD8308 19C748CA


  returned_bits is
                           6253DA3A AE8B88A3 B746E4C8 B2635C54
        0F6E9EA7 157EE69D D71EFB2E 8FF7BBE1 E3336888 38DD7DE4
        9CC88990 309C96CD B2AB9295 7436BF83 D1BD8308 19C748CA


--------------------------

  Update V

    0x03||V is
                                              038C9FB2 8D1B5CCC
        A47E7CFA 66BACE21 FF260A16 A5BABA7F 4E29A3F1 EA8566F6
        05D6FE79 6EBB03E8 0C13D885 908495D5 EDB0DFCF C987E4BE


    H is
                                              78BDC1C4 0B7665A8
        0B03BCC3 5B54885F A183D8CE 23C628A8 F6435398 931F0A4F
```

```
  Updated values

  V is
                                                 6DFD97 35FF0E0E
        3FE0522F 58188B53 ED3FF670 05465290 E17C5AD8 2DA92A05
        01AA663A A69FA5A0 B0812B4B 4FAFF3FE CE79CCF6 AADEC1D0


  reseed_counter is
                                                   0000 00000003


rnd_val is
                          6253DA3A AE8B88A3 B746E4C8 B2635C54
        0F6E9EA7 157EE69D D71EFB2E 8FF7BBE1 E3336888 38DD7DE4
        9CC88990 309C96CD B2AB9295 7436BF83 D1BD8308 19C748CA


################################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
    Nonce =
                                                20212223 24252627


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                20212223 24252627


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
```

```
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                        010000
    01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36202122 23242526 27404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
                                        A3E94E39 26FDA169
    C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


temp =
                                        A3E94E39 26FDA169
    C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36202122 23242526 27404142 43444546
    4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
    5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


Hash(counter||no_of_bits_to_return||input_string) is
                                        71564B45 6FF2EEC8
    36422ACC 5A029935 A7992990 94A1CA74 1B916DC0 26A7E107
```

```
    temp =
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  V is
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


    Hash(counter||no_of_bits_to_return||input_string) is
                                              44748A78 B16E7555
        9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


    temp =
                                              44748A78 B16E7555
        9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


    ------------
```

```
    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


    Hash(counter||no_of_bits_to_return||input_string) is
                                              5F42CB6A 20C89D7C
        6EF3DC61 0D8FF203 D6766CED 1919D094 ED485EF7 FADDB668


    temp =
                                               44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


  C is
                                               44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


-------------------------------------------------------------

First call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1
```

```
    data is
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


    w_i is
                                               4A62664F 266EE537
        B90D64B0 5E1D813D 28B159A9 79F1509D DE31B71D A43D546E


    W is
                                               4A62664F 266EE537
        B90D64B0 5E1D813D 28B159A9 79F1509D DE31B71D A43D546E


    ------------

    i = 2

    data is
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CB


    w_i is
                                               E8E78678 202DC237
        AD4AFE7D F310C9A4 13E38AAF 417D2D22 5AA365EC 4A7D2996


    W is
                          4A62664F 266EE537 B90D64B0 5E1D813D
        28B159A9 79F1509D DE31B71D A43D546E E8E78678 202DC237
        AD4AFE7D F310C9A4 13E38AAF 417D2D22 5AA365EC 4A7D2996


  returned_bits is
                          4A62664F 266EE537 B90D64B0 5E1D813D
        28B159A9 79F1509D DE31B71D A43D546E E8E78678 202DC237
        AD4AFE7D F310C9A4 13E38AAF 417D2D22 5AA365EC 4A7D2996


---------------------------
```

```
  Update V

    0x03||V is
                                                03A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


    H is
                                                19B1A221 4356F101
        FFA0E21C BF22F2CF 985EE127 7506C7BD BA35EC15 7A81BADE


  Updated values

  V is
                                                  E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A66E E736DBAA 3BF1D028
        3B717B33 6EB3AE5B DD04172E A26E5A48 F3B3FBAB F82F7679


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          4A62664F 266EE537 B90D64B0 5E1D813D
        28B159A9 79F1509D DE31B71D A43D546E E8E78678 202DC237
        AD4AFE7D F310C9A4 13E38AAF 417D2D22 5AA365EC 4A7D2996


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen
```

```
  requested_no_of_bits  = 512

  ------------

  i = 1

  data is
                                                E85DD8 B1D86C16
      BF628BF3 B5F99704 4D2A6913 8CD6A66E E736DBAA 3BF1D028
      3B717B33 6EB3AE5B DD04172E A26E5A48 F3B3FBAB F82F7679


  w_i is
                                              59583D3C 0AC37130
      C4789A83 11B8CA8F 985EF1E8 F94D954E 32E344A6 21C24B2F


  W is
                                              59583D3C 0AC37130
      C4789A83 11B8CA8F 985EF1E8 F94D954E 32E344A6 21C24B2F


  ------------

  i = 2

  data is
                                                E85DD8 B1D86C16
      BF628BF3 B5F99704 4D2A6913 8CD6A66E E736DBAA 3BF1D028
      3B717B33 6EB3AE5B DD04172E A26E5A48 F3B3FBAB F82F767A


  w_i is
                                              371DA9BA 3C33153F
      09E55145 E762926B 73AC147A 1E8631D1 CCD08567 CF677C72


  W is
                        59583D3C 0AC37130 C4789A83 11B8CA8F
      985EF1E8 F94D954E 32E344A6 21C24B2F 371DA9BA 3C33153F
      09E55145 E762926B 73AC147A 1E8631D1 CCD08567 CF677C72


returned_bits is
                        59583D3C 0AC37130 C4789A83 11B8CA8F
```

```
        985EF1E8 F94D954E 32E344A6 21C24B2F 371DA9BA 3C33153F
        09E55145 E762926B 73AC147A 1E8631D1 CCD08567 CF677C72


---------------------------

  Update V

    0x03||V is
                                              03E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A66E E736DBAA 3BF1D028
        3B717B33 6EB3AE5B DD04172E A26E5A48 F3B3FBAB F82F7679


    H is
                                              B9688961 AE7D4A6C
        5202575B 9AA536DB E355DF79 CD8079E3 04D82BED 33D6CF22


  Updated values

  V is
                                                2CD263 2A89DA8C
        15021411 07BAF502 B97D38C4 48480871 0A66F840 11D7028D
        14D3155A 7379ADD5 3CC8EA84 D0FC641D FC629E06 191F5F6D


  reseed_counter is
                                                  0000 00000003


rnd_val is
                         59583D3C 0AC37130 C4789A83 11B8CA8F
        985EF1E8 F94D954E 32E344A6 21C24B2F 371DA9BA 3C33153F
        09E55145 E762926B 73AC147A 1E8631D1 CCD08567 CF677C72


##############################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
```

```
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                              20212223 24252627


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    temp =
                                                A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                              020000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                71564B45 6FF2EEC8
        36422ACC 5A029935 A7992990 94A1CA74 1B916DC0 26A7E107


    temp =
                                                  A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  V is
                                                  A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                00A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
```

```
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


Hash(counter||no_of_bits_to_return||input_string) is
                                        44748A78 B16E7555
    9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


temp =
                                        44748A78 B16E7555
    9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


Hash(counter||no_of_bits_to_return||input_string) is
                                        5F42CB6A 20C89D7C
    6EF3DC61 0D8FF203 D6766CED 1919D094 ED485EF7 FADDB668


temp =
                                          44748A 78B16E75
    559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
    875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0
```

```
  C is
                                                  44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           02A3E9 4E3926FD A169C303 D6643839
        05E0D799 62D16544 6D63BDA6 54D132F7 2DB47156 4B456FF2
        EEC83642 2ACC5A02 9935A799 299094A1 CA606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    w=Hash(0x02||V||additional_input) is
                                                 3CBE9AC4 CEFC9E53
        84B05F3A 13305C81 BB347128 578D087A D9CD6168 A7BBD90A


    V is
                                                  A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D A07C4119 A02F9581
        3921B585 58A04F70 836AB353 23E70B14 0F74FA92 38507AD4


---------------------------
```

Hashgen

requested_no_of_bits = 512

---

i = 1

data is

                                          A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D A07C4119 A02F9581
    3921B585 58A04F70 836AB353 23E70B14 0F74FA92 38507AD4

w_i is

                                         E0B97C82 1268FD3B
    B2CABFD1 F9548478 AE8A6041 7F7B094A 26139546 062B521C

W is

                                         E0B97C82 1268FD3B
    B2CABFD1 F9548478 AE8A6041 7F7B094A 26139546 062B521C

---

i = 2

data is

                                          A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D A07C4119 A02F9581
    3921B585 58A04F70 836AB353 23E70B14 0F74FA92 38507AD5

w_i is

                                         FD33E4E3 9B9DCD0A
    3DA15209 C72ADBE5 8C20AB34 07026951 297AD254 307553A5

W is

                        E0B97C82 1268FD3B B2CABFD1 F9548478
    AE8A6041 7F7B094A 26139546 062B521C FD33E4E3 9B9DCD0A
    3DA15209 C72ADBE5 8C20AB34 07026951 297AD254 307553A5

```
  returned_bits is
                           E0B97C82 1268FD3B B2CABFD1 F9548478
        AE8A6041 7F7B094A 26139546 062B521C FD33E4E3 9B9DCD0A
        3DA15209 C72ADBE5 8C20AB34 07026951 297AD254 307553A5


--------------------------

  Update V

    0x03||V is
                                             03A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D A07C4119 A02F9581
        3921B585 58A04F70 836AB353 23E70B14 0F74FA92 38507AD4


    H is
                                             8264A739 7BB8A2B4
        5D09B864 EA8694B4 75668170 5EB44819 680AE7DE AC2CFFE4


  Updated values

  V is
                                               E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A66F 8CA87B87 4350202E
        1D8AB0B5 AD47ACC2 7540289F E3A8E31F 7B5658DD D1969489


  reseed_counter is
                                                 0000 00000002


rnd_val is
                           E0B97C82 1268FD3B B2CABFD1 F9548478
        AE8A6041 7F7B094A 26139546 062B521C FD33E4E3 9B9DCD0A
        3DA15209 C72ADBE5 8C20AB34 07026951 297AD254 307553A5


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 512

  additional_input
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Process additional_input

    0x02||V||additional_input is
                           02E85D D8B1D86C 16BF628B F3B5F997
        044D2A69 138CD6A6 6F8CA87B 87435020 2E1D8AB0 B5AD47AC
        C2754028 9FE3A8E3 1F7B5658 DDD19694 89A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    w=Hash(0x02||V||additional_input) is
                                               A2701C07 02B8A337
        615E949D 0B86D42B 002EF072 58584377 ECBF1094 62AFC8AC


    V is
                                                 E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A670 2F18978E 4608C365
        7EE94552 B8CE80ED 756F1912 3C012697 68156972 34465D35


---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                 E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A670 2F18978E 4608C365
        7EE94552 B8CE80ED 756F1912 3C012697 68156972 34465D35
```

```
    w_i is
                                                C1ACD3AD A4C8C495
        BF179DB5 9822C351 BC479ABE 4EB28F84 3957B11E 3C2BC048


    W is
                                                C1ACD3AD A4C8C495
        BF179DB5 9822C351 BC479ABE 4EB28F84 3957B11E 3C2BC048


    ------------

    i = 2

    data is
                                                  E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A670 2F18978E 4608C365
        7EE94552 B8CE80ED 756F1912 3C012697 68156972 34465D36


    w_i is
                                                83964297 975BD72D
        1024ABCF 6F6615D7 F5B4FD1E 40A64EEB 45BA2181 B83937ED


    W is
                            C1ACD3AD A4C8C495 BF179DB5 9822C351
        BC479ABE 4EB28F84 3957B11E 3C2BC048 83964297 975BD72D
        1024ABCF 6F6615D7 F5B4FD1E 40A64EEB 45BA2181 B83937ED


  returned_bits is
                            C1ACD3AD A4C8C495 BF179DB5 9822C351
        BC479ABE 4EB28F84 3957B11E 3C2BC048 83964297 975BD72D
        1024ABCF 6F6615D7 F5B4FD1E 40A64EEB 45BA2181 B83937ED


--------------------------

  Update V

    0x03||V is
                                                03E85DD8 B1D86C16
        BF628BF3 B5F99704 4D2A6913 8CD6A670 2F18978E 4608C365
```

```
        7EE94552 B8CE80ED 756F1912 3C012697 68156972 34465D35


    H is
                                                19978405 921CF6DE
        6BA76D7F 9F5F14C1 8D7A3AC2 2420B3D0 327F4EFB 9ED0F4C6


  Updated values

  V is
                                                  2CD263 2A89DA8C
        15021411 07BAF502 B97D38C4 48480871 B277AEC7 FF8DA23C
        71EFF59D C24E5E4C 7F5847B0 C12F6A59 9E6B2EDA C0306BCD


  reseed_counter is
                                                    0000 00000003


rnd_val is
                         C1ACD3AD A4C8C495 BF179DB5 9822C351
        BC479ABE 4EB28F84 3957B11E 3C2BC048 83964297 975BD72D
        1024ABCF 6F6615D7 F5B4FD1E 40A64EEB 45BA2181 B83937ED


##############################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                               20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                               20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    no_of_bits_to_return = 440
```

```
  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
              01000001 B8000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Hash(counter||no_of_bits_to_return||input_string) is
                                           AB41CDE4 37AB8B09
      1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


  temp =
                                           AB41CDE4 37AB8B09
      1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
              02000001 B8000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Hash(counter||no_of_bits_to_return||input_string) is
                                           167D84AF 64128C0D
      71F4D5B8 C0EDFBBE 3DF40448 D2D8E12F A91BA8B0 97969506


  temp =
                                             AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
      95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


V is
                                             AB41CD E437AB8B
      091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
      95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              E15DE4A8 E3B1419B
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    temp =
                                              E15DE4A8 E3B1419B
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              CFAAFDDC 90195902
```

```
        E979F79B 65357FEA 85998E4E 37D2C1D4 FD0F0D66 3A829565


    temp =
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


  C is
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                             01AB41 CDE437AB 8B091CA7 C5755D10
```

```
    F0110C1D BD462F22 6CFDABFB B04A8BCD EF95167D 84AF6412
    8C0D71F4 D5B8C0ED FBBE3DF4 0448D2D8 E1808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
             01000001 B801AB41 CDE437AB 8B091CA7 C5755D10
    F0110C1D BD462F22 6CFDABFB B04A8BCD EF95167D 84AF6412
    8C0D71F4 D5B8C0ED FBBE3DF4 0448D2D8 E1808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                        3C40E8DC 7172FDA2
    32550A1D 8E1447C1 1F474888 F96CD85C 3863D5E4 84266756


temp =
                                        3C40E8DC 7172FDA2
    32550A1D 8E1447C1 1F474888 F96CD85C 3863D5E4 84266756


------------

i = 2

counter||no_of_bits_to_return||input_string is
             02000001 B801AB41 CDE437AB 8B091CA7 C5755D10
    F0110C1D BD462F22 6CFDABFB B04A8BCD EF95167D 84AF6412
    8C0D71F4 D5B8C0ED FBBE3DF4 0448D2D8 E1808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                        28D08885 347C3EFD
    6292FDDC D1A1421E ED51B713 AB090FC9 AFC95C22 731A6AF6
```

```
    temp =
                                                3C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


  V is
                                                3C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                               003C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 003C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


    Hash(counter||no_of_bits_to_return||input_string) is
                                               E7568384 F264E4A7
        E7AE850D 9D501FD6 3183564F D7D39044 6F5BE5F6 7B50195B


    temp =
                                               E7568384 F264E4A7
        E7AE850D 9D501FD6 3183564F D7D39044 6F5BE5F6 7B50195B


    ------------
```

```
    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 003C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


    Hash(counter||no_of_bits_to_return||input_string) is
                                              5284692A D4B76DFD
        4F524BCF CCAB62C1 309F2515 17DFFD1F 5C4A6B96 ADC6B9D9


    temp =
                                                E75683 84F264E4
        A7E7AE85 0D9D501F D6318356 4FD7D390 446F5BE5 F67B5019
        5B528469 2AD4B76D FD4F524B CFCCAB62 C1309F25 1517DFFD


  C is
                                                E75683 84F264E4
        A7E7AE85 0D9D501F D6318356 4FD7D390 446F5BE5 F67B5019
        5B528469 2AD4B76D FD4F524B CFCCAB62 C1309F25 1517DFFD


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                3C40E8 DC7172FD
```

```
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


    w_i is
                                              92275523 C70E567B
        CF9B35EC 50B933F8 12616DF5 86B7F72E E1BC7735 A5C26543


    W is
                                              92275523 C70E567B
        CF9B35EC 50B933F8 12616DF5 86B7F72E E1BC7735 A5C26543


    ------------

    i = 2

    data is
                                                3C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB0910


    w_i is
                                              73CBBC72 316DFF84
        20A33BF0 2B97AC8D 1952583F 270ACD70 05CC027F 4CF1187E


    W is
                           92275523 C70E567B CF9B35EC 50B933F8
        12616DF5 86B7F72E E1BC7735 A5C26543 73CBBC72 316DFF84
        20A33BF0 2B97AC8D 1952583F 270ACD70 05CC027F 4CF1187E


  returned_bits is
                           92275523 C70E567B CF9B35EC 50B933F8
        12616DF5 86B7F72E E1BC7735 A5C26543 73CBBC72 316DFF84
        20A33BF0 2B97AC8D 1952583F 270ACD70 05CC027F 4CF1187E


---------------------------

  Update V

    0x03||V is
```

```
                                                033C40E8 DC7172FD
        A232550A 1D8E1447 C11F4748 88F96CD8 5C3863D5 E4842667
        5628D088 85347C3E FD6292FD DCD1A142 1EED51B7 13AB090F


    H is
                                                ECBC627D A003201D
        BD527DAB FCBC42D1 3210EB57 AA2A2E2B D3399828 DF1D4E6A


  Updated values

  V is
                                                  23976C 6163D7E2
        4A1A038F 2B2B6467 9750CA9E D8D14069 8D642239 7B02969E
        6ECDD29D ACC5767E 2CC2D0A1 56C87AD0 B3578905 07E03777


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          92275523 C70E567B CF9B35EC 50B933F8
        12616DF5 86B7F72E E1BC7735 A5C26543 73CBBC72 316DFF84
        20A33BF0 2B97AC8D 1952583F 270ACD70 05CC027F 4CF1187E


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

Generate FAILED: Reseed is required
---------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
```

```
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                           012397 6C6163D7 E24A1A03 8F2B2B64
        679750CA 9ED8D140 698D6422 397B0296 9E6ECDD2 9DACC576
        7E2CC2D0 A156C87A D0B35789 0507E037 77C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B8012397 6C6163D7 E24A1A03 8F2B2B64
        679750CA 9ED8D140 698D6422 397B0296 9E6ECDD2 9DACC576
        7E2CC2D0 A156C87A D0B35789 0507E037 77C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                               E983B166 A92A997E
        ABCC966C 6AA3D3B3 A1681FC5 8F582940 3B48601E C1775494


    temp =
                                               E983B166 A92A997E
        ABCC966C 6AA3D3B3 A1681FC5 8F582940 3B48601E C1775494


    ------------

    i = 2
```

```
    counter||no_of_bits_to_return||input_string is
                02000001 B8012397 6C6163D7 E24A1A03 8F2B2B64
        679750CA 9ED8D140 698D6422 397B0296 9E6ECDD2 9DACC576
        7E2CC2D0 A156C87A D0B35789 0507E037 77C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                            2E11C1CD 465B7DBE
        2A78CA04 2CF9B305 71FF12E3 B9F6C945 C634B91C 1BAC2021


    temp =
                                              E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


  V is
                                              E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                                              A9775CE1 655BFF95
        1BE0AF5B 7959725C 767D86F1 E19B11B8 9004F697 4DBFA046


    temp =
                                              A9775CE1 655BFF95
        1BE0AF5B 7959725C 767D86F1 E19B11B8 9004F697 4DBFA046


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


    Hash(counter||no_of_bits_to_return||input_string) is
                                              04458E5C 528E7E1D
        FAB3887B A4AADBD6 FBDE0B31 6F1D9138 F1EB0DD9 2D80C089


    temp =
                                                A9775C E1655BFF
        951BE0AF 5B795972 5C767D86 F1E19B11 B89004F6 974DBFA0
        4604458E 5C528E7E 1DFAB388 7BA4AADB D6FBDE0B 316F1D91


  C is
                                                A9775C E1655BFF
        951BE0AF 5B795972 5C767D86 F1E19B11 B89004F6 974DBFA0
        4604458E 5C528E7E 1DFAB388 7BA4AADB D6FBDE0B 316F1D91


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


    w_i is
                                               681A46B2 AA8694A0
        FE4DEEA7 20927A84 EAAA985E 59C19F8B E0984D8C BEF8C69B


    W is
                                               681A46B2 AA8694A0
        FE4DEEA7 20927A84 EAAA985E 59C19F8B E0984D8C BEF8C69B


    ------------

    i = 2

    data is
                                                E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6CA


    w_i is
                                               75416764 1946E040
        EE2043E1 CCB29DCF 063C0A50 830E428E 6DCA262E CD77C542


    W is
                           681A46B2 AA8694A0 FE4DEEA7 20927A84
        EAAA985E 59C19F8B E0984D8C BEF8C69B 75416764 1946E040
        EE2043E1 CCB29DCF 063C0A50 830E428E 6DCA262E CD77C542
```

```
  returned_bits is
                          681A46B2 AA8694A0 FE4DEEA7 20927A84
        EAAA985E 59C19F8B E0984D8C BEF8C69B 75416764 1946E040
        EE2043E1 CCB29DCF 063C0A50 830E428E 6DCA262E CD77C542


---------------------------

  Update V

    0x03||V is
                                               03E983B1 66A92A99
        7EABCC96 6C6AA3D3 B3A1681F C58F5829 403B4860 1EC17754
        942E11C1 CD465B7D BE2A78CA 042CF9B3 0571FF12 E3B9F6C9


    H is
                                               3870EB2D 3BBD1F7C
        AF12CAA5 C44D44AE D45E84EF 2789B831 45F27D6C 289E074C


  Updated values

  V is
                                                 92FB0E 480E8699
        13C7AD45 C7E3FD46 1017E5A6 B770F33B 313C3883 F1CC5671
        894521F5 EDE62EAA B083B141 A75B5CC0 22605A8A 3DC71BA7


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          681A46B2 AA8694A0 FE4DEEA7 20927A84
        EAAA985E 59C19F8B E0984D8C BEF8C69B 75416764 1946E040
        EE2043E1 CCB29DCF 063C0A50 830E428E 6DCA262E CD77C542


##############################################################

Hash_DRBG

    Requested Security Strength = 128
```

```
    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                               20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                 606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                              20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                 01000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                              AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95


    temp =
                                              AB41CDE4 37AB8B09
        1CA7C575 5D10F011 0C1DBD46 2F226CFD ABFBB04A 8BCDEF95
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                02000001 B8000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                              167D84AF 64128C0D
        71F4D5B8 C0EDFBBE 3DF40448 D2D8E12F A91BA8B0 97969506


    temp =
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


  V is
                                                AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
```

```
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              E15DE4A8 E3B1419B
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    temp =
                                              E15DE4A8 E3B1419B
        61D534F1 5DBD31EE 19EC595F 8B98111A 94F52237 AD5D66F0


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00AB41CD E437AB8B
        091CA7C5 755D10F0 110C1DBD 462F226C FDABFBB0 4A8BCDEF
        95167D84 AF64128C 0D71F4D5 B8C0EDFB BE3DF404 48D2D8E1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              CFAAFDDC 90195902
        E979F79B 65357FEA 85998E4E 37D2C1D4 FD0F0D66 3A829565


    temp =
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


  C is
                                                E15DE4 A8E3B141
        9B61D534 F15DBD31 EE19EC59 5F8B9811 1A94F522 37AD5D66
        F0CFAAFD DC901959 02E979F7 9B65357F EA85998E 4E37D2C1


----------------------------------------------------------------

First call to Generate

****************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01AB 41CDE437 AB8B091C A7C5755D 10F0110C 1DBD462F
        226CFDAB FBB04A8B CDEF9516 7D84AF64 128C0D71 F4D5B8C0
        EDFBBE3D F40448D2 D8E18081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    no_of_bits_to_return = 440

    ------------

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
                                                          010000
    01B801AB 41CDE437 AB8B091C A7C5755D 10F0110C 1DBD462F
    226CFDAB FBB04A8B CDEF9516 7D84AF64 128C0D71 F4D5B8C0
    EDFBBE3D F40448D2 D8E18081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                          57B2CF00 B5429746
    0B087E52 75D7DD74 23B6E3B6 5E3516D2 481199A0 17B53A22


temp =
                                          57B2CF00 B5429746
    0B087E52 75D7DD74 23B6E3B6 5E3516D2 481199A0 17B53A22


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                          020000
    01B801AB 41CDE437 AB8B091C A7C5755D 10F0110C 1DBD462F
    226CFDAB FBB04A8B CDEF9516 7D84AF64 128C0D71 F4D5B8C0
    EDFBBE3D F40448D2 D8E18081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                          2033FE68 A60BD0BD
    704026CD 5A3E7955 DB01DCB2 8448D1B1 21D18F19 55FEA723


temp =
                                            57B2CF 00B54297
    460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
    222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1
```

```
  V is
                                                  57B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                0057B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 0057B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1


    Hash(counter||no_of_bits_to_return||input_string) is
                                                5BC1C645 CC8D3215
        82AFBB00 16992B0F 3AFE0F54 7AE7A74C 9C05A144 02FBB1D5


    temp =
                                                5BC1C645 CC8D3215
        82AFBB00 16992B0F 3AFE0F54 7AE7A74C 9C05A144 02FBB1D5


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 0057B2CF 00B54297
```

```
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1


    Hash(counter||no_of_bits_to_return||input_string) is
                                              40E6809D 8BEEF599
        ED4C3916 4740EDA0 D9C3795D E552C5DF 0AC1CAC6 AE8C0116


    temp =
                                                5BC1C6 45CC8D32
        1582AFBB 0016992B 0F3AFE0F 547AE7A7 4C9C05A1 4402FBB1
        D540E680 9D8BEEF5 99ED4C39 164740ED A0D9C379 5DE552C5


  C is
                                                5BC1C6 45CC8D32
        1582AFBB 0016992B 0F3AFE0F 547AE7A7 4C9C05A1 4402FBB1
        D540E680 9D8BEEF5 99ED4C39 164740ED A0D9C379 5DE552C5


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                57B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1


    w_i is
```

```
                                              11601B72 CA608973
        6B204744 B29DA1AA AFBACAA5 288F06BE 484569CC EDBECE03


    W is
                                              11601B72 CA608973
        6B204744 B29DA1AA AFBACAA5 288F06BE 484569CC EDBECE03


    ------------

    i = 2

    data is
                                                57B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D2


    w_i is
                                              E822EAA5 B14F0E04
        948C05CD 3CC2E288 9A89FA03 D65D4D74 AC50FF6B D856E579


    W is
                           11601B72 CA608973 6B204744 B29DA1AA
        AFBACAA5 288F06BE 484569CC EDBECE03 E822EAA5 B14F0E04
        948C05CD 3CC2E288 9A89FA03 D65D4D74 AC50FF6B D856E579


  returned_bits is
                           11601B72 CA608973 6B204744 B29DA1AA
        AFBACAA5 288F06BE 484569CC EDBECE03 E822EAA5 B14F0E04
        948C05CD 3CC2E288 9A89FA03 D65D4D74 AC50FF6B D856E579


--------------------------

  Update V

    0x03||V is
                                              0357B2CF 00B54297
        460B087E 5275D7DD 7423B6E3 B65E3516 D2481199 A017B53A
        222033FE 68A60BD0 BD704026 CD5A3E79 55DB01DC B28448D1
```

```
    H is
                                                7FBCBE0A E8E26727
        3390B8F7 891507B0 D40B893F 491EFFE1 7D69F05C A0B8758E


  Updated values

  V is
                                                  B37495 4681CFC9
        5B8DB839 528C7108 835EB4F3 0AD91CBE 9EA0D545 CCFD1813
        2AF1D376 8F470277 2B69159F 2CC07F48 741EB5B2 B1221125


  reseed_counter is
                                                     0000 00000002


rnd_val is
                          11601B72 CA608973 6B204744 B29DA1AA
        AFBACAA5 288F06BE 484569CC EDBECE03 E822EAA5 B14F0E04
        948C05CD 3CC2E288 9A89FA03 D65D4D74 AC50FF6B D856E579


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  C0C1C2 C3C4C5C6
```

```
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01B3 74954681 CFC95B8D B839528C 7108835E B4F30AD9
        1CBE9EA0 D545CCFD 18132AF1 D3768F47 02772B69 159F2CC0
        7F48741E B5B2B122 1125C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                      010000
        01B801B3 74954681 CFC95B8D B839528C 7108835E B4F30AD9
        1CBE9EA0 D545CCFD 18132AF1 D3768F47 02772B69 159F2CC0
        7F48741E B5B2B122 1125C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                             5DC1C5F4 B41150CE
        E0EFC129 B837B31C 84D791FF 2E7EDAC2 9C2C50CF 8A40709B
```

```
    temp =
                                                5DC1C5F4 B41150CE
        E0EFC129 B837B31C 84D791FF 2E7EDAC2 9C2C50CF 8A40709B


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                          020000
        01B801B3 74954681 CFC95B8D B839528C 7108835E B4F30AD9
        1CBE9EA0 D545CCFD 18132AF1 D3768F47 02772B69 159F2CC0
        7F48741E B5B2B122 1125C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    Hash(counter||no_of_bits_to_return||input_string) is
                                                98640F7B BD32BCF0
        FCB613F9 6D55D160 56BB3CA6 A774059D EC8C65C6 853BDEFE


    temp =
                                                  5DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


  V is
                                                  5DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                005DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405
```

```
  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 005DC1C5 F4B41150
      CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
      9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


  Hash(counter||no_of_bits_to_return||input_string) is
                                          6222108C EDFE6D6A
      229F8C3C BF4468C8 F5172286 4CC416A4 2926D99B A6F045C1


  temp =
                                          6222108C EDFE6D6A
      229F8C3C BF4468C8 F5172286 4CC416A4 2926D99B A6F045C1


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 005DC1C5 F4B41150
      CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
      9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


  Hash(counter||no_of_bits_to_return||input_string) is
                                          F6211156 946C6E79
      3729974E B4C5A607 8F9A1D4D 1CD749DE FE72459A 097C1198


  temp =
                                            622210 8CEDFE6D
      6A229F8C 3CBF4468 C8F51722 864CC416 A42926D9 9BA6F045
      C1F62111 56946C6E 79372997 4EB4C5A6 078F9A1D 4D1CD749


C is
                                            622210 8CEDFE6D
```

```
        6A229F8C 3CBF4468 C8F51722 864CC416 A42926D9 9BA6F045
        C1F62111 56946C6E 79372997 4EB4C5A6 078F9A1D 4D1CD749


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                 5DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


    w_i is
                                               055BC128 CC2D0E25
        0F47E4E4 F582375D E3EE5E9F E8316874 97E5AF1E 7CB69EFD


    W is
                                               055BC128 CC2D0E25
        0F47E4E4 F582375D E3EE5E9F E8316874 97E5AF1E 7CB69EFD


    ------------

    i = 2

    data is
                                                 5DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77406
```

```
    w_i is
                                                EBD2FD31 C7CE2BBA
        0DBC6C74 C8A20A7D 72F60E6D 9F63ED50 9E963E54 A69E9048


    W is
                           055BC128 CC2D0E25 0F47E4E4 F582375D
        E3EE5E9F E8316874 97E5AF1E 7CB69EFD EBD2FD31 C7CE2BBA
        0DBC6C74 C8A20A7D 72F60E6D 9F63ED50 9E963E54 A69E9048


  returned_bits is
                           055BC128 CC2D0E25 0F47E4E4 F582375D
        E3EE5E9F E8316874 97E5AF1E 7CB69EFD EBD2FD31 C7CE2BBA
        0DBC6C74 C8A20A7D 72F60E6D 9F63ED50 9E963E54 A69E9048


----------------------------

  Update V

    0x03||V is
                                                035DC1C5 F4B41150
        CEE0EFC1 29B837B3 1C84D791 FF2E7EDA C29C2C50 CF8A4070
        9B98640F 7BBD32BC F0FCB613 F96D55D1 6056BB3C A6A77405


    H is
                                                B57A0660 EE3186F3
        EA802045 2C991ED0 6C740D20 4DE0A5D4 924A9B9F 8DCBC181


  Updated values

  V is
                                                  BFE3D6 81A20FBE
        39038F4D 66777C1B E579EEB4 857B42F2 1C3F598B 5962B7AA
        480EA565 FEEABDFB D6A7ECCB 9602C14B FA30F0F9 81900CD0


  reseed_counter is
                                                    0000 00000002
```

```
rnd_val is
                          055BC128 CC2D0E25 0F47E4E4 F582375D
        E3EE5E9F E8316874 97E5AF1E 7CB69EFD EBD2FD31 C7CE2BBA
        0DBC6C74 C8A20A7D 72F60E6D 9F63ED50 9E963E54 A69E9048


##############################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                               20212223 24252627


    PersonalizationString =
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

##############################################################
```

```
************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                               20212223 24252627


    personal_str is
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                       010000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
```

```
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                              A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    temp =
                                              A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                        020000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                              71564B45 6FF2EEC8
        36422ACC 5A029935 A7992990 94A1CA74 1B916DC0 26A7E107


    temp =
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  V is
                                                A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


--------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                                          00A3E94E 3926FDA1
      69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
      B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  no_of_bits_to_return = 440

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 000001B8 00A3E94E 3926FDA1
      69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
      B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  Hash(counter||no_of_bits_to_return||input_string) is
                                          44748A78 B16E7555
      9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


  temp =
                                          44748A78 B16E7555
      9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 000001B8 00A3E94E 3926FDA1
      69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
      B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  Hash(counter||no_of_bits_to_return||input_string) is
                                          5F42CB6A 20C89D7C
      6EF3DC61 0D8FF203 D6766CED 1919D094 ED485EF7 FADDB668


  temp =
```

```
                                                  44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


  C is
                                                  44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input <empty>

--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            01A3E9 4E3926FD A169C303 D6643839
        05E0D799 62D16544 6D63BDA6 54D132F7 2DB47156 4B456FF2
        EEC83642 2ACC5A02 9935A799 299094A1 CA808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
             01000001 B801A3E9 4E3926FD A169C303 D6643839
    05E0D799 62D16544 6D63BDA6 54D132F7 2DB47156 4B456FF2
    EEC83642 2ACC5A02 9935A799 299094A1 CA808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                        E026A5C2 E7623E62
    B71A2E04 C25F0B08 582BE216 3634C049 6D2B65DA 7EAA03B5


temp =
                                        E026A5C2 E7623E62
    B71A2E04 C25F0B08 582BE216 3634C049 6D2B65DA 7EAA03B5


------------

i = 2

counter||no_of_bits_to_return||input_string is
             02000001 B801A3E9 4E3926FD A169C303 D6643839
    05E0D799 62D16544 6D63BDA6 54D132F7 2DB47156 4B456FF2
    EEC83642 2ACC5A02 9935A799 299094A1 CA808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


Hash(counter||no_of_bits_to_return||input_string) is
                                        C3B6B510 BB3FE474
    34071F70 7AC7FE4C 396AAAEE 764C9068 F3A21A46 411C15BB


temp =
                                          E026A5 C2E7623E
    62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
```

```
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90


  V is
                                                E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90


    Hash(counter||no_of_bits_to_return||input_string) is
                                              C9EA754B EE0AB644
        15CA7FE3 2EBBFB07 ED932E7C 957ECEAE F0CD2FA7 7A46F9E8


    temp =
                                              C9EA754B EE0AB644
        15CA7FE3 2EBBFB07 ED932E7C 957ECEAE F0CD2FA7 7A46F9E8


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
```

```
                              02 000001B8 00E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90


    Hash(counter||no_of_bits_to_return||input_string) is
                                             59627897 54C6D298
        F9B5E459 6B4E0E6D F4F4B823 60DA3388 F6702DBF 2836D573


    temp =
                                               C9EA75 4BEE0AB6
        4415CA7F E32EBBFB 07ED932E 7C957ECE AEF0CD2F A77A46F9
        E8596278 9754C6D2 98F9B5E4 596B4E0E 6DF4F4B8 2360DA33


  C is
                                               C9EA75 4BEE0AB6
        4415CA7F E32EBBFB 07ED932E 7C957ECE AEF0CD2F A77A46F9
        E8596278 9754C6D2 98F9B5E4 596B4E0E 6DF4F4B8 2360DA33


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                               E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90
```

```
    w_i is
                                                7A33D390 33F86058
        9F375E73 35307552 9658BBED 99C8A0EF 5E28B351 B2DF3358


    W is
                                                7A33D390 33F86058
        9F375E73 35307552 9658BBED 99C8A0EF 5E28B351 B2DF3358


    ------------

    i = 2

    data is
                                                  E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C91


    w_i is
                                                B3D89BAC 7225DF9E
        3BCD0836 B99B5DBF 363A170C 7BB9BE41 A4AA9744 5ECEE41E


    W is
                            7A33D390 33F86058 9F375E73 35307552
        9658BBED 99C8A0EF 5E28B351 B2DF3358 B3D89BAC 7225DF9E
        3BCD0836 B99B5DBF 363A170C 7BB9BE41 A4AA9744 5ECEE41E


  returned_bits is
                            7A33D390 33F86058 9F375E73 35307552
        9658BBED 99C8A0EF 5E28B351 B2DF3358 B3D89BAC 7225DF9E
        3BCD0836 B99B5DBF 363A170C 7BB9BE41 A4AA9744 5ECEE41E


---------------------------

  Update V

    0x03||V is
                                                03E026A5 C2E7623E
        62B71A2E 04C25F0B 08582BE2 163634C0 496D2B65 DA7EAA03
        B5C3B6B5 10BB3FE4 7434071F 707AC7FE 4C396AAA EE764C90
```

```
    H is
                                                FAC59D54 E0D97A2A
        2A697018 1D83B3B9 B656F0A9 7B910686 F66DC805 F57BAB14


  Updated values

  V is
                                                  AA111B 0ED56CF4
        A6CCE4AD E7F11B06 1045BF10 92CBB38F F32395EA 62D26B27
        C8868945 C593BA70 C384ADAD 45771C93 B09C2769 0752D1D8


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          7A33D390 33F86058 9F375E73 35307552
        9658BBED 99C8A0EF 5E28B351 B2DF3358 B3D89BAC 7225DF9E
        3BCD0836 B99B5DBF 363A170C 7BB9BE41 A4AA9744 5ECEE41E


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                            01AA11 1B0ED56C F4A6CCE4 ADE7F11B
        061045BF 1092CBB3 8FF32395 EA62D26B 27C88689 45C593BA
        70C384AD AD45771C 93B09C27 690752D1 D8C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                01000001 B801AA11 1B0ED56C F4A6CCE4 ADE7F11B
        061045BF 1092CBB3 8FF32395 EA62D26B 27C88689 45C593BA
        70C384AD AD45771C 93B09C27 690752D1 D8C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                            FC5F5648 EDC4FC30
        7B5C5A53 D51289B5 0E73DCEC 4AA1CB47 A3BAD846 BB57C3C4


    temp =
                                            FC5F5648 EDC4FC30
        7B5C5A53 D51289B5 0E73DCEC 4AA1CB47 A3BAD846 BB57C3C4


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                02000001 B801AA11 1B0ED56C F4A6CCE4 ADE7F11B
        061045BF 1092CBB3 8FF32395 EA62D26B 27C88689 45C593BA
```

```
        70C384AD AD45771C 93B09C27 690752D1 D8C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Hash(counter||no_of_bits_to_return||input_string) is
                                              80491DF5 21C4669B
        FFF37A41 8BAF6E9B EAEC3496 D0F1A6DC 3210CCA3 071DD6B7


    temp =
                                                FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


  V is
                                                FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                              00FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 00FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


    Hash(counter||no_of_bits_to_return||input_string) is
                                              62B07DC3 9EBDF310
```

```
        87B85DDC ECFD4335 62E53BAE 9F721C5A FAB8F1CF 0161C88E


    temp =
                                              62B07DC3 9EBDF310
        87B85DDC ECFD4335 62E53BAE 9F721C5A FAB8F1CF 0161C88E


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 00FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


    Hash(counter||no_of_bits_to_return||input_string) is
                                              45503E15 B26E7B80
        D51DB0B9 2452362D C3DC570D FE6E1721 DB2A72BA 67BAE5E5


    temp =
                                                62B07D C39EBDF3
        1087B85D DCECFD43 3562E53B AE9F721C 5AFAB8F1 CF0161C8
        8E45503E 15B26E7B 80D51DB0 B9245236 2DC3DC57 0DFE6E17


  C is
                                                62B07D C39EBDF3
        1087B85D DCECFD43 3562E53B AE9F721C 5AFAB8F1 CF0161C8
        8E45503E 15B26E7B 80D51DB0 B9245236 2DC3DC57 0DFE6E17


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen
```

```
  requested_no_of_bits  = 512

  ------------

  i = 1

  data is
                                              FC5F56 48EDC4FC
      307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
      C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


  w_i is
                                            041ABD94 079A0571
      885F1665 944E0E7F 1BFACDEA EAE9D44E EDC11FAD D84C34C7


  W is
                                            041ABD94 079A0571
      885F1665 944E0E7F 1BFACDEA EAE9D44E EDC11FAD D84C34C7


  ------------

  i = 2

  data is
                                              FC5F56 48EDC4FC
      307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
      C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A7


  w_i is
                                            CAA73D09 A0193193
      FA40A19F 644F048D 2A541704 2553DF52 51741B40 EACFEB98


  W is
                        041ABD94 079A0571 885F1665 944E0E7F
      1BFACDEA EAE9D44E EDC11FAD D84C34C7 CAA73D09 A0193193
      FA40A19F 644F048D 2A541704 2553DF52 51741B40 EACFEB98


returned_bits is
                        041ABD94 079A0571 885F1665 944E0E7F
```

```
        1BFACDEA EAE9D44E EDC11FAD D84C34C7 CAA73D09 A0193193
        FA40A19F 644F048D 2A541704 2553DF52 51741B40 EACFEB98


---------------------------

  Update V

    0x03||V is
                                            03FC5F56 48EDC4FC
        307B5C5A 53D51289 B50E73DC EC4AA1CB 47A3BAD8 46BB57C3
        C480491D F521C466 9BFFF37A 418BAF6E 9BEAEC34 96D0F1A6


    H is
                                            A5D6F49E 03109586
        67190F26 4D427131 85C06133 B88E3214 E4501826 1D64AB22


  Updated values

  V is
                                              5F0FD4 0C8C82EF
        410314B8 30C20FCC EA715918 9AEA13E8 48756868 18CD4F12
        B9DEA882 5816A413 A295725E B33E33B9 ADFEE0B1 C2340AE0


  reseed_counter is
                                                0000 00000002


rnd_val is
                         041ABD94 079A0571 885F1665 944E0E7F
        1BFACDEA EAE9D44E EDC11FAD D84C34C7 CAA73D09 A0193193
        FA40A19F 644F048D 2A541704 2553DF52 51741B40 EACFEB98


################################################################

Hash_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
```

```
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                              20212223 24252627


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    temp =
                                                A3E94E39 26FDA169
        C303D664 383905E0 D79962D1 65446D63 BDA654D1 32F72DB4


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                              020000
        01B80001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    Hash(counter||no_of_bits_to_return||input_string) is
                                                71564B45 6FF2EEC8
        36422ACC 5A029935 A7992990 94A1CA74 1B916DC0 26A7E107


    temp =
                                                  A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


  V is
                                                  A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
        B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                00A3E94E 3926FDA1
        69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
```

```
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                            01 000001B8 00A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


Hash(counter||no_of_bits_to_return||input_string) is
                                        44748A78 B16E7555
    9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


temp =
                                        44748A78 B16E7555
    9F881D51 C15DFE6C 52CFB0BB 71620169 C7933427 67E7F887


------------

i = 2

counter||no_of_bits_to_return||input_string is
                            02 000001B8 00A3E94E 3926FDA1
    69C303D6 64383905 E0D79962 D165446D 63BDA654 D132F72D
    B471564B 456FF2EE C836422A CC5A0299 35A79929 9094A1CA


Hash(counter||no_of_bits_to_return||input_string) is
                                        5F42CB6A 20C89D7C
    6EF3DC61 0D8FF203 D6766CED 1919D094 ED485EF7 FADDB668


temp =
                                          44748A 78B16E75
    559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
    875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0
```

```
  C is
                                                  44748A 78B16E75
        559F881D 51C15DFE 6C52CFB0 BB716201 69C79334 2767E7F8
        875F42CB 6A20C89D 7C6EF3DC 610D8FF2 03D6766C ED1919D0


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  additional_input
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01A3 E94E3926 FDA169C3 03D66438 3905E0D7 9962D165
        446D63BD A654D132 F72DB471 564B456F F2EEC836 422ACC5A
```

```
    029935A7 99299094 A1CA8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


no_of_bits_to_return = 440

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    01B801A3 E94E3926 FDA169C3 03D66438 3905E0D7 9962D165
    446D63BD A654D132 F72DB471 564B456F F2EEC836 422ACC5A
    029935A7 99299094 A1CA8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Hash(counter||no_of_bits_to_return||input_string) is
                                          9875BB7C 7A0B236B
    F46F4EA6 6F67C7B4 4F80EF70 614BEFE8 B085CCAF 5589A76F


temp =
                                          9875BB7C 7A0B236B
    F46F4EA6 6F67C7B4 4F80EF70 614BEFE8 B085CCAF 5589A76F


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    01B801A3 E94E3926 FDA169C3 03D66438 3905E0D7 9962D165
    446D63BD A654D132 F72DB471 564B456F F2EEC836 422ACC5A
    029935A7 99299094 A1CA8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    Hash(counter||no_of_bits_to_return||input_string) is
                                                85FD9669 53E20A55
        D2F35BA5 81EF5111 BFBF0565 3AF7E73F 13E35ACD 3D548B70


    temp =
                                                  9875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


  V is
                                                  9875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                                009875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 000001B8 009875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


    Hash(counter||no_of_bits_to_return||input_string) is
                                                1280FE1F 05798CCA
        ED5D6DF6 E7D26F04 6E538CC5 2A6A030D A826B2B4 7982D6EE
```

```
    temp =
                                                1280FE1F 05798CCA
        ED5D6DF6 E7D26F04 6E538CC5 2A6A030D A826B2B4 7982D6EE


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 000001B8 009875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


    Hash(counter||no_of_bits_to_return||input_string) is
                                                8A686758 0706939E
        CC03FC11 B0059FE2 AEADEA0A 46985C64 0E0BF8E2 C4A6A026


    temp =
                                                  1280FE 1F05798C
        CAED5D6D F6E7D26F 046E538C C52A6A03 0DA826B2 B47982D6
        EE8A6867 58070693 9ECC03FC 11B0059F E2AEADEA 0A46985C


  C is
                                                  1280FE 1F05798C
        CAED5D6D F6E7D26F 046E538C C52A6A03 0DA826B2 B47982D6
        EE8A6867 58070693 9ECC03FC 11B0059F E2AEADEA 0A46985C


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512
```

```
  ------------

  i = 1

  data is
                                                 9875BB 7C7A0B23
      6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
      6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


  w_i is
                                               88973297 5B36E8E2
      E7B74050 AEA17139 DA2B8634 DCE2133B 0634743F 477557AB


  W is
                                               88973297 5B36E8E2
      E7B74050 AEA17139 DA2B8634 DCE2133B 0634743F 477557AB


  ------------

  i = 2

  data is
                                                 9875BB 7C7A0B23
      6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
      6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E8


  w_i is
                                               7B844ED3 F2A46CC6
      3EB23286 464C51D5 D76971C4 7BC5B55F ED72A804 3CBF664F


  W is
                         88973297 5B36E8E2 E7B74050 AEA17139
      DA2B8634 DCE2133B 0634743F 477557AB 7B844ED3 F2A46CC6
      3EB23286 464C51D5 D76971C4 7BC5B55F ED72A804 3CBF664F


returned_bits is
                         88973297 5B36E8E2 E7B74050 AEA17139
      DA2B8634 DCE2133B 0634743F 477557AB 7B844ED3 F2A46CC6
      3EB23286 464C51D5 D76971C4 7BC5B55F ED72A804 3CBF664F
```

```
---------------------------

  Update V

    0x03||V is
                                                039875BB 7C7A0B23
        6BF46F4E A66F67C7 B44F80EF 70614BEF E8B085CC AF5589A7
        6F85FD96 6953E20A 55D2F35B A581EF51 11BFBF05 653AF7E7


    H is
                                                CB7E3B10 D6DB1D73
        6A6A8068 F72BAB20 FFCD5A6A 9515CA0D 56C7085E 5C788E39


  Updated values

  V is
                                                  AAF6B9 9B7F84B0
        36E1CCBC 9D573A36 B8BDD47C 358BB5F3 C1D6E790 3AAA29F1
        C87AE666 B88693BE F46C51C2 4C47BEFE 4B35754D CBFA1E7D


  reseed_counter is
                                                    0000 00000002


rnd_val is
                          88973297 5B36E8E2 E7B74050 AEA17139
        DA2B8634 DCE2133B 0634743F 477557AB 7B844ED3 F2A46CC6
        3EB23286 464C51D5 D76971C4 7BC5B55F ED72A804 3CBF664F


-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input
```

```
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  additional_input
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01AA F6B99B7F 84B036E1 CCBC9D57 3A36B8BD D47C358B
        B5F3C1D6 E7903AAA 29F1C87A E666B886 93BEF46C 51C24C47
        BEFE4B35 754DCBFA 1E7DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        01B801AA F6B99B7F 84B036E1 CCBC9D57 3A36B8BD D47C358B
        B5F3C1D6 E7903AAA 29F1C87A E666B886 93BEF46C 51C24C47
```

```
    BEFE4B35 754DCBFA 1E7DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Hash(counter||no_of_bits_to_return||input_string) is
                                          B06DBFB1 4E7F4E01
    2562942F E4F2A960 1707559D 7DD19089 8BC80624 E5C8C1BB


  temp =
                                          B06DBFB1 4E7F4E01
    2562942F E4F2A960 1707559D 7DD19089 8BC80624 E5C8C1BB


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                    020000
    01B801AA F6B99B7F 84B036E1 CCBC9D57 3A36B8BD D47C358B
    B5F3C1D6 E7903AAA 29F1C87A E666B886 93BEF46C 51C24C47
    BEFE4B35 754DCBFA 1E7DC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Hash(counter||no_of_bits_to_return||input_string) is
                                          9B90FB2E EF12ED24
    BEBD8DF7 1EF65C70 FA4E9186 3A31BE73 7AF120FF 4E66AD23


  temp =
                                            B06DBF B14E7F4E
    01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
    BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


V is
                                            B06DBF B14E7F4E
    01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
```

```
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                                            00B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


    no_of_bits_to_return = 440

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                               01 000001B8 00B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


    Hash(counter||no_of_bits_to_return||input_string) is
                                            5C07B79C 12831BAC
        3652178B 2F907A69 619839D8 A7FAA2B6 95EFB310 82380135


    temp =
                                            5C07B79C 12831BAC
        3652178B 2F907A69 619839D8 A7FAA2B6 95EFB310 82380135


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                               02 000001B8 00B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                                85191F59 9C9907C7
        2192ED25 7E9F6CD3 77DD6BAC 337C19E4 9348D426 B2A13C96


    temp =
                                                  5C07B7 9C12831B
        AC365217 8B2F907A 69619839 D8A7FAA2 B695EFB3 10823801
        3585191F 599C9907 C72192ED 257E9F6C D377DD6B AC337C19


  C is
                                                  5C07B7 9C12831B
        AC365217 8B2F907A 69619839 D8A7FAA2 B695EFB3 10823801
        3585191F 599C9907 C72192ED 257E9F6C D377DD6B AC337C19


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 512

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 512

    ------------

    i = 1

    data is
                                                  B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


    w_i is
                                                BF49B889 BA984D34
        6387E864 7E98BB99 CD41A32F BEC1FCB3 B6A1B7D9 932BA7E1


    W is
```

```
                                                BF49B889 BA984D34
        6387E864 7E98BB99 CD41A32F BEC1FCB3 B6A1B7D9 932BA7E1


    ------------

    i = 2

    data is
                                                  B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BF


    w_i is
                                                1EE6BBD9 24405A2C
        7FCA890A 5E9A8DEA 66AC0CAC A0CA7BC1 8D74FBC0 2A11E453


    W is
                            BF49B889 BA984D34 6387E864 7E98BB99
        CD41A32F BEC1FCB3 B6A1B7D9 932BA7E1 1EE6BBD9 24405A2C
        7FCA890A 5E9A8DEA 66AC0CAC A0CA7BC1 8D74FBC0 2A11E453


  returned_bits is
                            BF49B889 BA984D34 6387E864 7E98BB99
        CD41A32F BEC1FCB3 B6A1B7D9 932BA7E1 1EE6BBD9 24405A2C
        7FCA890A 5E9A8DEA 66AC0CAC A0CA7BC1 8D74FBC0 2A11E453


--------------------------

  Update V

    0x03||V is
                                                03B06DBF B14E7F4E
        01256294 2FE4F2A9 60170755 9D7DD190 898BC806 24E5C8C1
        BB9B90FB 2EEF12ED 24BEBD8D F71EF65C 70FA4E91 863A31BE


    H is
                                                F35A4B8D F8320B8C
        BB1014B8 5552B8C3 8E4C1FEC 362484F6 CCB5175B F9E2318F
```

Updated values

V is

0C7577 4D610269
AD5BB4AB BB148323 C9789F8F 7625CC34 337C0347 2D9A0C4F
AC30BED2 DDDE64B8 7A2C7067 52C21AC0 11274359 2C4FDF67

reseed_counter is

0000 00000002

rnd_val is

BF49B889 BA984D34 6387E864 7E98BB99
CD41A32F BEC1FCB3 B6A1B7D9 932BA7E1 1EE6BBD9 24405A2C
7FCA890A 5E9A8DEA 66AC0CAC A0CA7BC1 8D74FBC0 2A11E453

```
###############################################################

Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                   20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

----------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                               01000003 78000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                        02000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
    E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4
    31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
    E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                        03000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        9B71197A 30150000 F1E5B6AD 1EB81AB2 7B8E19BE 185E4F70
        61F1D3CA 9B3A0DF4 FD597962 C2070B7E B064B31F 4F3E10BD


    temp =
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  V is
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


Hash(counter||no_of_bits_to_return||input_string) is
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        55F0BF84 2C6BF212 18612101 CB0E1A06 0E2E9C66 5E87E1BA
        9632F01B 4CF80D08 C9645BD1 830112EA 6EBFED69 A48CA9C9


    temp =
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


  C is
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
```

```
                          703AEC B83762E8 855BF167 2A52FAEF
      5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
      FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
      DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
      AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  w_i is
      04FF23AD 15E78790 ADD36B43 8BBC097C 7A11747C C2CCEEDE
      2C978B23 B3DC63B7 32C95306 1D776499 0ABFEFC4 7A581B92


  W is
      04FF23AD 15E78790 ADD36B43 8BBC097C 7A11747C C2CCEEDE
      2C978B23 B3DC63B7 32C95306 1D776499 0ABFEFC4 7A581B92


  ------------

  i = 2

  data is
                          703AEC B83762E8 855BF167 2A52FAEF
      5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
      FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
      DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
      AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81B


  w_i is
      1BC0428C 4F122124 60E406A0 F0651E7F 0CB9A90A BFDB07B5
      25565C74 F0AA0850 82F6CF21 3AAFAD0C 06468950 78F1E1FE


  W is
      04FF23AD 15E78790 ADD36B43 8BBC097C 7A11747C C2CCEEDE
      2C978B23 B3DC63B7 32C95306 1D776499 0ABFEFC4 7A581B92
      1BC0428C 4F122124 60E406A0 F0651E7F 0CB9A90A BFDB07B5
      25565C74 F0AA0850 82F6CF21 3AAFAD0C 06468950 78F1E1FE


returned_bits is
      04FF23AD 15E78790 ADD36B43 8BBC097C 7A11747C C2CCEEDE
      2C978B23 B3DC63B7 32C95306 1D776499 0ABFEFC4 7A581B92
      1BC0428C 4F122124 60E406A0 F0651E7F 0CB9A90A BFDB07B5
      25565C74 F0AA0850 82F6CF21 3AAFAD0C 06468950 78F1E1FE
```

```
---------------------------

  Update V

    0x03||V is
                           03703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    H is
        DAFD91E4 4FB509DF 5AFC7DA7 9B82820D 28A7153C C258E03A
        2400E763 3648DD95 B68BF28C 7DC37D68 854DADDB BB1A3D54


  Updated values

  V is
                             F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F48E
        5825A9C5 D61BA51D A06B3B90 4B20C712 D51713AE 30EC1137
        C244277E F8C53DE9 0A7D5465 7C1FFE5A 9857F4B3 6A040389


  reseed_counter is
                                                 0000 00000002


rnd_val is
        04FF23AD 15E78790 ADD36B43 8BBC097C 7A11747C C2CCEEDE
        2C978B23 B3DC63B7 32C95306 1D776499 0ABFEFC4 7A581B92
        1BC0428C 4F122124 60E406A0 F0651E7F 0CB9A90A BFDB07B5
        25565C74 F0AA0850 82F6CF21 3AAFAD0C 06468950 78F1E1FE


---------------------------------------------------------------

Second call to Generate

***************************************************************
```

```
Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                           F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F48E
        5825A9C5 D61BA51D A06B3B90 4B20C712 D51713AE 30EC1137
        C244277E F8C53DE9 0A7D5465 7C1FFE5A 9857F4B3 6A040389


    w_i is
        4F35B85F 95DEE3E8 73054905 CFD02341 653E18F5 29930CBE
        14D909F3 7FEAF2C7 90D22FAE 7516B459 0BE35D53 E2FE1A35


    W is
        4F35B85F 95DEE3E8 73054905 CFD02341 653E18F5 29930CBE
        14D909F3 7FEAF2C7 90D22FAE 7516B459 0BE35D53 E2FE1A35


    ------------

    i = 2

    data is
                           F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F48E
        5825A9C5 D61BA51D A06B3B90 4B20C712 D51713AE 30EC1137
        C244277E F8C53DE9 0A7D5465 7C1FFE5A 9857F4B3 6A04038A
```

```
    w_i is
        AFE4B660 7CB35858 9C3B4D09 4A1D81FE 0717F1DF 5BDDEB3E
        114F130B B781E66C 22B5B770 E8AE115F F39F8ADA F66DEEDF


    W is
        4F35B85F 95DEE3E8 73054905 CFD02341 653E18F5 29930CBE
        14D909F3 7FEAF2C7 90D22FAE 7516B459 0BE35D53 E2FE1A35
        AFE4B660 7CB35858 9C3B4D09 4A1D81FE 0717F1DF 5BDDEB3E
        114F130B B781E66C 22B5B770 E8AE115F F39F8ADA F66DEEDF


  returned_bits is
        4F35B85F 95DEE3E8 73054905 CFD02341 653E18F5 29930CBE
        14D909F3 7FEAF2C7 90D22FAE 7516B459 0BE35D53 E2FE1A35
        AFE4B660 7CB35858 9C3B4D09 4A1D81FE 0717F1DF 5BDDEB3E
        114F130B B781E66C 22B5B770 E8AE115F F39F8ADA F66DEEDF


---------------------------

  Update V

    0x03||V is
                          03F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F48E
        5825A9C5 D61BA51D A06B3B90 4B20C712 D51713AE 30EC1137
        C244277E F8C53DE9 0A7D5465 7C1FFE5A 9857F4B3 6A040389


    H is
        DFE8790D F7153FE5 E634CDD6 48943BAC 36AED716 064DEAED
        97954957 CD97E5CD CB2F723B 27823018 D414D93F 7EF82599


  Updated values

  V is
                            70F969 CD6BE43E 620C9FBA 38A66E8D
        FF8AEA3F 5F1C440C D8BEAFCC 7ED06BB8 9F8CE0BF FD3CD246
        F98DEAD1 2E042EAF D6B5E526 9679C734 9896C291 23204BE2
        DA5CF449 2EC336B8 6729E436 6E76D048 9594FA4B F0537AA1
        49B1C5D9 D8B0AE40 8F02B760 27CE9A65 7E852F13 EAC7373E
```

```
  reseed_counter is
                                                  0000 00000003


rnd_val is
        4F35B85F 95DEE3E8 73054905 CFD02341 653E18F5 29930CBE
        14D909F3 7FEAF2C7 90D22FAE 7516B459 0BE35D53 E2FE1A35
        AFE4B660 7CB35858 9C3B4D09 4A1D81FE 0717F1DF 5BDDEB3E
        114F130B B781E66C 22B5B770 E8AE115F F39F8ADA F66DEEDF


################################################################

Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B
```

```
    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

--------------------------

  Hash_df - Generate seed(which is V) - Step 2
```

```
seed_material is
                                                          000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                          01000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                          02000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B
```

```
  Hash(counter||no_of_bits_to_return||input_string) is
      31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
      E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


  temp =
      703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
      FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4
      31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
      E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


  ------------

  i = 3

  counter||no_of_bits_to_return||input_string is
                                          03000003 78000102
      03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
      1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
      33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
      4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
      63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


  Hash(counter||no_of_bits_to_return||input_string) is
      9B71197A 30150000 F1E5B6AD 1EB81AB2 7B8E19BE 185E4F70
      61F1D3CA 9B3A0DF4 FD597962 C2070B7E B064B31F 4F3E10BD


  temp =
                          703AEC B83762E8 855BF167 2A52FAEF
      5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
      FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
      DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
      AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


V is
                          703AEC B83762E8 855BF167 2A52FAEF
      5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
      FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
      DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
      AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    Hash(counter||no_of_bits_to_return||input_string) is
        805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
        DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


    temp =
        805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
        DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
```

```
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  Hash(counter||no_of_bits_to_return||input_string) is
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


  temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


  ------------

  i = 3

  counter||no_of_bits_to_return||input_string is
           03 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  Hash(counter||no_of_bits_to_return||input_string) is
    55F0BF84 2C6BF212 18612101 CB0E1A06 0E2E9C66 5E87E1BA
    9632F01B 4CF80D08 C9645BD1 830112EA 6EBFED69 A48CA9C9


  temp =
                       805F3E 8A9A40AA EE585729 8729B9CF
    5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
    7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
    A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
    EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


C is
                       805F3E 8A9A40AA EE585729 8729B9CF
    5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
    7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
    A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
    EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A
```

```
---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


---------------------------

  Process additional_input

    0x02||V||additional_input is
                                                02703A ECB83762
        E8855BF1 672A52FA EF5C7B5C 83E893D0 0130FEC6 3C9AC5F5
        3F23230D 5CCE766D 09FFF0DA C417C889 2FC43148 7080FDE0
        B521DEBC FC5AAB9D 39DAD946 6C24D449 8964E4E3 18D4DC77
        7C22A0EE E9B579B2 81AE6AEB 18B028D5 C99A9B71 197A3015
        0000F1E5 B6AD1EB8 1A606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    w=Hash(0x02||V||additional_input) is
        EE4375B2 9D2DB6EA 2FEBDE64 3BE768BB 5728BDCD 3CC2E9C7
        8DD9E04A 3B21D222 B5255FAD ADDAA214 FCEBFCBA 774E4C1F


    V is
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D3A
```

```
        C91CBC1E C2020073 94D0C17D 10C3E037 79C9ACB6 F23C9C49
        3C44CB62 EB4AA7EC 4FC0D0C7 280AB714 FDDDE271 246D0439


----------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                           703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D3A
        C91CBC1E C2020073 94D0C17D 10C3E037 79C9ACB6 F23C9C49
        3C44CB62 EB4AA7EC 4FC0D0C7 280AB714 FDDDE271 246D0439


    w_i is
        03D1294E 33F12491 597CF23D B8DF118F 9AD2BA71 D84B3C67
        60A43C58 39A3F449 ADE2B0F3 E02A13D2 2E1119C7 B95C207E


    W is
        03D1294E 33F12491 597CF23D B8DF118F 9AD2BA71 D84B3C67
        60A43C58 39A3F449 ADE2B0F3 E02A13D2 2E1119C7 B95C207E


    ------------

    i = 2

    data is
                           703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D3A
        C91CBC1E C2020073 94D0C17D 10C3E037 79C9ACB6 F23C9C49
        3C44CB62 EB4AA7EC 4FC0D0C7 280AB714 FDDDE271 246D043A


    w_i is
        0844A8BF E837C229 0BE251C8 DCC4D8CC 04B1CEF6 B42931CB
```

```
        54248C52 975CB5F7 5E2867B5 4C139B4C 0072E6EC 8A4EA49B


    W is
        03D1294E 33F12491 597CF23D B8DF118F 9AD2BA71 D84B3C67
        60A43C58 39A3F449 ADE2B0F3 E02A13D2 2E1119C7 B95C207E
        0844A8BF E837C229 0BE251C8 DCC4D8CC 04B1CEF6 B42931CB
        54248C52 975CB5F7 5E2867B5 4C139B4C 0072E6EC 8A4EA49B


  returned_bits is
        03D1294E 33F12491 597CF23D B8DF118F 9AD2BA71 D84B3C67
        60A43C58 39A3F449 ADE2B0F3 E02A13D2 2E1119C7 B95C207E
        0844A8BF E837C229 0BE251C8 DCC4D8CC 04B1CEF6 B42931CB
        54248C52 975CB5F7 5E2867B5 4C139B4C 0072E6EC 8A4EA49B


---------------------------

  Update V

    0x03||V is
                          03703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D3A
        C91CBC1E C2020073 94D0C17D 10C3E037 79C9ACB6 F23C9C49
        3C44CB62 EB4AA7EC 4FC0D0C7 280AB714 FDDDE271 246D0439


    H is
        EC6876DB 88ECA9C7 BC5F8875 B8D684F7 CDFA2747 D76628B5
        57AECAB4 07852B30 83E26D7F 9972C3F7 F1155371 5996C1C6


  Updated values

  V is
                            F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F48F
        57D4046F AC80FBF0 31BA24C2 A45C32B8 D192E386 82BC437A
        83CBEB1A 05235DA6 8CF92F06 45A9E6FF 010B9703 7FCED41A


  reseed_counter is
                                                0000 00000002
```

```
rnd_val is
        03D1294E 33F12491 597CF23D B8DF118F 9AD2BA71 D84B3C67
        60A43C58 39A3F449 ADE2B0F3 E02A13D2 2E1119C7 B95C207E
        0844A8BF E837C229 0BE251C8 DCC4D8CC 04B1CEF6 B42931CB
        54248C52 975CB5F7 5E2867B5 4C139B4C 0072E6EC 8A4EA49B


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
       AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
       C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
       DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
       F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


--------------------------

  Process additional_input

    0x02||V||additional_input is
                                                 02F09A 2B42D1A3
        9373B448 90B17CB4 BEAE0323 61A3D80A 0704DEBB 048CCB30
        7BE157F7 0E65D99F A87CBF62 CAA2E65B EFCD7396 CB8BBBD3
        F4DD3ABF C6BEE5F4 8F57D404 6FAC80FB F031BA24 C2A45C32
        B8D192E3 8682BC43 7A83CBEB 1A05235D A68CF92F 0645A9E6
        FF010B97 037FCED4 1AA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    w=Hash(0x02||V||additional_input) is
        D7D8B279 6E9806AC 119CBC1C 927B6B0E 4A22F083 2C0A53EF
```

```
        848D7133 30AE8B68 3625E0E3 4A8E4A72 0947CE2A F46128B8


    V is
                            F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F490
        2FACB6E9 1B19029C 4356E0DF 36D79DC7 1BB5D409 AEC6976A
        08595C4D 35D1E90E C31F0FE9 90383171 0A53652E 742FFCD2


----------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F490
        2FACB6E9 1B19029C 4356E0DF 36D79DC7 1BB5D409 AEC6976A
        08595C4D 35D1E90E C31F0FE9 90383171 0A53652E 742FFCD2


    w_i is
        D5398518 F8087E2F 155B3C56 47AF609C 8820D5F5 4B787490
        2934FB10 97C89440 A47A71E3 6A9A32A2 242F3799 66CD3F5D


    W is
        D5398518 F8087E2F 155B3C56 47AF609C 8820D5F5 4B787490
        2934FB10 97C89440 A47A71E3 6A9A32A2 242F3799 66CD3F5D


    ------------

    i = 2

    data is
                            F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
```

```
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F490
        2FACB6E9 1B19029C 4356E0DF 36D79DC7 1BB5D409 AEC6976A
        08595C4D 35D1E90E C31F0FE9 90383171 0A53652E 742FFCD3


    w_i is
        BBEF623B D6117BDE 441D2A94 815FD5C1 3638DE99 D50CFE0E
        390A2A6B 137B55A4 2452F182 8060DB3C 68AF5C86 A83AF833


    W is
        D5398518 F8087E2F 155B3C56 47AF609C 8820D5F5 4B787490
        2934FB10 97C89440 A47A71E3 6A9A32A2 242F3799 66CD3F5D
        BBEF623B D6117BDE 441D2A94 815FD5C1 3638DE99 D50CFE0E
        390A2A6B 137B55A4 2452F182 8060DB3C 68AF5C86 A83AF833


  returned_bits is
        D5398518 F8087E2F 155B3C56 47AF609C 8820D5F5 4B787490
        2934FB10 97C89440 A47A71E3 6A9A32A2 242F3799 66CD3F5D
        BBEF623B D6117BDE 441D2A94 815FD5C1 3638DE99 D50CFE0E
        390A2A6B 137B55A4 2452F182 8060DB3C 68AF5C86 A83AF833


--------------------------

  Update V

    0x03||V is
                          03F09A2B 42D1A393 73B44890 B17CB4BE
        AE032361 A3D80A07 04DEBB04 8CCB307B E157F70E 65D99FA8
        7CBF62CA A2E65BEF CD7396CB 8BBBD3F4 DD3ABFC6 BEE5F490
        2FACB6E9 1B19029C 4356E0DF 36D79DC7 1BB5D409 AEC6976A
        08595C4D 35D1E90E C31F0FE9 90383171 0A53652E 742FFCD2


    H is
        833DD309 055891D9 1B580F44 646C8AD9 B2839216 292FFC8F
        E13FA67E 2A56AC10 648A6E1C 5F810898 62581F7D 32829D4F


  Updated values

  V is
                            70F969 CD6BE43E 620C9FBA 38A66E8D
        FF8AEA3F 5F1C440C D8BEAFCC 7ED06BB8 9F8CE0BF FD3CD246
```

```
        F98DEAD1 2E042EAF D6B5E526 9679C734 9896C291 23204BE4
        55395B67 8203E62A 3F38CAF3 7605F62A 580875A7 91101275
        D97157CE 727C1FA8 E0FF6EC5 73E5A5FB 7EC3E5CC A87DA83D


  reseed_counter is
                                                0000 00000003


rnd_val is
        D5398518 F8087E2F 155B3C56 47AF609C 8820D5F5 4B787490
        2934FB10 97C89440 A47A71E3 6A9A32A2 242F3799 66CD3F5D
        BBEF623B D6117BDE 441D2A94 815FD5C1 3638DE99 D50CFE0E
        390A2A6B 137B55A4 2452F182 8060DB3C 68AF5C86 A83AF833


##############################################################

Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
```

```
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                20212223 24252627 28292A2B


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                20212223 24252627 28292A2B


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

---------------------------
```

```
Hash_df - Generate seed(which is V) - Step 2

  seed_material is
                  0001 02030405 06070809 0A0B0C0D 0E0F1011
      12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
      2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
      42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
      5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
      23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
      4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
      9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  no_of_bits_to_return = 888

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
        010000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
      12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
      2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
      42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
      5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
      23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
      4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
      9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Hash(counter||no_of_bits_to_return||input_string) is
      A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
      EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


  temp =
      A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
      EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


  ------------
```

```
i = 2

counter||no_of_bits_to_return||input_string is
      020000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


------------

i = 3

counter||no_of_bits_to_return||input_string is
      030000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
```

```
        A8989587 CED14C8E 80790CD7 146F3328 3D84860A 708750EA
        1FDCD1DA D814E76A CA6E310F 12AA0BBA 611A8E86 FC0EAE47


    temp =
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


  V is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        FD2CAD8E 501A9FA7 18212A41 9FA2251F 01E46C40 DDBF4D85
        223B6E11 48351858 CC99BE10 6D1A4301 A307DBAF DE079ADA


    temp =
                            DE0424 3D3BB302 329A9112 4D780ADC
        F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
        FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
        DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
        162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


  C is
                            DE0424 3D3BB302 329A9112 4D780ADC
        F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
        FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
        DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
        162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
```

```
      C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
      1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
      3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


  w_i is
      CB339E74 95C3645C 5961FF07 871F47ED F9D33B0A B471282F
      0E8FADD0 74661AEE 4D4F47C1 E39CE4FF 381A8BC4 DE0AA260


  W is
      CB339E74 95C3645C 5961FF07 871F47ED F9D33B0A B471282F
      0E8FADD0 74661AEE 4D4F47C1 E39CE4FF 381A8BC4 DE0AA260


  ------------

  i = 2

  data is
                          A028F8 43783D77 21E32AC5 FD923031
      884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
      C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
      1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
      3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F34


  w_i is
      ABD20471 17E89ED4 70829892 FC806CA1 33FC8435 340BE2EC
      8278AFC5 DF48595D 1D205F7F 835E2549 B9068A85 16FB1496


  W is
      CB339E74 95C3645C 5961FF07 871F47ED F9D33B0A B471282F
      0E8FADD0 74661AEE 4D4F47C1 E39CE4FF 381A8BC4 DE0AA260
      ABD20471 17E89ED4 70829892 FC806CA1 33FC8435 340BE2EC
      8278AFC5 DF48595D 1D205F7F 835E2549 B9068A85 16FB1496


returned_bits is
      CB339E74 95C3645C 5961FF07 871F47ED F9D33B0A B471282F
      0E8FADD0 74661AEE 4D4F47C1 E39CE4FF 381A8BC4 DE0AA260
      ABD20471 17E89ED4 70829892 FC806CA1 33FC8435 340BE2EC
      8278AFC5 DF48595D 1D205F7F 835E2549 B9068A85 16FB1496
```

```
--------------------------

  Update V

    0x03||V is
                          03A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    H is
        C51C82A3 D8EF332A 9C797699 F9E02289 F64D4850 CA0B186F
        BA66C32F 3971156C CA591193 6567EA3A 8EAEA908 EF1F29AE


  Updated values

  V is
                            7E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51BF
        B746C81A 39FDB5A5 89FD30B3 6DA6EDB5 97049299 164AB8FF
        0E63E360 B940DDCE 4FFED6D6 7B86D626 C4474340 07D33B07


  reseed_counter is
                                                0000 00000002


rnd_val is
        CB339E74 95C3645C 5961FF07 871F47ED F9D33B0A B471282F
        0E8FADD0 74661AEE 4D4F47C1 E39CE4FF 381A8BC4 DE0AA260
        ABD20471 17E89ED4 70829892 FC806CA1 33FC8435 340BE2EC
        8278AFC5 DF48595D 1D205F7F 835E2549 B9068A85 16FB1496


-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            7E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51BF
        B746C81A 39FDB5A5 89FD30B3 6DA6EDB5 97049299 164AB8FF
        0E63E360 B940DDCE 4FFED6D6 7B86D626 C4474340 07D33B07


    w_i is
        938BAB9C 357B9023 92AEFA66 8DFDB88C 9C671FC0 220ED319
        7F852B3B 9C27AD33 D99403E6 56510F77 E964130B 284759A0


    W is
        938BAB9C 357B9023 92AEFA66 8DFDB88C 9C671FC0 220ED319
        7F852B3B 9C27AD33 D99403E6 56510F77 E964130B 284759A0


    ------------

    i = 2

    data is
                            7E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51BF
        B746C81A 39FDB5A5 89FD30B3 6DA6EDB5 97049299 164AB8FF
        0E63E360 B940DDCE 4FFED6D6 7B86D626 C4474340 07D33B08


    w_i is
        EB42F933 E6B2D170 99744089 402ED23B C8C0CAD5 9BA485A9
```

```
        04B5456E 4EFEFC22 9415778F 50957FDD B559C053 FB97CE79


    W is
        938BAB9C 357B9023 92AEFA66 8DFDB88C 9C671FC0 220ED319
        7F852B3B 9C27AD33 D99403E6 56510F77 E964130B 284759A0
        EB42F933 E6B2D170 99744089 402ED23B C8C0CAD5 9BA485A9
        04B5456E 4EFEFC22 9415778F 50957FDD B559C053 FB97CE79


  returned_bits is
        938BAB9C 357B9023 92AEFA66 8DFDB88C 9C671FC0 220ED319
        7F852B3B 9C27AD33 D99403E6 56510F77 E964130B 284759A0
        EB42F933 E6B2D170 99744089 402ED23B C8C0CAD5 9BA485A9
        04B5456E 4EFEFC22 9415778F 50957FDD B559C053 FB97CE79


---------------------------

  Update V

    0x03||V is
                           037E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51BF
        B746C81A 39FDB5A5 89FD30B3 6DA6EDB5 97049299 164AB8FF
        0E63E360 B940DDCE 4FFED6D6 7B86D626 C4474340 07D33B07


    H is
        6A7CBF9C FBFDBBFB A6105685 736B5949 231723D9 902E60CB
        289AA32B 0B06A6FF D00F7F0A 29DFD1EF 461D8806 4F8A4AD5


  Updated values

  V is
                             5C3140 BDEFA37B 87184CEA 988245EB
        6F1B558E 4A2EA5EA 8639E1E7 5B708E47 9EFE58C6 3B2EFD15
        BEF130CD 38404BEA 5FBE2D47 83D6C792 4F9DA6B1 32F8DB60
        FE67DA3A 1D15AB85 DA31DF90 1723BF4E CFA16FC4 FF3D23EA
        4D2BA5EE 8EE0108C E80B828E 33B6C2B5 B17CEC70 98FD2803


  reseed_counter is
                                                 0000 00000003
```

```
rnd_val is
        938BAB9C 357B9023 92AEFA66 8DFDB88C 9C671FC0 220ED319
        7F852B3B 9C27AD33 D99403E6 56510F77 E964130B 284759A0
        EB42F933 E6B2D170 99744089 402ED23B C8C0CAD5 9BA485A9
        04B5456E 4EFEFC22 9415778F 50957FDD B559C053 FB97CE79


################################################################

Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                  20212223 24252627 28292A2B
```

PersonalizationString =
404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

AdditionalInput1 =
606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

AdditionalInput2 =
A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

##

****

Hash_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

nonce is
20212223 24252627 28292A2B

personal_str is
404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                    0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
          010000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
        A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
        EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964
```

```
temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


------------

i = 2

counter||no_of_bits_to_return||input_string is
      020000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


------------

i = 3

counter||no_of_bits_to_return||input_string is
      030000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
```

```
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
        A8989587 CED14C8E 80790CD7 146F3328 3D84860A 708750EA
        1FDCD1DA D814E76A CA6E310F 12AA0BBA 611A8E86 FC0EAE47


    temp =
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


  V is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
```

```
          01 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


------------

i = 3

counter||no_of_bits_to_return||input_string is
```

```
              03 00000378 00A028F8 43783D77 21E32AC5 FD923031
         884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
         C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
         1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
         3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    Hash(counter||no_of_bits_to_return||input_string) is
         FD2CAD8E 501A9FA7 18212A41 9FA2251F 01E46C40 DDBF4D85
         223B6E11 48351858 CC99BE10 6D1A4301 A307DBAF DE079ADA


    temp =
                             DE0424 3D3BB302 329A9112 4D780ADC
         F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
         FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
         DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
         162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


  C is
                             DE0424 3D3BB302 329A9112 4D780ADC
         F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
         FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
         DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
         162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                             606162 63646566 6768696A 6B6C6D6E
         6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
         8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
         9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
         B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
---------------------------

  Process additional_input

    0x02||V||additional_input is
                                                 02A028 F843783D
        7721E32A C5FD9230 31884CF9 D3F05FA2 BE09EB6A 82C782B6
        203C2938 47B98EC4 B9C0C867 4DEAE09E B964C747 54B6A1E7
        7C6C0DE0 245E3BC8 1E1585F2 F379F448 96435F61 C23DB552
        DB8B3190 F5F37B96 6F3DD000 CEB5373C A2BDA898 9587CED1
        4C8E8079 0CD7146F 33606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    w=Hash(0x02||V||additional_input) is
        89F101CF 9C3005E9 178BAD96 C069CF25 6FBB31FE A611220F
        860F6C0F CB4FE568 467A6238 53376C6D E4820FAE 06692A95


    V is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        9F76F4C3 16244E7F 5AEB0F58 FE1F2200 FAECC2F4 998CB87E
        C3DF6CDE 8087220B 0422FACD DB063DBA 730288BA DD7D99C8


---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        9F76F4C3 16244E7F 5AEB0F58 FE1F2200 FAECC2F4 998CB87E
        C3DF6CDE 8087220B 0422FACD DB063DBA 730288BA DD7D99C8
```

```
    w_i is
        5C0EDEEE 4E8060FE D022020C 83882E71 61F16100 9CCBC827
        E557091D 3FA172D8 E6EDFFB1 B4315D94 2448C8C5 42314E5C


    W is
        5C0EDEEE 4E8060FE D022020C 83882E71 61F16100 9CCBC827
        E557091D 3FA172D8 E6EDFFB1 B4315D94 2448C8C5 42314E5C


    ------------

    i = 2

    data is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        9F76F4C3 16244E7F 5AEB0F58 FE1F2200 FAECC2F4 998CB87E
        C3DF6CDE 8087220B 0422FACD DB063DBA 730288BA DD7D99C9


    w_i is
        F64BF9EE 10033D70 6BE38685 D3CA639A 14D54D3F 2877472E
        90794E29 BCD6E5EC A890E217 C7CA56A0 58113C6C 6483E455


    W is
        5C0EDEEE 4E8060FE D022020C 83882E71 61F16100 9CCBC827
        E557091D 3FA172D8 E6EDFFB1 B4315D94 2448C8C5 42314E5C
        F64BF9EE 10033D70 6BE38685 D3CA639A 14D54D3F 2877472E
        90794E29 BCD6E5EC A890E217 C7CA56A0 58113C6C 6483E455


  returned_bits is
        5C0EDEEE 4E8060FE D022020C 83882E71 61F16100 9CCBC827
        E557091D 3FA172D8 E6EDFFB1 B4315D94 2448C8C5 42314E5C
        F64BF9EE 10033D70 6BE38685 D3CA639A 14D54D3F 2877472E
        90794E29 BCD6E5EC A890E217 C7CA56A0 58113C6C 6483E455


--------------------------

  Update V
```

```
    0x03||V is
                          03A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        9F76F4C3 16244E7F 5AEB0F58 FE1F2200 FAECC2F4 998CB87E
        C3DF6CDE 8087220B 0422FACD DB063DBA 730288BA DD7D99C8


    H is
        3A9852A9 482B8F08 D0AA4A59 8938647C 53958EDE D90D362B
        29AABCC3 0CFE18A1 82DB77D5 35BC98E7 CE6132F1 6A11FBE2


  Updated values

  V is
                            7E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51BF
        B6B399EF 456A176C D5B9B209 BD68FECD 64080B25 CB5DF8CA
        03B74904 581DC66B 4EFB9F50 9F12F141 E87BDCD6 892F37D0


  reseed_counter is
                                                0000 00000002


rnd_val is
        5C0EDEEE 4E8060FE D022020C 83882E71 61F16100 9CCBC827
        E557091D 3FA172D8 E6EDFFB1 B4315D94 2448C8C5 42314E5C
        F64BF9EE 10033D70 6BE38685 D3CA639A 14D54D3F 2877472E
        90794E29 BCD6E5EC A890E217 C7CA56A0 58113C6C 6483E455


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number__of_bits = 768

  additional_input
```

```
                          A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


---------------------------

  Process additional_input

    0x02||V||additional_input is
                                              027E2D 1C80B3F0
        79547DBB D84B0A3B 0E7BB427 B11D4724 544812A6 351179A2
        33ED93C8 86FA5EE0 E7BFDCCC 0D919075 51E242BA 4E1D3C57
        875DD5C3 6AC89A51 BFB6B399 EF456A17 6CD5B9B2 09BD68FE
        CD64080B 25CB5DF8 CA03B749 04581DC6 6B4EFB9F 509F12F1
        41E87BDC D6892F37 D0A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    w=Hash(0x02||V||additional_input) is
        F8B39FAA C0A147A4 FB8A4344 6EA54F62 1417A1E4 06A73BF5
        6BAF2965 1A4278CD 051C2AA4 5ED0E030 01481C22 8EC4D71F


    V is
                          7E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51C0
        AF67399A 060B5F11 D143F54E 2C0E4E2F 781FAD09 D20534BF
        6F667269 72603F38 5417C9F4 FDE3D171 E9C3F8F9 17F40EEF


---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1
```

```
  data is
                          7E2D1C 80B3F079 547DBBD8 4B0A3B0E
      7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
      BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51C0
      AF67399A 060B5F11 D143F54E 2C0E4E2F 781FAD09 D20534BF
      6F667269 72603F38 5417C9F4 FDE3D171 E9C3F8F9 17F40EEF


  w_i is
      C80CAED7 81EF9B2A 31E2138F C4461243 6D992B6B EDFBBC82
      EEA943ED 49209F36 E0AE25F4 ED5FBA96 BE0357F1 64964D32


  W is
      C80CAED7 81EF9B2A 31E2138F C4461243 6D992B6B EDFBBC82
      EEA943ED 49209F36 E0AE25F4 ED5FBA96 BE0357F1 64964D32


  ------------

  i = 2

  data is
                          7E2D1C 80B3F079 547DBBD8 4B0A3B0E
      7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
      BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51C0
      AF67399A 060B5F11 D143F54E 2C0E4E2F 781FAD09 D20534BF
      6F667269 72603F38 5417C9F4 FDE3D171 E9C3F8F9 17F40EF0


  w_i is
      267F5736 6C89A1B0 CFE86D02 5CA1E21D 14F0B4C0 998DADF4
      684BFB21 18F82241 3D87693C B99AC0B5 9D5E0494 BF74293B


  W is
      C80CAED7 81EF9B2A 31E2138F C4461243 6D992B6B EDFBBC82
      EEA943ED 49209F36 E0AE25F4 ED5FBA96 BE0357F1 64964D32
      267F5736 6C89A1B0 CFE86D02 5CA1E21D 14F0B4C0 998DADF4
      684BFB21 18F82241 3D87693C B99AC0B5 9D5E0494 BF74293B


returned_bits is
      C80CAED7 81EF9B2A 31E2138F C4461243 6D992B6B EDFBBC82
      EEA943ED 49209F36 E0AE25F4 ED5FBA96 BE0357F1 64964D32
```

```
        267F5736 6C89A1B0 CFE86D02 5CA1E21D 14F0B4C0 998DADF4
        684BFB21 18F82241 3D87693C B99AC0B5 9D5E0494 BF74293B


---------------------------

  Update V

    0x03||V is
                         037E2D1C 80B3F079 547DBBD8 4B0A3B0E
        7BB427B1 1D472454 4812A635 1179A233 ED93C886 FA5EE0E7
        BFDCCC0D 91907551 E242BA4E 1D3C5787 5DD5C36A C89A51C0
        AF67399A 060B5F11 D143F54E 2C0E4E2F 781FAD09 D20534BF
        6F667269 72603F38 5417C9F4 FDE3D171 E9C3F8F9 17F40EEF


    H is
        A9EE2234 CE80829B C041F6C6 6767C640 A755BC7E 1448E311
        BE81C684 5FD345ED FD46BBFB 374CBCCC E2CB1C30 A03D0E44


  Updated values

  V is
                           5C3140 BDEFA37B 87184CEA 988245EB
        6F1B558E 4A2EA5EA 8639E1E7 5B708E47 9EFE58C6 3B2EFD15
        BEF130CD 38404BEA 5FBE2D47 83D6C792 4F9DA6B1 32F8DB62
        35F9AE51 BBA61B92 3BAA446B C9878CC0 34FB22DA 3F1221F1
        44155850 9CCC10E5 195BB29D C380A8DE 73A73653 F9D0BF5A


  reseed_counter is
                                                0000 00000003


rnd_val is
        C80CAED7 81EF9B2A 31E2138F C4461243 6D992B6B EDFBBC82
        EEA943ED 49209F36 E0AE25F4 ED5FBA96 BE0357F1 64964D32
        267F5736 6C89A1B0 CFE86D02 5CA1E21D 14F0B4C0 998DADF4
        684BFB21 18F82241 3D87693C B99AC0B5 9D5E0494 BF74293B


##############################################################

Hash_DRBG
```

```
    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                   20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
```

```
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                   20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                               01000003 78000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
        703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
        FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4
```

```
temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                          02000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
    E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4
    31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
    E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                          03000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    9B71197A 30150000 F1E5B6AD 1EB81AB2 7B8E19BE 185E4F70
    61F1D3CA 9B3A0DF4 FD597962 C2070B7E B064B31F 4F3E10BD
```

```
    temp =
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  V is
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    Hash(counter||no_of_bits_to_return||input_string) is
        805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
```

```
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


Hash(counter||no_of_bits_to_return||input_string) is
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


Hash(counter||no_of_bits_to_return||input_string) is
    55F0BF84 2C6BF212 18612101 CB0E1A06 0E2E9C66 5E87E1BA
```

```
        9632F01B 4CF80D08 C9645BD1 830112EA 6EBFED69 A48CA9C9


    temp =
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


  C is
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

Generate FAILED: Reseed is required
---------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input <empty>
```

```
--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                 01703A ECB83762
        E8855BF1 672A52FA EF5C7B5C 83E893D0 0130FEC6 3C9AC5F5
        3F23230D 5CCE766D 09FFF0DA C417C889 2FC43148 7080FDE0
        B521DEBC FC5AAB9D 39DAD946 6C24D449 8964E4E3 18D4DC77
        7C22A0EE E9B579B2 81AE6AEB 18B028D5 C99A9B71 197A3015
        0000F1E5 B6AD1EB8 1A808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                  01000003 7801703A ECB83762
        E8855BF1 672A52FA EF5C7B5C 83E893D0 0130FEC6 3C9AC5F5
        3F23230D 5CCE766D 09FFF0DA C417C889 2FC43148 7080FDE0
        B521DEBC FC5AAB9D 39DAD946 6C24D449 8964E4E3 18D4DC77
        7C22A0EE E9B579B2 81AE6AEB 18B028D5 C99A9B71 197A3015
        0000F1E5 B6AD1EB8 1A808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    Hash(counter||no_of_bits_to_return||input_string) is
        7E5DAD76 6ACF7AAF B519AACA 20DDE991 7C71518B 26AA4D22
        59D74355 01D36678 FAC6ED03 02D6CB58 19B41DE1 BE37D52F


    temp =
        7E5DAD76 6ACF7AAF B519AACA 20DDE991 7C71518B 26AA4D22
        59D74355 01D36678 FAC6ED03 02D6CB58 19B41DE1 BE37D52F
```

```
------------

i = 2

counter||no_of_bits_to_return||input_string is
                                02000003 7801703A ECB83762
    E8855BF1 672A52FA EF5C7B5C 83E893D0 0130FEC6 3C9AC5F5
    3F23230D 5CCE766D 09FFF0DA C417C889 2FC43148 7080FDE0
    B521DEBC FC5AAB9D 39DAD946 6C24D449 8964E4E3 18D4DC77
    7C22A0EE E9B579B2 81AE6AEB 18B028D5 C99A9B71 197A3015
    0000F1E5 B6AD1EB8 1A808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


Hash(counter||no_of_bits_to_return||input_string) is
    4CF663DE 1206F3E7 155A77DE CCD25928 52C5ABC0 5E965EEF
    D9A037B8 0F543BDE 841A2995 17DD59E4 D2B94266 688FCAE8


temp =
    7E5DAD76 6ACF7AAF B519AACA 20DDE991 7C71518B 26AA4D22
    59D74355 01D36678 FAC6ED03 02D6CB58 19B41DE1 BE37D52F
    4CF663DE 1206F3E7 155A77DE CCD25928 52C5ABC0 5E965EEF
    D9A037B8 0F543BDE 841A2995 17DD59E4 D2B94266 688FCAE8


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                03000003 7801703A ECB83762
    E8855BF1 672A52FA EF5C7B5C 83E893D0 0130FEC6 3C9AC5F5
    3F23230D 5CCE766D 09FFF0DA C417C889 2FC43148 7080FDE0
    B521DEBC FC5AAB9D 39DAD946 6C24D449 8964E4E3 18D4DC77
    7C22A0EE E9B579B2 81AE6AEB 18B028D5 C99A9B71 197A3015
    0000F1E5 B6AD1EB8 1A808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        0FE80879 F630AC0C 8AD29B88 CE04BA06 1205867D E4370C70
        8EA1D26A AA5404A5 BDEC5A21 D4C67A06 0E1EEC9B 3DAE4D5A


    temp =
                            7E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA


  V is
                            7E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           007E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 007E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    0FAEFA23 5A4B132C 0E1FE14C DFBF3B74 CB7AA766 5ADE588A
    A944BD29 0A544B1A 51D131B6 FE18970F ED180A8A 6F20FEB1


temp =
    0FAEFA23 5A4B132C 0E1FE14C DFBF3B74 CB7AA766 5ADE588A
    A944BD29 0A544B1A 51D131B6 FE18970F ED180A8A 6F20FEB1


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 007E5DAD 766ACF7A AFB519AA CA20DDE9
    917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
    5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
    2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
    E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA


Hash(counter||no_of_bits_to_return||input_string) is
    DC4E2903 A842F51D 513F106E D4C52B41 5C888415 720628B2
    BE042776 1EC657E4 A5732C05 F47EBEF6 9942E47D E7387959


temp =
    0FAEFA23 5A4B132C 0E1FE14C DFBF3B74 CB7AA766 5ADE588A
    A944BD29 0A544B1A 51D131B6 FE18970F ED180A8A 6F20FEB1
    DC4E2903 A842F51D 513F106E D4C52B41 5C888415 720628B2
    BE042776 1EC657E4 A5732C05 F47EBEF6 9942E47D E7387959


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 007E5DAD 766ACF7A AFB519AA CA20DDE9
    917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
    5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
    2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
    E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        DBA8857F B0CCCB33 CDC1F142 FB0E0826 309E9715 1671A68D
        A86CADA4 55F42B5F D57762B9 43CCDEF3 856B0F59 CE548570


    temp =
                            0FAEFA 235A4B13 2C0E1FE1 4CDFBF3B
        74CB7AA7 665ADE58 8AA944BD 290A544B 1A51D131 B6FE1897
        0FED180A 8A6F20FE B1DC4E29 03A842F5 1D513F10 6ED4C52B
        415C8884 15720628 B2BE0427 761EC657 E4A5732C 05F47EBE
        F69942E4 7DE73879 59DBA885 7FB0CCCB 33CDC1F1 42FB0E08


  C is
                            0FAEFA 235A4B13 2C0E1FE1 4CDFBF3B
        74CB7AA7 665ADE58 8AA944BD 290A544B 1A51D131 B6FE1897
        0FED180A 8A6F20FE B1DC4E29 03A842F5 1D513F10 6ED4C52B
        415C8884 15720628 B2BE0427 761EC657 E4A5732C 05F47EBE
        F69942E4 7DE73879 59DBA885 7FB0CCCB 33CDC1F1 42FB0E08


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            7E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA
```

```
    w_i is
        97993B78 F7C31C0E 876DC92E B7D6C408 E09D608A D6B99D0E
        A2229B05 A578C426 334FCC8A 1C7E676E D2D89A5B 4CDF5B3F


    W is
        97993B78 F7C31C0E 876DC92E B7D6C408 E09D608A D6B99D0E
        A2229B05 A578C426 334FCC8A 1C7E676E D2D89A5B 4CDF5B3F


    ------------

    i = 2

    data is
                            7E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BB


    w_i is
        4ADF1193 6BF14F4E 10909DBA 9C24F4FD FFDE7235 1DA8E2CC
        3B135A39 5373899E 5F1A5955 B880CA9B 9E9DD4C9 CA7FA4D4


    W is
        97993B78 F7C31C0E 876DC92E B7D6C408 E09D608A D6B99D0E
        A2229B05 A578C426 334FCC8A 1C7E676E D2D89A5B 4CDF5B3F
        4ADF1193 6BF14F4E 10909DBA 9C24F4FD FFDE7235 1DA8E2CC
        3B135A39 5373899E 5F1A5955 B880CA9B 9E9DD4C9 CA7FA4D4


  returned_bits is
        97993B78 F7C31C0E 876DC92E B7D6C408 E09D608A D6B99D0E
        A2229B05 A578C426 334FCC8A 1C7E676E D2D89A5B 4CDF5B3F
        4ADF1193 6BF14F4E 10909DBA 9C24F4FD FFDE7235 1DA8E2CC
        3B135A39 5373899E 5F1A5955 B880CA9B 9E9DD4C9 CA7FA4D4


--------------------------

  Update V
```

```
    0x03||V is
                          037E5DAD 766ACF7A AFB519AA CA20DDE9
        917C7151 8B26AA4D 2259D743 5501D366 78FAC6ED 0302D6CB
        5819B41D E1BE37D5 2F4CF663 DE1206F3 E7155A77 DECCD259
        2852C5AB C05E965E EFD9A037 B80F543B DE841A29 9517DD59
        E4D2B942 66688FCA E80FE808 79F630AC 0C8AD29B 88CE04BA


    H is
        2470C998 B8CD701E 9BE7C781 35CD4AE1 16A1A45F B5201E46
        44F1EDA5 21397674 22F94411 88315066 971E8650 94367968


  Updated values

  V is
                            8E0CA7 99C51A8D DBC3398C 17009D25
        0647EBF8 F18188A5 AD031C00 7E0C27B1 934C981E BA00EF62
        6806CC28 6C2D58D3 E129448C E1BA49E9 04669988 4DA19784
        8E2017C8 8E9E0CA6 3E7F6BE0 63FB6574 D9CB31B5 502C7A5F
        205DE9CC 05893EB8 64E4D49F 81D84DDD D7771ADD 5FFF8C2B


  reseed_counter is
                                                0000 00000002


rnd_val is
        97993B78 F7C31C0E 876DC92E B7D6C408 E09D608A D6B99D0E
        A2229B05 A578C426 334FCC8A 1C7E676E D2D89A5B 4CDF5B3F
        4ADF1193 6BF14F4E 10909DBA 9C24F4FD FFDE7235 1DA8E2CC
        3B135A39 5373899E 5F1A5955 B880CA9B 9E9DD4C9 CA7FA4D4


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>
```

```
Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                              018E0C A799C51A
        8DDBC339 8C17009D 250647EB F8F18188 A5AD031C 007E0C27
        B1934C98 1EBA00EF 626806CC 286C2D58 D3E12944 8CE1BA49
        E9046699 884DA197 848E2017 C88E9E0C A63E7F6B E063FB65
        74D9CB31 B5502C7A 5F205DE9 CC05893E B864E4D4 9F81D84D
        DDD7771A DD5FFF8C 2BC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                   01000003 78018E0C A799C51A
        8DDBC339 8C17009D 250647EB F8F18188 A5AD031C 007E0C27
        B1934C98 1EBA00EF 626806CC 286C2D58 D3E12944 8CE1BA49
        E9046699 884DA197 848E2017 C88E9E0C A63E7F6B E063FB65
        74D9CB31 B5502C7A 5F205DE9 CC05893E B864E4D4 9F81D84D
        DDD7771A DD5FFF8C 2BC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Hash(counter||no_of_bits_to_return||input_string) is
    3B501497 7E9BEF76 896882A3 74700D0F 005EC2B8 1A3DDC55
    40ACD3E9 F977A973 EEA7CFFB 39723992 3A1AA7B0 46237084


temp =
    3B501497 7E9BEF76 896882A3 74700D0F 005EC2B8 1A3DDC55
    40ACD3E9 F977A973 EEA7CFFB 39723992 3A1AA7B0 46237084


------------

i = 2

counter||no_of_bits_to_return||input_string is
                              02000003 78018E0C A799C51A
    8DDBC339 8C17009D 250647EB F8F18188 A5AD031C 007E0C27
    B1934C98 1EBA00EF 626806CC 286C2D58 D3E12944 8CE1BA49
    E9046699 884DA197 848E2017 C88E9E0C A63E7F6B E063FB65
    74D9CB31 B5502C7A 5F205DE9 CC05893E B864E4D4 9F81D84D
    DDD7771A DD5FFF8C 2BC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Hash(counter||no_of_bits_to_return||input_string) is
    E969AA92 E830907F F9539E22 3F819AB5 9BF925D9 29F358E0
    BD65668D B0D6435F 36231B96 24DC29B9 6E5F31AE 187179FF


temp =
    3B501497 7E9BEF76 896882A3 74700D0F 005EC2B8 1A3DDC55
    40ACD3E9 F977A973 EEA7CFFB 39723992 3A1AA7B0 46237084
    E969AA92 E830907F F9539E22 3F819AB5 9BF925D9 29F358E0
    BD65668D B0D6435F 36231B96 24DC29B9 6E5F31AE 187179FF


------------
```

```
    i = 3

    counter||no_of_bits_to_return||input_string is
                                    03000003 78018E0C A799C51A
        8DDBC339 8C17009D 250647EB F8F18188 A5AD031C 007E0C27
        B1934C98 1EBA00EF 626806CC 286C2D58 D3E12944 8CE1BA49
        E9046699 884DA197 848E2017 C88E9E0C A63E7F6B E063FB65
        74D9CB31 B5502C7A 5F205DE9 CC05893E B864E4D4 9F81D84D
        DDD7771A DD5FFF8C 2BC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Hash(counter||no_of_bits_to_return||input_string) is
        C683593C 29EAC84F FA3A7080 00F693AE 7D74F667 BFE35F02
        5339D960 956FD38D 73940468 762FF5D2 DA586BF0 7E493167


    temp =
                            3B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
        B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


  V is
                            3B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
        B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           003B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
```

```
    B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 003B5014 977E9BEF 76896882 A374700D
    0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
    923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
    B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
    B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


Hash(counter||no_of_bits_to_return||input_string) is
    8D07901B B7A8BF92 96741892 EC320FD3 25277543 ADA4C852
    E958037A D711C4D9 5F27E87C CAB1CB05 BE2EDFF3 8D929EDC


temp =
    8D07901B B7A8BF92 96741892 EC320FD3 25277543 ADA4C852
    E958037A D711C4D9 5F27E87C CAB1CB05 BE2EDFF3 8D929EDC


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 003B5014 977E9BEF 76896882 A374700D
    0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
    923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
    B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
    B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


Hash(counter||no_of_bits_to_return||input_string) is
    5E81C2BB 672FB37F F264402F A005D14E D6A38D76 491E9A82
    EEB01A7B 24138027 EC192B21 B111323C 5AD635D8 A291F3CA


temp =
    8D07901B B7A8BF92 96741892 EC320FD3 25277543 ADA4C852
```

E958037A D711C4D9 5F27E87C CAB1CB05 BE2EDFF3 8D929EDC
E81C2BB 672FB37F F264402F A005D14E D6A38D76 491E9A82
EEB01A7B 24138027 EC192B21 B111323C 5AD635D8 A291F3CA

---

i = 3

counter||no_of_bits_to_return||input_string is
03 00000378 003B5014 977E9BEF 76896882 A374700D
0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693

Hash(counter||no_of_bits_to_return||input_string) is
EA30D4CA 4A632217 75764E63 C166E12B 110EA234 149CA55C
2691229B E6BBB238 FACF8924 ACB5F9F8 96FD5264 A2F46BE2

temp =
8D0790 1BB7A8BF 92967418 92EC320F
D3252775 43ADA4C8 52E95803 7AD711C4 D95F27E8 7CCAB1CB
05BE2EDF F38D929E DC5E81C2 BB672FB3 7FF26440 2FA005D1
4ED6A38D 76491E9A 82EEB01A 7B241380 27EC192B 21B11132
3C5AD635 D8A291F3 CAEA30D4 CA4A6322 1775764E 63C166E1

C is
8D0790 1BB7A8BF 92967418 92EC320F
D3252775 43ADA4C8 52E95803 7AD711C4 D95F27E8 7CCAB1CB
05BE2EDF F38D929E DC5E81C2 BB672FB3 7FF26440 2FA005D1
4ED6A38D 76491E9A 82EEB01A 7B241380 27EC192B 21B11132
3C5AD635 D8A291F3 CAEA30D4 CA4A6322 1775764E 63C166E1

****

Hash_DRBG_Generate_algorithm

requested_number_of_bits = 768

additional_input <empty>

```
---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            3B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
        B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


    w_i is
        F5983946 320E36C6 4EF283CA 1F65D197 CF81624E C6778E77
        0E78949D 84EF21A4 5CDD62D1 DB76920D 4C2836FC 6AE5299F


    W is
        F5983946 320E36C6 4EF283CA 1F65D197 CF81624E C6778E77
        0E78949D 84EF21A4 5CDD62D1 DB76920D 4C2836FC 6AE5299F


    ------------

    i = 2

    data is
                            3B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
        B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F694


    w_i is
        AF1357D9 701FAD10 FBD88D1E 28322394 36D76EB2 71BDC3CA
        04425EC8 8BC0E89A 4D5C37FF CE7C6C3A BDE9C413 AE6D3FEA


    W is
```

```
        F5983946 320E36C6 4EF283CA 1F65D197 CF81624E C6778E77
        0E78949D 84EF21A4 5CDD62D1 DB76920D 4C2836FC 6AE5299F
        AF1357D9 701FAD10 FBD88D1E 28322394 36D76EB2 71BDC3CA
        04425EC8 8BC0E89A 4D5C37FF CE7C6C3A BDE9C413 AE6D3FEA


  returned_bits is
        F5983946 320E36C6 4EF283CA 1F65D197 CF81624E C6778E77
        0E78949D 84EF21A4 5CDD62D1 DB76920D 4C2836FC 6AE5299F
        AF1357D9 701FAD10 FBD88D1E 28322394 36D76EB2 71BDC3CA
        04425EC8 8BC0E89A 4D5C37FF CE7C6C3A BDE9C413 AE6D3FEA


---------------------------

  Update V

    0x03||V is
                          033B5014 977E9BEF 76896882 A374700D
        0F005EC2 B81A3DDC 5540ACD3 E9F977A9 73EEA7CF FB397239
        923A1AA7 B0462370 84E969AA 92E83090 7FF9539E 223F819A
        B59BF925 D929F358 E0BD6566 8DB0D643 5F36231B 9624DC29
        B96E5F31 AE187179 FFC68359 3C29EAC8 4FFA3A70 8000F693


    H is
        2EE3D634 22DF47F0 9117EB31 793BFD6D 3FA27D8A E9DD51CE
        5EF32DBA 5B099597 423B310B E0292C29 9FD141FC 91A9FC11


  Updated values

  V is
                            C857A4 B33644AF 091FDC9B 3660A21C
        E2258637 FBC7E2A4 A82A04D7 64D0896E 4D4DCFB8 78042404
        97F84987 A3D3B60F 6147EB6D 4E4F6043 FFEBB7DE 51DF876C
        335672E7 725259E3 F4C400B2 8210E730 C6C4B9D1 A1B33F2A
        54BC6321 E1C49905 0CEBE539 E69D7A14 0740F2BB 756C5986


  reseed_counter is
                                                0000 00000002


rnd_val is
        F5983946 320E36C6 4EF283CA 1F65D197 CF81624E C6778E77
```

0E78949D 84EF21A4 5CDD62D1 DB76920D 4C2836FC 6AE5299F
AF1357D9 701FAD10 FBD88D1E 28322394 36D76EB2 71BDC3CA
04425EC8 8BC0E89A 4D5C37FF CE7C6C3A BDE9C413 AE6D3FEA

##

Hash_DRBG

Requested Security Strength = 192

Requested Hash Algorithm = SHA-384

prediction_resistance_flag = "ENABLED"
EntropyInput =
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

EntropyInput1 (for Reseed1) =
808182 83848586 8788898A 8B8C8D8E
8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE

EntropyInput2 (for Reseed2) =
C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

Nonce =
20212223 24252627 28292A2B

PersonalizationString = <empty>

AdditionalInput1 =
606162 63646566 6768696A 6B6C6D6E

```
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##############################################################

**************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
```

```
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                        01000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


temp =
    703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
    FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                        02000003 78000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


Hash(counter||no_of_bits_to_return||input_string) is
    31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
    E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A
```

```
    temp =
        703AECB8 3762E885 5BF1672A 52FAEF5C 7B5C83E8 93D00130
        FEC63C9A C5F53F23 230D5CCE 766D09FF F0DAC417 C8892FC4
        31487080 FDE0B521 DEBCFC5A AB9D39DA D9466C24 D4498964
        E4E318D4 DC777C22 A0EEE9B5 79B281AE 6AEB18B0 28D5C99A


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
                                              03000003 78000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
        9B71197A 30150000 F1E5B6AD 1EB81AB2 7B8E19BE 185E4F70
        61F1D3CA 9B3A0DF4 FD597962 C2070B7E B064B31F 4F3E10BD


    temp =
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


  V is
                            703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
```

```
                    00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


Hash(counter||no_of_bits_to_return||input_string) is
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


temp =
    805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
    DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00703AEC B83762E8 855BF167 2A52FAEF
    5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
    FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
    DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
    AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


Hash(counter||no_of_bits_to_return||input_string) is
    424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
    89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9
```

```
    temp =
        805F3E8A 9A40AAEE 58572987 29B9CF51 87C6DDBB 443A05D3
        DFF4C7F2 053B3CBE 34E9B197 63329E7C CE88068B 1DD2C009
        424E5B0A BDF33FBB 5C02CA64 3A5753A2 4ED17561 9251B4E0
        89DACFDA C1CD8989 CF0F87B9 197E7BEF D8550312 538A89B9


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
              03 00000378 00703AEC B83762E8 855BF167 2A52FAEF
        5C7B5C83 E893D001 30FEC63C 9AC5F53F 23230D5C CE766D09
        FFF0DAC4 17C8892F C4314870 80FDE0B5 21DEBCFC 5AAB9D39
        DAD9466C 24D44989 64E4E318 D4DC777C 22A0EEE9 B579B281
        AE6AEB18 B028D5C9 9A9B7119 7A301500 00F1E5B6 AD1EB81A


    Hash(counter||no_of_bits_to_return||input_string) is
        55F0BF84 2C6BF212 18612101 CB0E1A06 0E2E9C66 5E87E1BA
        9632F01B 4CF80D08 C9645BD1 830112EA 6EBFED69 A48CA9C9


    temp =
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


  C is
                            805F3E 8A9A40AA EE585729 8729B9CF
        5187C6DD BB443A05 D3DFF4C7 F2053B3C BE34E9B1 9763329E
        7CCE8806 8B1DD2C0 09424E5B 0ABDF33F BB5C02CA 643A5753
        A24ED175 619251B4 E089DACF DAC1CD89 89CF0F87 B9197E7B
        EFD85503 12538A89 B955F0BF 842C6BF2 12186121 01CB0E1A


------------------------------------------------------------

First call to Generate
```

```
**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
--------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0170 3AECB837 62E8855B F1672A52 FAEF5C7B 5C83E893
        D00130FE C63C9AC5 F53F2323 0D5CCE76 6D09FFF0 DAC417C8
        892FC431 487080FD E0B521DE BCFC5AAB 9D39DAD9 466C24D4
        498964E4 E318D4DC 777C22A0 EEE9B579 B281AE6A EB18B028
        D5C99A9B 71197A30 150000F1 E5B6AD1E B81A8081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
```

```
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    03780170 3AECB837 62E8855B F1672A52 FAEF5C7B 5C83E893
    D00130FE C63C9AC5 F53F2323 0D5CCE76 6D09FFF0 DAC417C8
    892FC431 487080FD E0B521DE BCFC5AAB 9D39DAD9 466C24D4
    498964E4 E318D4DC 777C22A0 EEE9B579 B281AE6A EB18B028
    D5C99A9B 71197A30 150000F1 E5B6AD1E B81A8081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
    2EC68512 4C44A241 41B27CE0 A667988B 1862B83B 74885C0F
    ED758F3D 214F663E 3487B2C0 08FF214C 1FB7B815 7E0B45E9


temp =
    2EC68512 4C44A241 41B27CE0 A667988B 1862B83B 74885C0F
    ED758F3D 214F663E 3487B2C0 08FF214C 1FB7B815 7E0B45E9


------------
```

```
i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    03780170 3AECB837 62E8855B F1672A52 FAEF5C7B 5C83E893
    D00130FE C63C9AC5 F53F2323 0D5CCE76 6D09FFF0 DAC417C8
    892FC431 487080FD E0B521DE BCFC5AAB 9D39DAD9 466C24D4
    498964E4 E318D4DC 777C22A0 EEE9B579 B281AE6A EB18B028
    D5C99A9B 71197A30 150000F1 E5B6AD1E B81A8081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
    D3F65CB3 AF39B4BF 15E6DA8A BC9902E2 CE5B297F 01E89E31
    0A6515C0 8F42FAB2 91F08335 3EDF23DB 76584ABF 527837C6


temp =
    2EC68512 4C44A241 41B27CE0 A667988B 1862B83B 74885C0F
    ED758F3D 214F663E 3487B2C0 08FF214C 1FB7B815 7E0B45E9
    D3F65CB3 AF39B4BF 15E6DA8A BC9902E2 CE5B297F 01E89E31
    0A6515C0 8F42FAB2 91F08335 3EDF23DB 76584ABF 527837C6


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                                        030000
    03780170 3AECB837 62E8855B F1672A52 FAEF5C7B 5C83E893
    D00130FE C63C9AC5 F53F2323 0D5CCE76 6D09FFF0 DAC417C8
    892FC431 487080FD E0B521DE BCFC5AAB 9D39DAD9 466C24D4
    498964E4 E318D4DC 777C22A0 EEE9B579 B281AE6A EB18B028
    D5C99A9B 71197A30 150000F1 E5B6AD1E B81A8081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
```

```
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    Hash(counter||no_of_bits_to_return||input_string) is
        04C46773 69F62CB5 0C897A5D 438FDBC0 408F1139 53ED6641
        E119F9A1 724830AA A78D3C51 CC430F24 19BAE40B A6151252


    temp =
                            2EC685 124C44A2 4141B27C E0A66798
        8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
        4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
        E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
        DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


  V is
                            2EC685 124C44A2 4141B27C E0A66798
        8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
        4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
        E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
        DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           002EC685 124C44A2 4141B27C E0A66798
        8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
        4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
        E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
        DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


    no_of_bits_to_return = 888

    ------------

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
          01 00000378 002EC685 124C44A2 4141B27C E0A66798
    8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
    4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
    E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
    DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


Hash(counter||no_of_bits_to_return||input_string) is
    CFF74C15 F913106A 8D4C3201 1866ECE3 48203068 66A53E0B
    D56E68A4 E61A9D62 A73233E6 7D5BDB9C FFDA6063 0AD61EE9


temp =
    CFF74C15 F913106A 8D4C3201 1866ECE3 48203068 66A53E0B
    D56E68A4 E61A9D62 A73233E6 7D5BDB9C FFDA6063 0AD61EE9


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 002EC685 124C44A2 4141B27C E0A66798
    8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
    4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
    E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
    DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


Hash(counter||no_of_bits_to_return||input_string) is
    1DCE24C8 0C295386 9DF89D86 2AC5080E E7000A4F 68B878D2
    D62437F1 E0C84C5D 2E0F1C55 21E5EF75 905ECF95 C5471A15


temp =
    CFF74C15 F913106A 8D4C3201 1866ECE3 48203068 66A53E0B
    D56E68A4 E61A9D62 A73233E6 7D5BDB9C FFDA6063 0AD61EE9
    1DCE24C8 0C295386 9DF89D86 2AC5080E E7000A4F 68B878D2
    D62437F1 E0C84C5D 2E0F1C55 21E5EF75 905ECF95 C5471A15


------------

i = 3
```

```
    counter||no_of_bits_to_return||input_string is
              03 00000378 002EC685 124C44A2 4141B27C E0A66798
        8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
        4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
        E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
        DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


    Hash(counter||no_of_bits_to_return||input_string) is
        F671096A 2C471C7D 586DB04A FDB4F459 DA6FC12F BAD53E8F
        8E7DF27E BD701D43 6A82C950 5FBA3AC0 23967BD9 55C95899


    temp =
                            CFF74C 15F91310 6A8D4C32 011866EC
        E3482030 6866A53E 0BD56E68 A4E61A9D 62A73233 E67D5BDB
        9CFFDA60 630AD61E E91DCE24 C80C2953 869DF89D 862AC508
        0EE7000A 4F68B878 D2D62437 F1E0C84C 5D2E0F1C 5521E5EF
        75905ECF 95C5471A 15F67109 6A2C471C 7D586DB0 4AFDB4F4


  C is
                            CFF74C 15F91310 6A8D4C32 011866EC
        E3482030 6866A53E 0BD56E68 A4E61A9D 62A73233 E67D5BDB
        9CFFDA60 630AD61E E91DCE24 C80C2953 869DF89D 862AC508
        0EE7000A 4F68B878 D2D62437 F1E0C84C 5D2E0F1C 5521E5EF
        75905ECF 95C5471A 15F67109 6A2C471C 7D586DB0 4AFDB4F4


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------
```

```
  i = 1

  data is
                          2EC685 124C44A2 4141B27C E0A66798
      8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
      4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
      E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
      DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


  w_i is
      1D332DE2 79BD8828 3A8FB9E9 C595227C 870F77D1 80FC743F
      758FEEC7 CD372472 26A35B6E BC073529 AED940B3 4829143E


  W is
      1D332DE2 79BD8828 3A8FB9E9 C595227C 870F77D1 80FC743F
      758FEEC7 CD372472 26A35B6E BC073529 AED940B3 4829143E


  ------------

  i = 2

  data is
                          2EC685 124C44A2 4141B27C E0A66798
      8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
      4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
      E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
      DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDC


  w_i is
      587E175A D24D3D41 6C57F1C6 90D82C69 DB4C96AC 04ADAD2F
      8BA5A651 B1D7476A 4ED3B683 324685AB 8DB9F811 F79B1BA7


  W is
      1D332DE2 79BD8828 3A8FB9E9 C595227C 870F77D1 80FC743F
      758FEEC7 CD372472 26A35B6E BC073529 AED940B3 4829143E
      587E175A D24D3D41 6C57F1C6 90D82C69 DB4C96AC 04ADAD2F
      8BA5A651 B1D7476A 4ED3B683 324685AB 8DB9F811 F79B1BA7


returned_bits is
      1D332DE2 79BD8828 3A8FB9E9 C595227C 870F77D1 80FC743F
```

```
        758FEEC7 CD372472 26A35B6E BC073529 AED940B3 4829143E
        587E175A D24D3D41 6C57F1C6 90D82C69 DB4C96AC 04ADAD2F
        8BA5A651 B1D7476A 4ED3B683 324685AB 8DB9F811 F79B1BA7


---------------------------

  Update V

    0x03||V is
                          032EC685 124C44A2 4141B27C E0A66798
        8B1862B8 3B74885C 0FED758F 3D214F66 3E3487B2 C008FF21
        4C1FB7B8 157E0B45 E9D3F65C B3AF39B4 BF15E6DA 8ABC9902
        E2CE5B29 7F01E89E 310A6515 C08F42FA B291F083 353EDF23
        DB76584A BF527837 C604C467 7369F62C B50C897A 5D438FDB


    H is
        7A17B8BD 2EA72A06 BB316EE2 959B48F9 BA59C3E8 987B6744
        2B6F8027 4EEFF4A4 CD391467 BA5B0F3D 61AA24EB 715284C8


  Updated values

  V is
                            FEBDD1 284557B2 ABCEFEAE E1BECE85
        6E6082E8 A3DB2D9A 1BC2E3F7 E2076A03 A0DBB9E6 A6865AFC
        E91F9218 7888E164 D2F1C481 7BBB6308 45B3DF78 10E75E0B
        6BCD13F0 FD11CB1D BF11F830 480B5440 CA19C388 22DC2C57
        7C763741 A407B3F6 A93449D8 97F14C86 940F1C16 1993C998


  reseed_counter is
                                                0000 00000002


rnd_val is
        1D332DE2 79BD8828 3A8FB9E9 C595227C 870F77D1 80FC743F
        758FEEC7 CD372472 26A35B6E BC073529 AED940B3 4829143E
        587E175A D24D3D41 6C57F1C6 90D82C69 DB4C96AC 04ADAD2F
        8BA5A651 B1D7476A 4ED3B683 324685AB 8DB9F811 F79B1BA7


-------------------------------------------------------------

Second call to Generate
```

```
************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01FE BDD12845 57B2ABCE FEAEE1BE CE856E60 82E8A3DB
        2D9A1BC2 E3F7E207 6A03A0DB B9E6A686 5AFCE91F 92187888
        E164D2F1 C4817BBB 630845B3 DF7810E7 5E0B6BCD 13F0FD11
        CB1DBF11 F830480B 5440CA19 C38822DC 2C577C76 3741A407
        B3F6A934 49D897F1 4C86940F 1C161993 C998C0C1 C2C3C4C5
```

```
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    037801FE BDD12845 57B2ABCE FEAEE1BE CE856E60 82E8A3DB
    2D9A1BC2 E3F7E207 6A03A0DB B9E6A686 5AFCE91F 92187888
    E164D2F1 C4817BBB 630845B3 DF7810E7 5E0B6BCD 13F0FD11
    CB1DBF11 F830480B 5440CA19 C38822DC 2C577C76 3741A407
    B3F6A934 49D897F1 4C86940F 1C161993 C998C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Hash(counter||no_of_bits_to_return||input_string) is
    0CBC7C85 938D2C85 24D4FA7F 75CD7868 AE192376 E0912491
    D0E72C2B AFE33204 0400AF3E F3543A92 ABA503E9 226CE0E0


temp =
    0CBC7C85 938D2C85 24D4FA7F 75CD7868 AE192376 E0912491
    D0E72C2B AFE33204 0400AF3E F3543A92 ABA503E9 226CE0E0


------------
```

```
i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    037801FE BDD12845 57B2ABCE FEAEE1BE CE856E60 82E8A3DB
    2D9A1BC2 E3F7E207 6A03A0DB B9E6A686 5AFCE91F 92187888
    E164D2F1 C4817BBB 630845B3 DF7810E7 5E0B6BCD 13F0FD11
    CB1DBF11 F830480B 5440CA19 C38822DC 2C577C76 3741A407
    B3F6A934 49D897F1 4C86940F 1C161993 C998C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Hash(counter||no_of_bits_to_return||input_string) is
    8A938880 74BC3D00 7303A5EE 0874F8ED 82064F30 F2472D8E
    7B966403 CBDC23E4 A0523F2E 3E11F6ED B1ADF5C6 C469A377


temp =
    0CBC7C85 938D2C85 24D4FA7F 75CD7868 AE192376 E0912491
    D0E72C2B AFE33204 0400AF3E F3543A92 ABA503E9 226CE0E0
    8A938880 74BC3D00 7303A5EE 0874F8ED 82064F30 F2472D8E
    7B966403 CBDC23E4 A0523F2E 3E11F6ED B1ADF5C6 C469A377


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                                        030000
    037801FE BDD12845 57B2ABCE FEAEE1BE CE856E60 82E8A3DB
    2D9A1BC2 E3F7E207 6A03A0DB B9E6A686 5AFCE91F 92187888
    E164D2F1 C4817BBB 630845B3 DF7810E7 5E0B6BCD 13F0FD11
    CB1DBF11 F830480B 5440CA19 C38822DC 2C577C76 3741A407
    B3F6A934 49D897F1 4C86940F 1C161993 C998C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
```

```
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    Hash(counter||no_of_bits_to_return||input_string) is
        91A0A74D 14AE0597 DDE0D324 6219D784 2C2CB510 093EBAE1
        38C579CB 623BFCDE B9E9CC6E 05F351BF A2C17770 667CB1F1


    temp =
                            0CBC7C 85938D2C 8524D4FA 7F75CD78
        68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
        92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
        ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
        EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


  V is
                            0CBC7C 85938D2C 8524D4FA 7F75CD78
        68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
        92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
        ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
        EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           000CBC7C 85938D2C 8524D4FA 7F75CD78
        68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
        92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
        ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
        EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


    no_of_bits_to_return = 888

    ------------
```

```
i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 000CBC7C 85938D2C 8524D4FA 7F75CD78
    68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
    92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
    ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
    EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


Hash(counter||no_of_bits_to_return||input_string) is
    6957C0B9 A4E6023B 9429FD5E 97B7D15A F22EAE23 C4D97282
    43737CF7 388CC109 44671C90 B5CC8332 AE225A1A A6F90D6A


temp =
    6957C0B9 A4E6023B 9429FD5E 97B7D15A F22EAE23 C4D97282
    43737CF7 388CC109 44671C90 B5CC8332 AE225A1A A6F90D6A


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 000CBC7C 85938D2C 8524D4FA 7F75CD78
    68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
    92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
    ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
    EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


Hash(counter||no_of_bits_to_return||input_string) is
    74B0B25C 0064E888 36146F27 D908F901 62BD1B97 7803E346
    90DA2225 E2999EEA BF842516 0A3BED3B 3571AD12 BE4E2E69


temp =
    6957C0B9 A4E6023B 9429FD5E 97B7D15A F22EAE23 C4D97282
    43737CF7 388CC109 44671C90 B5CC8332 AE225A1A A6F90D6A
    74B0B25C 0064E888 36146F27 D908F901 62BD1B97 7803E346
    90DA2225 E2999EEA BF842516 0A3BED3B 3571AD12 BE4E2E69


------------
```

```
    i = 3

    counter||no_of_bits_to_return||input_string is
              03 00000378 000CBC7C 85938D2C 8524D4FA 7F75CD78
        68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
        92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
        ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
        EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


    Hash(counter||no_of_bits_to_return||input_string) is
        95E73825 F6DF0B03 09180685 A51C43F8 6D268199 75F63082
        E9FAE867 6876B8E2 BEF09A87 26B8B8C9 1B1DA259 625B81F9


    temp =
                            6957C0 B9A4E602 3B9429FD 5E97B7D1
        5AF22EAE 23C4D972 8243737C F7388CC1 0944671C 90B5CC83
        32AE225A 1AA6F90D 6A74B0B2 5C0064E8 8836146F 27D908F9
        0162BD1B 977803E3 4690DA22 25E2999E EABF8425 160A3BED
        3B3571AD 12BE4E2E 6995E738 25F6DF0B 03091806 85A51C43


  C is
                            6957C0 B9A4E602 3B9429FD 5E97B7D1
        5AF22EAE 23C4D972 8243737C F7388CC1 0944671C 90B5CC83
        32AE225A 1AA6F90D 6A74B0B2 5C0064E8 8836146F 27D908F9
        0162BD1B 977803E3 4690DA22 25E2999E EABF8425 160A3BED
        3B3571AD 12BE4E2E 6995E738 25F6DF0B 03091806 85A51C43


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------
```

```
  i = 1

  data is
                          0CBC7C 85938D2C 8524D4FA 7F75CD78
      68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
      92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
      ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
      EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


  w_i is
      4B7FF453 EB17F58C 49041450 8ABCCA50 E760FB71 13308E29
      F4E8A9B7 A67AC594 2ADBB6AC 445077EB B8D47B8C 92A7161B


  W is
      4B7FF453 EB17F58C 49041450 8ABCCA50 E760FB71 13308E29
      F4E8A9B7 A67AC594 2ADBB6AC 445077EB B8D47B8C 92A7161B


  ------------

  i = 2

  data is
                          0CBC7C 85938D2C 8524D4FA 7F75CD78
      68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
      92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
      ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
      EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D8


  w_i is
      E9020087 F87DAAD6 7E8F0BEE B5E53BCD 806243C8 E6362CB3
      5BACE034 00B5CDC9 5EFF9DE4 135A398F F50FC0F5 903B8073


  W is
      4B7FF453 EB17F58C 49041450 8ABCCA50 E760FB71 13308E29
      F4E8A9B7 A67AC594 2ADBB6AC 445077EB B8D47B8C 92A7161B
      E9020087 F87DAAD6 7E8F0BEE B5E53BCD 806243C8 E6362CB3
      5BACE034 00B5CDC9 5EFF9DE4 135A398F F50FC0F5 903B8073


returned_bits is
```

```
        4B7FF453 EB17F58C 49041450 8ABCCA50 E760FB71 13308E29
        F4E8A9B7 A67AC594 2ADBB6AC 445077EB B8D47B8C 92A7161B
        E9020087 F87DAAD6 7E8F0BEE B5E53BCD 806243C8 E6362CB3
        5BACE034 00B5CDC9 5EFF9DE4 135A398F F50FC0F5 903B8073


--------------------------

  Update V

    0x03||V is
                          030CBC7C 85938D2C 8524D4FA 7F75CD78
        68AE1923 76E09124 91D0E72C 2BAFE332 040400AF 3EF3543A
        92ABA503 E9226CE0 E08A9388 8074BC3D 007303A5 EE0874F8
        ED82064F 30F2472D 8E7B9664 03CBDC23 E4A0523F 2E3E11F6
        EDB1ADF5 C6C469A3 7791A0A7 4D14AE05 97DDE0D3 246219D7


    H is
        3EB6BAA9 3ADF6560 38CF1960 7D08A3E0 8D04D674 28FFEFEA
        C6DFC2EE 869DBC36 9F26D852 8FDCBD23 5ED55CEC 83AA2005


  Updated values

  V is
                            76143D 3F38732E C0B8FEF7 DE0D8549
        C3A047D1 9AA56A97 14145AA9 22E86FF3 0D4867CB CFA920BD
        C559C75E 03C965EE 4AFF443A DC752125 88A91815 15E17DF2
        2D9B7E14 0349B071 0DDB89E6 A6B719A3 5C64ACD8 6D483DCE
        EFC6E291 60207408 804E6032 02E84A33 F9BC55C6 2DB15620


  reseed_counter is
                                                0000 00000002


rnd_val is
        4B7FF453 EB17F58C 49041450 8ABCCA50 E760FB71 13308E29
        F4E8A9B7 A67AC594 2ADBB6AC 445077EB B8D47B8C 92A7161B
        E9020087 F87DAAD6 7E8F0BEE B5E53BCD 806243C8 E6362CB3
        5BACE034 00B5CDC9 5EFF9DE4 135A398F F50FC0F5 903B8073


################################################################
```

```
Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

################################################################
```

```
************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                     0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    no_of_bits_to_return = 888
```

```
------------

i = 1

counter||no_of_bits_to_return||input_string is
      010000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


------------

i = 2

counter||no_of_bits_to_return||input_string is
      020000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
```

```
        5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


    temp =
        A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
        EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964
        C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
        5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
          030000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
        A8989587 CED14C8E 80790CD7 146F3328 3D84860A 708750EA
        1FDCD1DA D814E76A CA6E310F 12AA0BBA 611A8E86 FC0EAE47


    temp =
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


V is
                            A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    Hash(counter||no_of_bits_to_return||input_string) is
        DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
        273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


    temp =
        DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
        273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
```

```
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    FD2CAD8E 501A9FA7 18212A41 9FA2251F 01E46C40 DDBF4D85
    223B6E11 48351858 CC99BE10 6D1A4301 A307DBAF DE079ADA


temp =
                        DE0424 3D3BB302 329A9112 4D780ADC
    F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
    FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
    DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
    162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


C is
                        DE0424 3D3BB302 329A9112 4D780ADC
    F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
    FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
    DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
```

```
        162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


-------------------------------------------------------------

First call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                01A028 F843783D
        7721E32A C5FD9230 31884CF9 D3F05FA2 BE09EB6A 82C782B6
        203C2938 47B98EC4 B9C0C867 4DEAE09E B964C747 54B6A1E7
        7C6C0DE0 245E3BC8 1E1585F2 F379F448 96435F61 C23DB552
        DB8B3190 F5F37B96 6F3DD000 CEB5373C A2BDA898 9587CED1
        4C8E8079 0CD7146F 33808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                01000003 7801A028 F843783D
    7721E32A C5FD9230 31884CF9 D3F05FA2 BE09EB6A 82C782B6
    203C2938 47B98EC4 B9C0C867 4DEAE09E B964C747 54B6A1E7
    7C6C0DE0 245E3BC8 1E1585F2 F379F448 96435F61 C23DB552
    DB8B3190 F5F37B96 6F3DD000 CEB5373C A2BDA898 9587CED1
    4C8E8079 0CD7146F 33808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


Hash(counter||no_of_bits_to_return||input_string) is
    B8FB4017 52EA402B 40088B38 B9E21FAF B07F86D2 EEFA0281
    2177C28A 76ABD2EA F0B450B6 7ED4F746 50EAF2DB 8F9C720A


temp =
    B8FB4017 52EA402B 40088B38 B9E21FAF B07F86D2 EEFA0281
    2177C28A 76ABD2EA F0B450B6 7ED4F746 50EAF2DB 8F9C720A


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                02000003 7801A028 F843783D
    7721E32A C5FD9230 31884CF9 D3F05FA2 BE09EB6A 82C782B6
    203C2938 47B98EC4 B9C0C867 4DEAE09E B964C747 54B6A1E7
    7C6C0DE0 245E3BC8 1E1585F2 F379F448 96435F61 C23DB552
    DB8B3190 F5F37B96 6F3DD000 CEB5373C A2BDA898 9587CED1
    4C8E8079 0CD7146F 33808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
  Hash(counter||no_of_bits_to_return||input_string) is
      81AEAEC8 4BB298FE 4D5974CE E9FD5218 B50B6CCB C77DAF80
      9FB549BB 18974D0C 8B93B38E E6CE54C7 6EEB3D08 DEF2817D


  temp =
      B8FB4017 52EA402B 40088B38 B9E21FAF B07F86D2 EEFA0281
      2177C28A 76ABD2EA F0B450B6 7ED4F746 50EAF2DB 8F9C720A
      81AEAEC8 4BB298FE 4D5974CE E9FD5218 B50B6CCB C77DAF80
      9FB549BB 18974D0C 8B93B38E E6CE54C7 6EEB3D08 DEF2817D


  ------------

  i = 3

  counter||no_of_bits_to_return||input_string is
                                03000003 7801A028 F843783D
      7721E32A C5FD9230 31884CF9 D3F05FA2 BE09EB6A 82C782B6
      203C2938 47B98EC4 B9C0C867 4DEAE09E B964C747 54B6A1E7
      7C6C0DE0 245E3BC8 1E1585F2 F379F448 96435F61 C23DB552
      DB8B3190 F5F37B96 6F3DD000 CEB5373C A2BDA898 9587CED1
      4C8E8079 0CD7146F 33808182 83848586 8788898A 8B8C8D8E
      8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
      D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  Hash(counter||no_of_bits_to_return||input_string) is
      72E347E6 D5CB535C 70672C3A BDF0EFA4 6C9A7825 B88095E6
      5A8C9D11 3A31E537 ADB6C58D E33365EA 1E6A964C 98246E96


  temp =
                          B8FB40 1752EA40 2B40088B 38B9E21F
      AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
      4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
      18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
      C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


V is
                          B8FB40 1752EA40 2B40088B 38B9E21F
      AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
```

```
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00B8FB40 1752EA40 2B40088B 38B9E21F
        AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00B8FB40 1752EA40 2B40088B 38B9E21F
        AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


    Hash(counter||no_of_bits_to_return||input_string) is
        A00A98C1 82E4603D A4DEA867 148EBB96 693D9023 2B5369D0
        8B42EC27 146D80C5 BF9703DB D40E8BA5 80F6E695 8A8B99D9


    temp =
        A00A98C1 82E4603D A4DEA867 148EBB96 693D9023 2B5369D0
        8B42EC27 146D80C5 BF9703DB D40E8BA5 80F6E695 8A8B99D9


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
```

```
          02 00000378 00B8FB40 1752EA40 2B40088B 38B9E21F
      AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
      4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
      18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
      C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


  Hash(counter||no_of_bits_to_return||input_string) is
      7487DB59 E24C9E95 4E3AF35C F2BD6FB4 2D65D637 51DF2849
      85C28A78 97BBA5D9 F0CD57CE F2D510F0 B5B301ED 9DBC6D3F


  temp =
      A00A98C1 82E4603D A4DEA867 148EBB96 693D9023 2B5369D0
      8B42EC27 146D80C5 BF9703DB D40E8BA5 80F6E695 8A8B99D9
      7487DB59 E24C9E95 4E3AF35C F2BD6FB4 2D65D637 51DF2849
      85C28A78 97BBA5D9 F0CD57CE F2D510F0 B5B301ED 9DBC6D3F


  ------------

  i = 3

  counter||no_of_bits_to_return||input_string is
          03 00000378 00B8FB40 1752EA40 2B40088B 38B9E21F
      AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
      4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
      18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
      C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


  Hash(counter||no_of_bits_to_return||input_string) is
      CDF6BD79 4CBDFA51 F81D20A2 5BA13FFB 26B1CA0F 18161497
      9170A047 60F93748 01FC5EAF 8648F5F1 66CB4ED5 771C15BD


  temp =
                          A00A98 C182E460 3DA4DEA8 67148EBB
      96693D90 232B5369 D08B42EC 27146D80 C5BF9703 DBD40E8B
      A580F6E6 958A8B99 D97487DB 59E24C9E 954E3AF3 5CF2BD6F
      B42D65D6 3751DF28 4985C28A 7897BBA5 D9F0CD57 CEF2D510
      F0B5B301 ED9DBC6D 3FCDF6BD 794CBDFA 51F81D20 A25BA13F


C is
                          A00A98 C182E460 3DA4DEA8 67148EBB
```

```
        96693D90 232B5369 D08B42EC 27146D80 C5BF9703 DBD40E8B
        A580F6E6 958A8B99 D97487DB 59E24C9E 954E3AF3 5CF2BD6F
        B42D65D6 3751DF28 4985C28A 7897BBA5 D9F0CD57 CEF2D510
        F0B5B301 ED9DBC6D 3FCDF6BD 794CBDFA 51F81D20 A25BA13F


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            B8FB40 1752EA40 2B40088B 38B9E21F
        AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


    w_i is
        8D77F997 4D6EFCAF 503E24DB 4BC0E0F8 1E5E4931 60D3FFF8
        02F5AE66 4088B9C7 8381E88C CB992BF6 BCD72CDC 85CBDFCB


    W is
        8D77F997 4D6EFCAF 503E24DB 4BC0E0F8 1E5E4931 60D3FFF8
        02F5AE66 4088B9C7 8381E88C CB992BF6 BCD72CDC 85CBDFCB


    ------------

    i = 2
```

```
    data is
                             B8FB40 1752EA40 2B40088B 38B9E21F
        AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0F0


    w_i is
        D7A34759 D30CBB66 A97768F7 84654B25 98CF3814 8EEF1421
        0F2DC1A7 7479CE26 548BF86F B86AC16D 00064255 1F2BF597


    W is
        8D77F997 4D6EFCAF 503E24DB 4BC0E0F8 1E5E4931 60D3FFF8
        02F5AE66 4088B9C7 8381E88C CB992BF6 BCD72CDC 85CBDFCB
        D7A34759 D30CBB66 A97768F7 84654B25 98CF3814 8EEF1421
        0F2DC1A7 7479CE26 548BF86F B86AC16D 00064255 1F2BF597


  returned_bits is
        8D77F997 4D6EFCAF 503E24DB 4BC0E0F8 1E5E4931 60D3FFF8
        02F5AE66 4088B9C7 8381E88C CB992BF6 BCD72CDC 85CBDFCB
        D7A34759 D30CBB66 A97768F7 84654B25 98CF3814 8EEF1421
        0F2DC1A7 7479CE26 548BF86F B86AC16D 00064255 1F2BF597


--------------------------

  Update V

    0x03||V is
                           03B8FB40 1752EA40 2B40088B 38B9E21F
        AFB07F86 D2EEFA02 812177C2 8A76ABD2 EAF0B450 B67ED4F7
        4650EAF2 DB8F9C72 0A81AEAE C84BB298 FE4D5974 CEE9FD52
        18B50B6C CBC77DAF 809FB549 BB18974D 0C8B93B3 8EE6CE54
        C76EEB3D 08DEF281 7D72E347 E6D5CB53 5C70672C 3ABDF0EF


    H is
        4BC7D597 C62A8AB9 DF7D575B 36600197 989C10B4 7DBD39A7
        3A34661B 75FD5697 B1A503B8 62697571 D235D54B ECF1B172


  Updated values
```

```
  V is
                            5905D8 D8D5CEA0 68E4E733 9FCE70DB
        4619BD16 F61A4D6C 51ACBAAE B18B1953 B0B04B54 9252E382
        EBD1E1D9 711A280B E3F6368A 222DFF37 939B9468 2BDCBAC2
        18AA46DA C943E791 A9A2CF2F 6A10548A 7F1871BF DB96DD0C
        F259045A 6C7A0586 6EE5DDBD C28BFEBF 809E5998 CA0B43A1


  reseed_counter is
                                                 0000 00000002


rnd_val is
        8D77F997 4D6EFCAF 503E24DB 4BC0E0F8 1E5E4931 60D3FFF8
        02F5AE66 4088B9C7 8381E88C CB992BF6 BCD72CDC 85CBDFCB
        D7A34759 D30CBB66 A97768F7 84654B25 98CF3814 8EEF1421
        0F2DC1A7 7479CE26 548BF86F B86AC16D 00064255 1F2BF597


----------------------------------------------------------------

Second call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

Generate FAILED: Reseed is required
----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input <empty>
```

```
--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                 015905 D8D8D5CE
        A068E4E7 339FCE70 DB4619BD 16F61A4D 6C51ACBA AEB18B19
        53B0B04B 549252E3 82EBD1E1 D9711A28 0BE3F636 8A222DFF
        37939B94 682BDCBA C218AA46 DAC943E7 91A9A2CF 2F6A1054
        8A7F1871 BFDB96DD 0CF25904 5A6C7A05 866EE5DD BDC28BFE
        BF809E59 98CA0B43 A1C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                 01000003 78015905 D8D8D5CE
        A068E4E7 339FCE70 DB4619BD 16F61A4D 6C51ACBA AEB18B19
        53B0B04B 549252E3 82EBD1E1 D9711A28 0BE3F636 8A222DFF
        37939B94 682BDCBA C218AA46 DAC943E7 91A9A2CF 2F6A1054
        8A7F1871 BFDB96DD 0CF25904 5A6C7A05 866EE5DD BDC28BFE
        BF809E59 98CA0B43 A1C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Hash(counter||no_of_bits_to_return||input_string) is
        E0E8FA8A 274E1C52 EC32FF2D B7B20DE3 11A687FE DCCE16BA
        2174D649 79CBC4EE 88E38C50 41CC1449 D9025CD7 CA8CDB4B


    temp =
        E0E8FA8A 274E1C52 EC32FF2D B7B20DE3 11A687FE DCCE16BA
        2174D649 79CBC4EE 88E38C50 41CC1449 D9025CD7 CA8CDB4B
```

```
------------

i = 2

counter||no_of_bits_to_return||input_string is
                                02000003 78015905 D8D8D5CE
    A068E4E7 339FCE70 DB4619BD 16F61A4D 6C51ACBA AEB18B19
    53B0B04B 549252E3 82EBD1E1 D9711A28 0BE3F636 8A222DFF
    37939B94 682BDCBA C218AA46 DAC943E7 91A9A2CF 2F6A1054
    8A7F1871 BFDB96DD 0CF25904 5A6C7A05 866EE5DD BDC28BFE
    BF809E59 98CA0B43 A1C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Hash(counter||no_of_bits_to_return||input_string) is
    D4AB3A72 3B82DDFA E3726CDF 44448476 95254A09 27E159EA
    84D51C35 8B1E09F6 3C33CDB7 60C7CF2F 0BC717E1 A7C79F88


temp =
    E0E8FA8A 274E1C52 EC32FF2D B7B20DE3 11A687FE DCCE16BA
    2174D649 79CBC4EE 88E38C50 41CC1449 D9025CD7 CA8CDB4B
    D4AB3A72 3B82DDFA E3726CDF 44448476 95254A09 27E159EA
    84D51C35 8B1E09F6 3C33CDB7 60C7CF2F 0BC717E1 A7C79F88


------------

i = 3

counter||no_of_bits_to_return||input_string is
                                03000003 78015905 D8D8D5CE
    A068E4E7 339FCE70 DB4619BD 16F61A4D 6C51ACBA AEB18B19
    53B0B04B 549252E3 82EBD1E1 D9711A28 0BE3F636 8A222DFF
    37939B94 682BDCBA C218AA46 DAC943E7 91A9A2CF 2F6A1054
    8A7F1871 BFDB96DD 0CF25904 5A6C7A05 866EE5DD BDC28BFE
    BF809E59 98CA0B43 A1C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        0522B3EB 10EF6620 3FDFB8BD 78A4C9AA 3928F7C8 BF1D3B9C
        174C4BC2 6740B28B E351D4B1 A15100FF A92658D4 FBAB23A4


    temp =
                            E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9


  V is
                            E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    EF628007 43C7CB83 2F07C89A 2C83B2B7 DFA75554 51B5ED66
    8AFA1BCE 3A515971 78045783 4A80E93E 56148083 734E6A8A


temp =
    EF628007 43C7CB83 2F07C89A 2C83B2B7 DFA75554 51B5ED66
    8AFA1BCE 3A515971 78045783 4A80E93E 56148083 734E6A8A


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00E0E8FA 8A274E1C 52EC32FF 2DB7B20D
    E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
    49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
    7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
    2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9


Hash(counter||no_of_bits_to_return||input_string) is
    C09EAEFF 50386CEF C43FD862 A87AD414 8300FA72 B4D95F8D
    EC98BDB8 594237B3 B9226818 36323998 A07CDECE D262579F


temp =
    EF628007 43C7CB83 2F07C89A 2C83B2B7 DFA75554 51B5ED66
    8AFA1BCE 3A515971 78045783 4A80E93E 56148083 734E6A8A
    C09EAEFF 50386CEF C43FD862 A87AD414 8300FA72 B4D95F8D
    EC98BDB8 594237B3 B9226818 36323998 A07CDECE D262579F


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00E0E8FA 8A274E1C 52EC32FF 2DB7B20D
    E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
    49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
    7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
    2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        C0E1040B 9FC9BD97 78F36A8B 145C5088 345FFC14 B02B3136
        3401857D 89571268 366A5B46 090E2B1C A276EA7F FFA9AB38


    temp =
                            EF6280 0743C7CB 832F07C8 9A2C83B2
        B7DFA755 5451B5ED 668AFA1B CE3A5159 71780457 834A80E9
        3E561480 83734E6A 8AC09EAE FF50386C EFC43FD8 62A87AD4
        148300FA 72B4D95F 8DEC98BD B8594237 B3B92268 18363239
        98A07CDE CED26257 9FC0E104 0B9FC9BD 9778F36A 8B145C50


  C is
                            EF6280 0743C7CB 832F07C8 9A2C83B2
        B7DFA755 5451B5ED 668AFA1B CE3A5159 71780457 834A80E9
        3E561480 83734E6A 8AC09EAE FF50386C EFC43FD8 62A87AD4
        148300FA 72B4D95F 8DEC98BD B8594237 B3B92268 18363239
        98A07CDE CED26257 9FC0E104 0B9FC9BD 9778F36A 8B145C50


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9
```

```
    w_i is
        82393433 28419150 D8FAC3F7 943AFD48 5EE0F857 4E7A7EDD
        730B7D03 92DFB8A5 D933AF34 0677BBA0 24BE0983 4D86442E


    W is
        82393433 28419150 D8FAC3F7 943AFD48 5EE0F857 4E7A7EDD
        730B7D03 92DFB8A5 D933AF34 0677BBA0 24BE0983 4D86442E


    ------------

    i = 2

    data is
                            E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4CA


    w_i is
        CCAAAA83 6BF42EC2 3A1A86B7 2A645474 81EE7644 2297D058
        8BFC4356 7F09029B 41EE880C 1A5D60C9 ED4E843B 46958E04


    W is
        82393433 28419150 D8FAC3F7 943AFD48 5EE0F857 4E7A7EDD
        730B7D03 92DFB8A5 D933AF34 0677BBA0 24BE0983 4D86442E
        CCAAAA83 6BF42EC2 3A1A86B7 2A645474 81EE7644 2297D058
        8BFC4356 7F09029B 41EE880C 1A5D60C9 ED4E843B 46958E04


  returned_bits is
        82393433 28419150 D8FAC3F7 943AFD48 5EE0F857 4E7A7EDD
        730B7D03 92DFB8A5 D933AF34 0677BBA0 24BE0983 4D86442E
        CCAAAA83 6BF42EC2 3A1A86B7 2A645474 81EE7644 2297D058
        8BFC4356 7F09029B 41EE880C 1A5D60C9 ED4E843B 46958E04


--------------------------

  Update V
```

```
    0x03||V is
                          03E0E8FA 8A274E1C 52EC32FF 2DB7B20D
        E311A687 FEDCCE16 BA2174D6 4979CBC4 EE88E38C 5041CC14
        49D9025C D7CA8CDB 4BD4AB3A 723B82DD FAE3726C DF444484
        7695254A 0927E159 EA84D51C 358B1E09 F63C33CD B760C7CF
        2F0BC717 E1A7C79F 880522B3 EB10EF66 203FDFB8 BD78A4C9


    H is
        BF25C69C 42BC7161 B9408D6E 99DB68D9 74D76E32 CA975077
        D05014FF D5B7585B F40CE7DC DACF1A12 A56048AA 983103E5


  Updated values

  V is
                            D04B7A 916B15E7 D61B3AC7 C7E435C0
        9AF14DDD 532E8404 20AC6EF2 17B41D1E 6000E7E3 D38C4CFD
        882F16DD 5B3DDB45 D69549E9 718BBB4A EAA7B245 41ECBF59
        4A3DECE0 BE992C1B 31B1FB48 87BFC91B 1ECCC468 9A2E4A80
        97FC58F6 86318253 1BD2EB94 D17FD336 5D191BCD E0BE04FF


  reseed_counter is
                                                0000 00000002


rnd_val is
        82393433 28419150 D8FAC3F7 943AFD48 5EE0F857 4E7A7EDD
        730B7D03 92DFB8A5 D933AF34 0677BBA0 24BE0983 4D86442E
        CCAAAA83 6BF42EC2 3A1A86B7 2A645474 81EE7644 2297D058
        8BFC4356 7F09029B 41EE880C 1A5D60C9 ED4E843B 46958E04


###############################################################

Hash_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
```

```
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
    3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                         808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                         C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                                20212223 24252627 28292A2B


PersonalizationString =
                         404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                         606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


AdditionalInput2 =
                         A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
```

DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

##

****

Hash_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

nonce is
20212223 24252627 28292A2B

personal_str is
404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

prediction_resistance_flag = "PredictionResistance"

Hash_df - Generate seed(which is V) - Step 2

seed_material is
0001 02030405 06070809 0A0B0C0D 0E0F1011
12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

```
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
      010000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964


------------

i = 2

counter||no_of_bits_to_return||input_string is
      020000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
```

```
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


temp =
    A028F843 783D7721 E32AC5FD 92303188 4CF9D3F0 5FA2BE09
    EB6A82C7 82B6203C 293847B9 8EC4B9C0 C8674DEA E09EB964
    C74754B6 A1E77C6C 0DE0245E 3BC81E15 85F2F379 F4489643
    5F61C23D B552DB8B 3190F5F3 7B966F3D D000CEB5 373CA2BD


------------

i = 3

counter||no_of_bits_to_return||input_string is
      030000 03780001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
    A8989587 CED14C8E 80790CD7 146F3328 3D84860A 708750EA
    1FDCD1DA D814E76A CA6E310F 12AA0BBA 611A8E86 FC0EAE47


temp =
                        A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


V is
```

```
                          A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                         00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00A028F8 43783D77 21E32AC5 FD923031
        884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
        C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
        1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
        3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


    Hash(counter||no_of_bits_to_return||input_string) is
        DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
        273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


    temp =
        DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
        273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D


    ------------

    i = 2
```

```
counter||no_of_bits_to_return||input_string is
          02 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


temp =
    DE04243D 3BB30232 9A91124D 780ADCF3 672DDD2C E781963E
    273BB249 F6EC13B1 6A903F40 D01C2DFF 1464BFA6 AFD6987D
    7B72F966 9A700AF1 C7E3466A 5E89A0DC A45282E7 1A39E4AA
    24585736 11785015 85B95258 C40A2016 2D1F62CA 988BBEC7


------------

i = 3

counter||no_of_bits_to_return||input_string is
          03 00000378 00A028F8 43783D77 21E32AC5 FD923031
    884CF9D3 F05FA2BE 09EB6A82 C782B620 3C293847 B98EC4B9
    C0C8674D EAE09EB9 64C74754 B6A1E77C 6C0DE024 5E3BC81E
    1585F2F3 79F44896 435F61C2 3DB552DB 8B3190F5 F37B966F
    3DD000CE B5373CA2 BDA89895 87CED14C 8E80790C D7146F33


Hash(counter||no_of_bits_to_return||input_string) is
    FD2CAD8E 501A9FA7 18212A41 9FA2251F 01E46C40 DDBF4D85
    223B6E11 48351858 CC99BE10 6D1A4301 A307DBAF DE079ADA


temp =
                        DE0424 3D3BB302 329A9112 4D780ADC
    F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
    FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
    DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
    162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225
```

```
  C is
                            DE0424 3D3BB302 329A9112 4D780ADC
        F3672DDD 2CE78196 3E273BB2 49F6EC13 B16A903F 40D01C2D
        FF1464BF A6AFD698 7D7B72F9 669A700A F1C7E346 6A5E89A0
        DCA45282 E71A39E4 AA245857 36117850 1585B952 58C40A20
        162D1F62 CA988BBE C7FD2CAD 8E501A9F A718212A 419FA225


---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
---------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01A0 28F84378 3D7721E3 2AC5FD92 3031884C F9D3F05F
        A2BE09EB 6A82C782 B6203C29 3847B98E C4B9C0C8 674DEAE0
        9EB964C7 4754B6A1 E77C6C0D E0245E3B C81E1585 F2F379F4
        4896435F 61C23DB5 52DB8B31 90F5F37B 966F3DD0 00CEB537
        3CA2BDA8 989587CE D14C8E80 790CD714 6F338081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        037801A0 28F84378 3D7721E3 2AC5FD92 3031884C F9D3F05F
        A2BE09EB 6A82C782 B6203C29 3847B98E C4B9C0C8 674DEAE0
        9EB964C7 4754B6A1 E77C6C0D E0245E3B C81E1585 F2F379F4
        4896435F 61C23DB5 52DB8B31 90F5F37B 966F3DD0 00CEB537
        3CA2BDA8 989587CE D14C8E80 790CD714 6F338081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    DB62C08C B482A38A D2D4EABC 474050BD FB0D1344 FBE6BB0F
    5BBBAF71 6D2BDF7D D3BA3B46 CE78908F 2DEC6B26 3BD00FEB


temp =
    DB62C08C B482A38A D2D4EABC 474050BD FB0D1344 FBE6BB0F
    5BBBAF71 6D2BDF7D D3BA3B46 CE78908F 2DEC6B26 3BD00FEB


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    037801A0 28F84378 3D7721E3 2AC5FD92 3031884C F9D3F05F
    A2BE09EB 6A82C782 B6203C29 3847B98E C4B9C0C8 674DEAE0
    9EB964C7 4754B6A1 E77C6C0D E0245E3B C81E1585 F2F379F4
    4896435F 61C23DB5 52DB8B31 90F5F37B 966F3DD0 00CEB537
    3CA2BDA8 989587CE D14C8E80 790CD714 6F338081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
    C329E496 23AE4992 EADE0E6B CDC36DE3 4B03FC5C FD61A532
    5582D29B C2780A96 8CBB5376 004D708B AE3B054F 1CF82925


temp =
    DB62C08C B482A38A D2D4EABC 474050BD FB0D1344 FBE6BB0F
    5BBBAF71 6D2BDF7D D3BA3B46 CE78908F 2DEC6B26 3BD00FEB
    C329E496 23AE4992 EADE0E6B CDC36DE3 4B03FC5C FD61A532
    5582D29B C2780A96 8CBB5376 004D708B AE3B054F 1CF82925


------------
```

```
    i = 3

    counter||no_of_bits_to_return||input_string is
                                                          030000
        037801A0 28F84378 3D7721E3 2AC5FD92 3031884C F9D3F05F
        A2BE09EB 6A82C782 B6203C29 3847B98E C4B9C0C8 674DEAE0
        9EB964C7 4754B6A1 E77C6C0D E0245E3B C81E1585 F2F379F4
        4896435F 61C23DB5 52DB8B31 90F5F37B 966F3DD0 00CEB537
        3CA2BDA8 989587CE D14C8E80 790CD714 6F338081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    Hash(counter||no_of_bits_to_return||input_string) is
        094C757A B0DAE5E9 4BFCDC9A 5A049377 21DB8F8A 8FCBD7C2
        DE6DE5B7 6658B977 3F0B2FF8 B824D1CE D60B7FAB 387347B2


    temp =
                            DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


  V is
                            DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
```

```
                    00DB62C0 8CB482A3 8AD2D4EA BC474050
    BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
    8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
    E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
    8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 00DB62C0 8CB482A3 8AD2D4EA BC474050
    BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
    8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
    E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
    8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


Hash(counter||no_of_bits_to_return||input_string) is
    1FD805B7 12393932 B7F08472 36B8A96E D29CE6CC 7D1880B8
    81F3DA77 2E8850D8 56BD997E 5D5E3B20 75EB584F 9ACE259F


temp =
    1FD805B7 12393932 B7F08472 36B8A96E D29CE6CC 7D1880B8
    81F3DA77 2E8850D8 56BD997E 5D5E3B20 75EB584F 9ACE259F


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00DB62C0 8CB482A3 8AD2D4EA BC474050
    BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
    8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
    E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
    8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


Hash(counter||no_of_bits_to_return||input_string) is
    BD78AB1A CF9171F9 DBBE44E4 EFA42A0E 152868CA 4B27D976
    8C2E7157 A70442A8 DC5CDBCE 8084BE66 09817B44 79C30028
```

```
    temp =
        1FD805B7 12393932 B7F08472 36B8A96E D29CE6CC 7D1880B8
        81F3DA77 2E8850D8 56BD997E 5D5E3B20 75EB584F 9ACE259F
        BD78AB1A CF9171F9 DBBE44E4 EFA42A0E 152868CA 4B27D976
        8C2E7157 A70442A8 DC5CDBCE 8084BE66 09817B44 79C30028


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
              03 00000378 00DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


    Hash(counter||no_of_bits_to_return||input_string) is
        00FA7F1A E23870A1 11626EB7 3116C82A 57E59BE5 129548E3
        3D5C183C BD8DE667 FF128572 CA8344FC 77E057DD 7F143B17


    temp =
                            1FD805 B7123939 32B7F084 7236B8A9
        6ED29CE6 CC7D1880 B881F3DA 772E8850 D856BD99 7E5D5E3B
        2075EB58 4F9ACE25 9FBD78AB 1ACF9171 F9DBBE44 E4EFA42A
        0E152868 CA4B27D9 768C2E71 57A70442 A8DC5CDB CE8084BE
        6609817B 4479C300 2800FA7F 1AE23870 A111626E B73116C8


  C is
                            1FD805 B7123939 32B7F084 7236B8A9
        6ED29CE6 CC7D1880 B881F3DA 772E8850 D856BD99 7E5D5E3B
        2075EB58 4F9ACE25 9FBD78AB 1ACF9171 F9DBBE44 E4EFA42A
        0E152868 CA4B27D9 768C2E71 57A70442 A8DC5CDB CE8084BE
        6609817B 4479C300 2800FA7F 1AE23870 A111626E B73116C8


**************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


    w_i is
        9CEE8FCB 915311B3 70DD3599 14067376 F24D8568 000895E2
        B56CD255 3E468D26 B9171B62 21910E90 A290F051 1A6F7486


    W is
        9CEE8FCB 915311B3 70DD3599 14067376 F24D8568 000895E2
        B56CD255 3E468D26 B9171B62 21910E90 A290F051 1A6F7486


    ------------

    i = 2

    data is
                            DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0494


    w_i is
        E19F8EF6 44BFF873 2E1F022F 7CE483A8 E538E7B8 A979C647
```

```
        63128B4A 54B0D7E3 9ADCD785 FC94469B 2C02726A 55122901


    W is
        9CEE8FCB 915311B3 70DD3599 14067376 F24D8568 000895E2
        B56CD255 3E468D26 B9171B62 21910E90 A290F051 1A6F7486
        E19F8EF6 44BFF873 2E1F022F 7CE483A8 E538E7B8 A979C647
        63128B4A 54B0D7E3 9ADCD785 FC94469B 2C02726A 55122901


  returned_bits is
        9CEE8FCB 915311B3 70DD3599 14067376 F24D8568 000895E2
        B56CD255 3E468D26 B9171B62 21910E90 A290F051 1A6F7486
        E19F8EF6 44BFF873 2E1F022F 7CE483A8 E538E7B8 A979C647
        63128B4A 54B0D7E3 9ADCD785 FC94469B 2C02726A 55122901


---------------------------

  Update V

    0x03||V is
                           03DB62C0 8CB482A3 8AD2D4EA BC474050
        BDFB0D13 44FBE6BB 0F5BBBAF 716D2BDF 7DD3BA3B 46CE7890
        8F2DEC6B 263BD00F EBC329E4 9623AE49 92EADE0E 6BCDC36D
        E34B03FC 5CFD61A5 325582D2 9BC2780A 968CBB53 76004D70
        8BAE3B05 4F1CF829 25094C75 7AB0DAE5 E94BFCDC 9A5A0493


    H is
        7A5A7039 09050FFC 52DC3BF5 9896C6A5 34E03732 C39B5756
        EDA3A9F6 D53E815F 9738EB81 5AE6F94B F9A785CA 8D4FC634


  Updated values

  V is
                             FB3AC6 43C6BBDC BD8AC56F 2E7DF8FA
        2CCDA9FA 1178FF3B C7DDAF89 E89BB430 562A77D4 C52BD6CB
        AFA3D7C3 75D69E35 8B80A28F B0F33FBB 8CC69C53 50BD6798
        6BBA9C9E 304D997A FBBDED39 8C0042F2 74494F62 081C2985
        DF5B6677 68D53C88 E4433275 F07A0CA2 8404E515 DEDAE190


  reseed_counter is
                                                0000 00000002
```

```
rnd_val is
        9CEE8FCB 915311B3 70DD3599 14067376 F24D8568 000895E2
        B56CD255 3E468D26 B9171B62 21910E90 A290F051 1A6F7486
        E19F8EF6 44BFF873 2E1F022F 7CE483A8 E538E7B8 A979C647
        63128B4A 54B0D7E3 9ADCD785 FC94469B 2C02726A 55122901


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 768

  additional_input
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
---------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01FB 3AC643C6 BBDCBD8A C56F2E7D F8FA2CCD A9FA1178
        FF3BC7DD AF89E89B B430562A 77D4C52B D6CBAFA3 D7C375D6
        9E358B80 A28FB0F3 3FBB8CC6 9C5350BD 67986BBA 9C9E304D
        997AFBBD ED398C00 42F27449 4F62081C 2985DF5B 667768D5
        3C88E443 3275F07A 0CA28404 E515DEDA E190C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        037801FB 3AC643C6 BBDCBD8A C56F2E7D F8FA2CCD A9FA1178
        FF3BC7DD AF89E89B B430562A 77D4C52B D6CBAFA3 D7C375D6
        9E358B80 A28FB0F3 3FBB8CC6 9C5350BD 67986BBA 9C9E304D
        997AFBBD ED398C00 42F27449 4F62081C 2985DF5B 667768D5
        3C88E443 3275F07A 0CA28404 E515DEDA E190C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
Hash(counter||no_of_bits_to_return||input_string) is
    1C5C55A6 39ABE953 F81466FB 846F8CCC 974D024A CB68AA22
    11C29FA0 3D9766E7 6E5A87A0 805211E0 C28A85E7 82DE92FE


temp =
    1C5C55A6 39ABE953 F81466FB 846F8CCC 974D024A CB68AA22
    11C29FA0 3D9766E7 6E5A87A0 805211E0 C28A85E7 82DE92FE


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    037801FB 3AC643C6 BBDCBD8A C56F2E7D F8FA2CCD A9FA1178
    FF3BC7DD AF89E89B B430562A 77D4C52B D6CBAFA3 D7C375D6
    9E358B80 A28FB0F3 3FBB8CC6 9C5350BD 67986BBA 9C9E304D
    997AFBBD ED398C00 42F27449 4F62081C 2985DF5B 667768D5
    3C88E443 3275F07A 0CA28404 E515DEDA E190C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Hash(counter||no_of_bits_to_return||input_string) is
    0C89980C 03D37FC8 C9649303 3B5FF024 E3A13BD3 CB950C82
    42DAD044 CD1C4B3A ACE28237 4D967B21 4075B091 0E1FC16A


temp =
    1C5C55A6 39ABE953 F81466FB 846F8CCC 974D024A CB68AA22
    11C29FA0 3D9766E7 6E5A87A0 805211E0 C28A85E7 82DE92FE
    0C89980C 03D37FC8 C9649303 3B5FF024 E3A13BD3 CB950C82
    42DAD044 CD1C4B3A ACE28237 4D967B21 4075B091 0E1FC16A


------------
```

```
    i = 3

    counter||no_of_bits_to_return||input_string is
                                                          030000
        037801FB 3AC643C6 BBDCBD8A C56F2E7D F8FA2CCD A9FA1178
        FF3BC7DD AF89E89B B430562A 77D4C52B D6CBAFA3 D7C375D6
        9E358B80 A28FB0F3 3FBB8CC6 9C5350BD 67986BBA 9C9E304D
        997AFBBD ED398C00 42F27449 4F62081C 2985DF5B 667768D5
        3C88E443 3275F07A 0CA28404 E515DEDA E190C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    Hash(counter||no_of_bits_to_return||input_string) is
        DA59C63A 7AD92A5E 050568E6 2A96FA0F 16DE14AD 3E4597F1
        C9215E33 B203E5EC A0182C22 D2A34099 83219A8A A89B1666


    temp =
                            1C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


  V is
                            1C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


--------------------------

  Hash_df - Generate C - Step 4
```

```
0x00||V is
                      001C5C55 A639ABE9 53F81466 FB846F8C
    CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
    E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
    24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
    214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 001C5C55 A639ABE9 53F81466 FB846F8C
    CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
    E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
    24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
    214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


Hash(counter||no_of_bits_to_return||input_string) is
    143C078E 3B909E09 9399AB04 683F27CF B77221F7 BBB9720C
    1ED63F27 C6664449 B8536D54 35EFFA5F C13B937D 0FE423F5


temp =
    143C078E 3B909E09 9399AB04 683F27CF B77221F7 BBB9720C
    1ED63F27 C6664449 B8536D54 35EFFA5F C13B937D 0FE423F5


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 001C5C55 A639ABE9 53F81466 FB846F8C
    CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
    E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
    24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
    214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


Hash(counter||no_of_bits_to_return||input_string) is
    12176168 89B7B466 7CF9CAFA 266048EA 24BA75B7 9E9A8093
```

```
        E14C3AA1 A44F3007 5351D077 412E08A3 8BB9CE5A CAC9B822


    temp =
        143C078E 3B909E09 9399AB04 683F27CF B77221F7 BBB9720C
        1ED63F27 C6664449 B8536D54 35EFFA5F C13B937D 0FE423F5
        12176168 89B7B466 7CF9CAFA 266048EA 24BA75B7 9E9A8093
        E14C3AA1 A44F3007 5351D077 412E08A3 8BB9CE5A CAC9B822


    ------------

    i = 3

    counter||no_of_bits_to_return||input_string is
              03 00000378 001C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


    Hash(counter||no_of_bits_to_return||input_string) is
        F6D9E446 0241694F 2DD12B6C FB07BC69 C9022603 DCE63FA7
        FDAFCA3A B05C0F3B BA73DAB0 4E0E3977 F0C0BC0C DA52464C


    temp =
                            143C07 8E3B909E 099399AB 04683F27
        CFB77221 F7BBB972 0C1ED63F 27C66644 49B8536D 5435EFFA
        5FC13B93 7D0FE423 F5121761 6889B7B4 667CF9CA FA266048
        EA24BA75 B79E9A80 93E14C3A A1A44F30 075351D0 77412E08
        A38BB9CE 5ACAC9B8 22F6D9E4 46024169 4F2DD12B 6CFB07BC


  C is
                            143C07 8E3B909E 099399AB 04683F27
        CFB77221 F7BBB972 0C1ED63F 27C66644 49B8536D 5435EFFA
        5FC13B93 7D0FE423 F5121761 6889B7B4 667CF9CA FA266048
        EA24BA75 B79E9A80 93E14C3A A1A44F30 075351D0 77412E08
        A38BB9CE 5ACAC9B8 22F6D9E4 46024169 4F2DD12B 6CFB07BC


**************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 768

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 768

    ------------

    i = 1

    data is
                            1C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


    w_i is
        476727C7 96489765 62C987DA 997128A7 5CD23971 265F89E6
        65448938 1A619DE0 AB3E707E 2A071A47 FD5D5B09 2711A6E4


    W is
        476727C7 96489765 62C987DA 997128A7 5CD23971 265F89E6
        65448938 1A619DE0 AB3E707E 2A071A47 FD5D5B09 2711A6E4


    ------------

    i = 2

    data is
                            1C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FB


    w_i is
```

```
        69E20CEE 2F5A18DE E45988E5 A02EA991 40DB6EB6 F74B703D
        1D56C025 08AF1E8E 6033B480 26CED342 C0A0FF4C 00DE1DE5


    W is
        476727C7 96489765 62C987DA 997128A7 5CD23971 265F89E6
        65448938 1A619DE0 AB3E707E 2A071A47 FD5D5B09 2711A6E4
        69E20CEE 2F5A18DE E45988E5 A02EA991 40DB6EB6 F74B703D
        1D56C025 08AF1E8E 6033B480 26CED342 C0A0FF4C 00DE1DE5


  returned_bits is
        476727C7 96489765 62C987DA 997128A7 5CD23971 265F89E6
        65448938 1A619DE0 AB3E707E 2A071A47 FD5D5B09 2711A6E4
        69E20CEE 2F5A18DE E45988E5 A02EA991 40DB6EB6 F74B703D
        1D56C025 08AF1E8E 6033B480 26CED342 C0A0FF4C 00DE1DE5


--------------------------

  Update V

    0x03||V is
                          031C5C55 A639ABE9 53F81466 FB846F8C
        CC974D02 4ACB68AA 2211C29F A03D9766 E76E5A87 A0805211
        E0C28A85 E782DE92 FE0C8998 0C03D37F C8C96493 033B5FF0
        24E3A13B D3CB950C 8242DAD0 44CD1C4B 3AACE282 374D967B
        214075B0 910E1FC1 6ADA59C6 3A7AD92A 5E050568 E62A96FA


    H is
        858F0D53 6D7F0A1D E63050A9 8502F779 3800C351 9083D52C
        B182332F 1C7D372C 586404E6 6940B71D D0EAF869 6ECF536D


  Updated values

  V is
                            30985D 34753C87 5D8BAE11 FFECAEB4
        9C4EBF24 4287221C 2E3098DE C803FDAB 3126ADF4 F4B6420C
        4083C619 6492C2B6 F31EA0F9 748D8B34 2F465E5D FD61C039
        94976904 F8E939AA FC5477B4 6B7462F4 7A00F7A4 3F1299B0
        764E62AE 085620A5 E6353890 E9BDD1B1 7E1DCEFD C1F4F224


  reseed_counter is
```

0000 00000002

rnd_val is
476727C7 96489765 62C987DA 997128A7 5CD23971 265F89E6
65448938 1A619DE0 AB3E707E 2A071A47 FD5D5B09 2711A6E4
69E20CEE 2F5A18DE E45988E5 A02EA991 40DB6EB6 F74B703D
1D56C025 08AF1E8E 6033B480 26CED342 C0A0FF4C 00DE1DE5

```
################################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                           20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                    01000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                      152D908B 0EDF7253 D5D19F0A F96518D3
    AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
    BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


temp =
                      152D908B 0EDF7253 D5D19F0A F96518D3
    AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
    BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                02000003 78000102 03040506
    0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
    1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
    3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


Hash(counter||no_of_bits_to_return||input_string) is
                      D466C1D9 AC010D21 B28CD9FD 124DF56D
    4D3B75B9 604827B3 CF49928E C4DA204F C374888E 278C0319
    DB45E1FD 3BCAD38C C355D2D6 55C1D606 60AEA6D6 BBE4E7C1


temp =
                        152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


V is
                        152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    Hash(counter||no_of_bits_to_return||input_string) is
                          2B22189F 32CB92C1 508BC343 69B8C37F
        D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
        10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


    temp =
                          2B22189F 32CB92C1 508BC343 69B8C37F
        D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
        10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
```

```
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    Hash(counter||no_of_bits_to_return||input_string) is
                         051F8441 D411B910 71605B9A 44B6643E
        67225358 2AE3148F 4A57E8FD A8E81155 108E4AFC C0E939BF
        D95FAB62 E8B1E4FD BDA34B60 C9220A37 EC6BD096 A6DAE159


    temp =
                           2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


  C is
                           2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------
```

```
i = 1

data is
                        152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


w_i is
                      170CC707 C71C69CE 45C43CBA FF521014
    0572D478 59521BA1 3141BADD 2E5B9A7B 3E802062 5CD8893F
    D6A4739C 581ED5BE 7FA3148A 05D7F54A E9EADAE8 F1A7194D


W is
                      170CC707 C71C69CE 45C43CBA FF521014
    0572D478 59521BA1 3141BADD 2E5B9A7B 3E802062 5CD8893F
    D6A4739C 581ED5BE 7FA3148A 05D7F54A E9EADAE8 F1A7194D


------------

i = 2

data is
                        152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD4


w_i is
                      F94B6B75 5B948E0C 27E1747F 02F663D6
    B514A0F5 86F94E53 D32169E1 CCC6211A D0348124 19B6BA8F
    3C829304 898393BF 39E57E2F EDF775FC 6E5EB0E3 07EDCA0B


W is
                                          170CC707 C71C69CE
    45C43CBA FF521014 0572D478 59521BA1 3141BADD 2E5B9A7B
    3E802062 5CD8893F D6A4739C 581ED5BE 7FA3148A 05D7F54A
    E9EADAE8 F1A7194D F94B6B75 5B948E0C 27E1747F 02F663D6
    B514A0F5 86F94E53 D32169E1 CCC6211A D0348124 19B6BA8F
```

```
       3C829304 898393BF 39E57E2F EDF775FC 6E5EB0E3 07EDCA0B


  returned_bits is
                                                 170CC707 C71C69CE
       45C43CBA FF521014 0572D478 59521BA1 3141BADD 2E5B9A7B
       3E802062 5CD8893F D6A4739C 581ED5BE 7FA3148A 05D7F54A
       E9EADAE8 F1A7194D F94B6B75 5B948E0C 27E1747F 02F663D6
       B514A0F5 86F94E53 D32169E1 CCC6211A D0348124 19B6BA8F
       3C829304 898393BF 39E57E2F EDF775FC 6E5EB0E3 07EDCA0B


--------------------------

  Update V

    0x03||V is
                          03152D90 8B0EDF72 53D5D19F 0AF96518
       D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
       67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
       6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
       B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    H is
                          DB1068C4 546A551B 34DEFD9B 7C714A81
       3F648F40 D44A98B7 C5E730ED D5CB6EC3 B665FCA6 9A490F4F
       7C033201 72F4A20D 632C24D0 A0833718 A57BAA63 AA2E269E


  Updated values

  V is
                            404FA9 2A41AB05 15265D62 4E631DDC
       53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
       DCCC30B4 5663EE69 55855C39 C8D0799F AC40384C D78E1C46
       803E1586 EFCAAB7D F80B1E23 6D22731D 621A5A6F ABD43A8B
       BF1CD37C FF62643F 080027A4 2B6BAC55 7F304FF1 0A52A356


  reseed_counter is
                                                     0000 00000002


rnd_val is
                                                 170CC707 C71C69CE
```

```
        45C43CBA FF521014 0572D478 59521BA1 3141BADD 2E5B9A7B
        3E802062 5CD8893F D6A4739C 581ED5BE 7FA3148A 05D7F54A
        E9EADAE8 F1A7194D F94B6B75 5B948E0C 27E1747F 02F663D6
        B514A0F5 86F94E53 D32169E1 CCC6211A D0348124 19B6BA8F
        3C829304 898393BF 39E57E2F EDF775FC 6E5EB0E3 07EDCA0B


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                          404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 55855C39 C8D0799F AC40384C D78E1C46
        803E1586 EFCAAB7D F80B1E23 6D22731D 621A5A6F ABD43A8B
        BF1CD37C FF62643F 080027A4 2B6BAC55 7F304FF1 0A52A356


    w_i is
                         D515B92B 1811F5AA D02AAC9B 39DFA5B8
        B1A95048 7D3429B1 081D0FEC 28D57686 D85BC6B4 5AB8B84C
        54DD80B2 82591F55 07ED9B3F B1CDEEFD 58AD5A98 12ED929C


    W is
                         D515B92B 1811F5AA D02AAC9B 39DFA5B8
        B1A95048 7D3429B1 081D0FEC 28D57686 D85BC6B4 5AB8B84C
```

```
        54DD80B2 82591F55 07ED9B3F B1CDEEFD 58AD5A98 12ED929C


    ------------

    i = 2

    data is
                            404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 55855C39 C8D0799F AC40384C D78E1C46
        803E1586 EFCAAB7D F80B1E23 6D22731D 621A5A6F ABD43A8B
        BF1CD37C FF62643F 080027A4 2B6BAC55 7F304FF1 0A52A357


    w_i is
                          779B0F54 BADF2CAF BACFACB3 ECACC127
        C7640CBB 67154F54 5A622BE0 A9B552A2 4208313B FA491F53
        AAA3074B DC48BC5B DB3FF0E2 D05BB477 B59F87E3 A1EAB3E6


    W is
                                             D515B92B 1811F5AA
        D02AAC9B 39DFA5B8 B1A95048 7D3429B1 081D0FEC 28D57686
        D85BC6B4 5AB8B84C 54DD80B2 82591F55 07ED9B3F B1CDEEFD
        58AD5A98 12ED929C 779B0F54 BADF2CAF BACFACB3 ECACC127
        C7640CBB 67154F54 5A622BE0 A9B552A2 4208313B FA491F53
        AAA3074B DC48BC5B DB3FF0E2 D05BB477 B59F87E3 A1EAB3E6


  returned_bits is
                                             D515B92B 1811F5AA
        D02AAC9B 39DFA5B8 B1A95048 7D3429B1 081D0FEC 28D57686
        D85BC6B4 5AB8B84C 54DD80B2 82591F55 07ED9B3F B1CDEEFD
        58AD5A98 12ED929C 779B0F54 BADF2CAF BACFACB3 ECACC127
        C7640CBB 67154F54 5A622BE0 A9B552A2 4208313B FA491F53
        AAA3074B DC48BC5B DB3FF0E2 D05BB477 B59F87E3 A1EAB3E6


--------------------------

  Update V

    0x03||V is
                          03404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
```

```
        DCCC30B4 5663EE69 55855C39 C8D0799F AC40384C D78E1C46
        803E1586 EFCAAB7D F80B1E23 6D22731D 621A5A6F ABD43A8B
        BF1CD37C FF62643F 080027A4 2B6BAC55 7F304FF1 0A52A356


    H is
                         21A210E7 77772CDB 2F0C82FD 86A05AA6
        691E02D8 DCCC8546 F427A69B FFF1CA7B 189EB235 85E48648
        64134F01 F2824DD7 92BBBA16 5B61BB5E A840C4DC AA129622


  Updated values

  V is
                           6B71C1 C9747697 D676E925 91CCD69F
        D35FE672 A309FF0B 7C5F7694 A93D29D6 7D50246C 82A3D38D
        51DCEED3 BB0B991E CEBF8E3A A046A9D2 A7A12015 23FEED42
        BF6137E4 0E6B427D FCA4251B 0758F3FC B9202EF8 89E3A3E8
        B27A7A67 EF8D9A27 EFCC7005 838E50ED E74A7479 174DEB5E


  reseed_counter is
                                                0000 00000003


rnd_val is
                                              D515B92B 1811F5AA
        D02AAC9B 39DFA5B8 B1A95048 7D3429B1 081D0FEC 28D57686
        D85BC6B4 5AB8B84C 54DD80B2 82591F55 07ED9B3F B1CDEEFD
        58AD5A98 12ED929C 779B0F54 BADF2CAF BACFACB3 ECACC127
        C7640CBB 67154F54 5A622BE0 A9B552A2 4208313B FA491F53
        AAA3074B DC48BC5B DB3FF0E2 D05BB477 B59F87E3 A1EAB3E6


##################################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                           000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
```

```
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

################################################################

****************************************************************
```

```
Hash_DRBG_Instantiate_algorithm

    entropy_input is
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                   01000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F
```

```
  Hash(counter||no_of_bits_to_return||input_string) is
                        152D908B 0EDF7253 D5D19F0A F96518D3
      AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
      BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


  temp =
                        152D908B 0EDF7253 D5D19F0A F96518D3
      AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
      BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
                                02000003 78000102 03040506
      0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
      1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
      3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
      4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
      6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                        D466C1D9 AC010D21 B28CD9FD 124DF56D
      4D3B75B9 604827B3 CF49928E C4DA204F C374888E 278C0319
      DB45E1FD 3BCAD38C C355D2D6 55C1D606 60AEA6D6 BBE4E7C1


  temp =
                          152D90 8B0EDF72 53D5D19F 0AF96518
      D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
      67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
      6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
      B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


V is
                          152D90 8B0EDF72 53D5D19F 0AF96518
      D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
      67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
      6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
      B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3
```

```
---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    Hash(counter||no_of_bits_to_return||input_string) is
                          2B22189F 32CB92C1 508BC343 69B8C37F
        D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
        10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


    temp =
                          2B22189F 32CB92C1 508BC343 69B8C37F
        D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
        10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
```

```
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


    Hash(counter||no_of_bits_to_return||input_string) is
                            051F8441 D411B910 71605B9A 44B6643E
        67225358 2AE3148F 4A57E8FD A8E81155 108E4AFC C0E939BF
        D95FAB62 E8B1E4FD BDA34B60 C9220A37 EC6BD096 A6DAE159


    temp =
                              2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


  C is
                              2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                              606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
---------------------------

  Process additional_input

    0x02||V||additional_input is
                                                 02152D 908B0EDF
        7253D5D1 9F0AF965 18D3AD33 F2EF3151 A0C956D9 D3EE6DC0
        8B70F1EB 75982501 CE67BB72 94F1BC43 B322DCD2 5C146721
        2CAB0CD5 E6954C5B 6F6AD466 C1D9AC01 0D21B28C D9FD124D
        F56D4D3B 75B96048 27B3CF49 928EC4DA 204FC374 888E278C
        0319DB45 E1FD3BCA D3606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    w=Hash(0x02||V||additional_input) is
                          79FD8B26 36E78437 378D4914 89E1A32D
        D89A9B62 4AD030DD E1748E57 D996D7DB 727AF114 4808A659
        52CBF908 7F4379BC 9DB1D25B 78D27EC8 BDC583D7 63C3122E


    V is
                            152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 9CDA5D82 4B4EA563 E29A1EFB 1F2DFE9D
        436F0224 247C31EB 03271B31 D6A925D0 DFC82C8A 0168EE81
        069B429B 0E0853DC ED7546E4 06FA0ACB D7A0C9B9 60FEDD01


---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 9CDA5D82 4B4EA563 E29A1EFB 1F2DFE9D
        436F0224 247C31EB 03271B31 D6A925D0 DFC82C8A 0168EE81
```

```
    069B429B 0E0853DC ED7546E4 06FA0ACB D7A0C9B9 60FEDD01


  w_i is
                       3EF283D8 E1A5F5A8 D5D8AD9C 45577576
    DD018161 387C97B3 2EB5A104 A9649E9E DC85F9E4 DF40A823
    A66E5494 CB3FB655 99D81A02 E415704C A738D2C8 D5020C42


  W is
                       3EF283D8 E1A5F5A8 D5D8AD9C 45577576
    DD018161 387C97B3 2EB5A104 A9649E9E DC85F9E4 DF40A823
    A66E5494 CB3FB655 99D81A02 E415704C A738D2C8 D5020C42


  ------------

  i = 2

  data is
                         152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 9CDA5D82 4B4EA563 E29A1EFB 1F2DFE9D
    436F0224 247C31EB 03271B31 D6A925D0 DFC82C8A 0168EE81
    069B429B 0E0853DC ED7546E4 06FA0ACB D7A0C9B9 60FEDD02


  w_i is
                       08F364A8 750251A8 74AF6FFD 88638094
    8B7138A6 81E093B5 32A6E67E 9F3AC97E 1364A1E2 BC8E1121
    5771CA69 4D933FCF 86CD3500 121AD1AF 66821B61 92BE3C97


  W is
                                          3EF283D8 E1A5F5A8
    D5D8AD9C 45577576 DD018161 387C97B3 2EB5A104 A9649E9E
    DC85F9E4 DF40A823 A66E5494 CB3FB655 99D81A02 E415704C
    A738D2C8 D5020C42 08F364A8 750251A8 74AF6FFD 88638094
    8B7138A6 81E093B5 32A6E67E 9F3AC97E 1364A1E2 BC8E1121
    5771CA69 4D933FCF 86CD3500 121AD1AF 66821B61 92BE3C97


returned_bits is
                                          3EF283D8 E1A5F5A8
    D5D8AD9C 45577576 DD018161 387C97B3 2EB5A104 A9649E9E
    DC85F9E4 DF40A823 A66E5494 CB3FB655 99D81A02 E415704C
```

```
        A738D2C8 D5020C42 08F364A8 750251A8 74AF6FFD 88638094
        8B7138A6 81E093B5 32A6E67E 9F3AC97E 1364A1E2 BC8E1121
        5771CA69 4D933FCF 86CD3500 121AD1AF 66821B61 92BE3C97


---------------------------

  Update V

    0x03||V is
                          03152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 9CDA5D82 4B4EA563 E29A1EFB 1F2DFE9D
        436F0224 247C31EB 03271B31 D6A925D0 DFC82C8A 0168EE81
        069B429B 0E0853DC ED7546E4 06FA0ACB D7A0C9B9 60FEDD01


    H is
                          E2C0A9BB 3EF85708 AA5C141C 81558C82
        383E2BB6 27DAE468 AB6C9849 CC42948C 7068AD57 D722FDCF
        AA7FE7D4 C792F1A1 0FA378F9 21534BAE 4F52B5CE 6E324F13


  Updated values

  V is
                            404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 D7332856 EA45FFC4 594A97E2 66540175
        51B24D5E 8E2B280C BF0513D7 3D3070C1 8E97FC35 30B6CF65
        40658258 D3442D8F 52294E28 250E3FB3 E6CCDF33 3219DDF9


  reseed_counter is
                                                0000 00000002


rnd_val is
                                             3EF283D8 E1A5F5A8
        D5D8AD9C 45577576 DD018161 387C97B3 2EB5A104 A9649E9E
        DC85F9E4 DF40A823 A66E5494 CB3FB655 99D81A02 E415704C
        A738D2C8 D5020C42 08F364A8 750251A8 74AF6FFD 88638094
        8B7138A6 81E093B5 32A6E67E 9F3AC97E 1364A1E2 BC8E1121
        5771CA69 4D933FCF 86CD3500 121AD1AF 66821B61 92BE3C97
```

```
-----------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


---------------------------

  Process additional_input

    0x02||V||additional_input is
                                              02404F A92A41AB
        0515265D 624E631D DC53868D 32C91DA8 5622DB28 344BD575
        30F72107 F10D646A ADDCCC30 B45663EE 69D73328 56EA45FF
        C4594A97 E2665401 7551B24D 5E8E2B28 0CBF0513 D73D3070
        C18E97FC 3530B6CF 65406582 58D3442D 8F52294E 28250E3F
        B3E6CCDF 333219DD F9A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    w=Hash(0x02||V||additional_input) is
                         16873523 6B8FA61E 40744598 B64BD50D
        F278C925 8E1A8849 E2EA3F54 70867ABA D5E797B3 C459A0F2
        64B9F8F8 8B5500D6 FDDB804E 6ED9134E EA77C7BF B255702F


    V is
                           404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 EDBA5D7A 55D5A5E2 99BEDD7B 1C9FD683
        442B1684 1C45B056 A1EF532B ADB6EB7C 647F93E8 F5107057
```

```
        A51F7B51 5E992E66 5004CE76 93E75302 D144A6F2 E46F4E28


---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 EDBA5D7A 55D5A5E2 99BEDD7B 1C9FD683
        442B1684 1C45B056 A1EF532B ADB6EB7C 647F93E8 F5107057
        A51F7B51 5E992E66 5004CE76 93E75302 D144A6F2 E46F4E28


    w_i is
                           8EB0575C E1500BB0 52259F8A 995DC7AE
        F54FBD38 E9CE6AEA F3F05FA7 0768AF36 99A24D90 BF60E3E6
        509B4326 A5473B2C E98DE137 DB06EF9F 03A125BF 1367DEFB


    W is
                           8EB0575C E1500BB0 52259F8A 995DC7AE
        F54FBD38 E9CE6AEA F3F05FA7 0768AF36 99A24D90 BF60E3E6
        509B4326 A5473B2C E98DE137 DB06EF9F 03A125BF 1367DEFB


    ------------

    i = 2

    data is
                            404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 EDBA5D7A 55D5A5E2 99BEDD7B 1C9FD683
        442B1684 1C45B056 A1EF532B ADB6EB7C 647F93E8 F5107057
        A51F7B51 5E992E66 5004CE76 93E75302 D144A6F2 E46F4E29


    w_i is
```

```
                        8098633F A2EF8493 454F6792 F1F94C52
        5282EEC9 D0352D93 B966966B AA85DBAC 596B3240 E2E28D35
        E71E7B73 05C92473 AE706480 E9061CD8 DA37F147 700B67B8


    W is
                                              8EB0575C E1500BB0
        52259F8A 995DC7AE F54FBD38 E9CE6AEA F3F05FA7 0768AF36
        99A24D90 BF60E3E6 509B4326 A5473B2C E98DE137 DB06EF9F
        03A125BF 1367DEFB 8098633F A2EF8493 454F6792 F1F94C52
        5282EEC9 D0352D93 B966966B AA85DBAC 596B3240 E2E28D35
        E71E7B73 05C92473 AE706480 E9061CD8 DA37F147 700B67B8


  returned_bits is
                                              8EB0575C E1500BB0
        52259F8A 995DC7AE F54FBD38 E9CE6AEA F3F05FA7 0768AF36
        99A24D90 BF60E3E6 509B4326 A5473B2C E98DE137 DB06EF9F
        03A125BF 1367DEFB 8098633F A2EF8493 454F6792 F1F94C52
        5282EEC9 D0352D93 B966966B AA85DBAC 596B3240 E2E28D35
        E71E7B73 05C92473 AE706480 E9061CD8 DA37F147 700B67B8


---------------------------

  Update V

    0x03||V is
                        03404FA9 2A41AB05 15265D62 4E631DDC
        53868D32 C91DA856 22DB2834 4BD57530 F72107F1 0D646AAD
        DCCC30B4 5663EE69 EDBA5D7A 55D5A5E2 99BEDD7B 1C9FD683
        442B1684 1C45B056 A1EF532B ADB6EB7C 647F93E8 F5107057
        A51F7B51 5E992E66 5004CE76 93E75302 D144A6F2 E46F4E28


    H is
                        A2513F21 58ED78EB 67F6DA75 18BA4DEA
        E2E65C34 302C18FC 88A55FD2 0D84168D FF0297D3 D129D4B7
        B0B35603 CE3C2BDF 5E7A617D 5EC2FAC6 049C7270 C0C39507


  Updated values

  V is
                          6B71C1 C9747697 D676E925 91CCD69F
        D35FE672 A309FF0B 7C5F7694 A93D29D6 7D50246C 82A3D38D
```

```
        51DCEED3 BB0B991F E7A3BDB5 0EC22225 CE0A1CBA FB2A9AC3
        FD16923C 8E45DB0C 3B061359 557FB86E A1E94E10 1E652823
        E51D293E 2A7E4257 038FBE3E EF6B3702 95BA790F 081B9515


  reseed_counter is
                                                 0000 00000003


rnd_val is
                                               8EB0575C E1500BB0
        52259F8A 995DC7AE F54FBD38 E9CE6AEA F3F05FA7 0768AF36
        99A24D90 BF60E3E6 509B4326 A5473B2C E98DE137 DB06EF9F
        03A125BF 1367DEFB 8098633F A2EF8493 454F6792 F1F94C52
        5282EEC9 D0352D93 B966966B AA85DBAC 596B3240 E2E28D35
        E71E7B73 05C92473 AE706480 E9061CD8 DA37F147 700B67B8


################################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
```

```
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"
```

```
---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
                          E5A5C585 D6A9E11C 58581F35 14EE19A7
        048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
        7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


    temp =
                          E5A5C585 D6A9E11C 58581F35 14EE19A7
```

```
        048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
        7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                                        020000
        03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
                          80B87195 7508538D 2D87A4A3 B5728ADB
        4191974A 384F323D 2E585869 5C152F99 D0E8CF4C B41BC2A6
        12955B4C 4838B9FB EB00568D 36F727E1 742FF774 E8542A4B


    temp =
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


  V is
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


--------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                       00E5A5C5 85D6A9E1 1C58581F 3514EE19
      A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
      A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
      EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
      3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


  no_of_bits_to_return = 888

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
            01 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
      A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
      A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
      EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
      3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


  Hash(counter||no_of_bits_to_return||input_string) is
                       0C193DBC 1942C121 C63513ED 95ECA91C
      62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
      421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


  temp =
                       0C193DBC 1942C121 C63513ED 95ECA91C
      62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
      421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
            02 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
      A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
      A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
      EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
      3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                          0176FE93 A4C199A2 258615DD A840AE6F
        C2E7DB39 1315119E 57774F94 396C81F5 F8D4835D 618D960B
        297E97F1 A21B35E3 E450A877 4819D918 961DFC01 FFC73630


    temp =
                            0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


  C is
                            0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


---------------------------------------------------------------

First call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1
```

```
data is
                        E5A5C5 85D6A9E1 1C58581F 3514EE19
    A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
    A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
    EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
    3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


w_i is
                      B72E446C 3985DA7B F5009134 C2C59BAF
    7918AEA7 27FAC3CA 39C31DD6 45357AC9 168DA218 027BD5D8
    642C1306 895765A0 4757EF52 F4D81C55 8DE70751 3FE96C08


W is
                      B72E446C 3985DA7B F5009134 C2C59BAF
    7918AEA7 27FAC3CA 39C31DD6 45357AC9 168DA218 027BD5D8
    642C1306 895765A0 4757EF52 F4D81C55 8DE70751 3FE96C08


------------

i = 2

data is
                        E5A5C5 85D6A9E1 1C58581F 3514EE19
    A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
    A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
    EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
    3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838BA


w_i is
                      56E390B1 45F5B016 A3649D07 A1A9F5C6
    DF1E27A8 830451DB FA12AB97 70A998D7 AD7D3EB3 488328FF
    874E6C12 94A60539 199C9A99 C75BFE5F A0446DAE 248E0DCB


W is
                                        B72E446C 3985DA7B
    F5009134 C2C59BAF 7918AEA7 27FAC3CA 39C31DD6 45357AC9
    168DA218 027BD5D8 642C1306 895765A0 4757EF52 F4D81C55
    8DE70751 3FE96C08 56E390B1 45F5B016 A3649D07 A1A9F5C6
    DF1E27A8 830451DB FA12AB97 70A998D7 AD7D3EB3 488328FF
    874E6C12 94A60539 199C9A99 C75BFE5F A0446DAE 248E0DCB
```

```
  returned_bits is
                                                B72E446C 3985DA7B
        F5009134 C2C59BAF 7918AEA7 27FAC3CA 39C31DD6 45357AC9
        168DA218 027BD5D8 642C1306 895765A0 4757EF52 F4D81C55
        8DE70751 3FE96C08 56E390B1 45F5B016 A3649D07 A1A9F5C6
        DF1E27A8 830451DB FA12AB97 70A998D7 AD7D3EB3 488328FF
        874E6C12 94A60539 199C9A99 C75BFE5F A0446DAE 248E0DCB


---------------------------

  Update V

    0x03||V is
                          03E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    H is
                          BBC2684F FBE0AA6C E4E6F228 15A9A70E
        B8B8749B 143EAC0C EEB60CAF F29BC1D7 3B76C880 78C8D124
        ABD77981 93EB39CE 0AC5380A 7A5F0F30 4559F487 AE775A58


  Updated values

  V is
                            F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 6E244CC6 FF2B5779 15C97AE3 D6545183
        1E3AA40B 3D5875FA 1E091A6A 73F97510 867B41F2 FC143568
        875D4929 9180BB7F 9A8EF55D 2474B888 F696087A EC61AE47


  reseed_counter is
                                                    0000 00000002


rnd_val is
                                                B72E446C 3985DA7B
        F5009134 C2C59BAF 7918AEA7 27FAC3CA 39C31DD6 45357AC9
        168DA218 027BD5D8 642C1306 895765A0 4757EF52 F4D81C55
```

```
        8DE70751 3FE96C08 56E390B1 45F5B016 A3649D07 A1A9F5C6
        DF1E27A8 830451DB FA12AB97 70A998D7 AD7D3EB3 488328FF
        874E6C12 94A60539 199C9A99 C75BFE5F A0446DAE 248E0DCB


---------------------------------------------------------------

Second call to Generate

***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                           F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 6E244CC6 FF2B5779 15C97AE3 D6545183
        1E3AA40B 3D5875FA 1E091A6A 73F97510 867B41F2 FC143568
        875D4929 9180BB7F 9A8EF55D 2474B888 F696087A EC61AE47


    w_i is
                         557C2284 16B46E30 A3E703F6 A5270130
        7003615D 0DFCD1D4 F5E1F147 BAB4461F 4AF69FE4 13AAA932
        F537BA0B BEF93FA0 BA6EE187 8B86312A E9259DEC 73D73F27


    W is
                         557C2284 16B46E30 A3E703F6 A5270130
        7003615D 0DFCD1D4 F5E1F147 BAB4461F 4AF69FE4 13AAA932
        F537BA0B BEF93FA0 BA6EE187 8B86312A E9259DEC 73D73F27
```

```
    ------------

    i = 2

    data is
                            F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 6E244CC6 FF2B5779 15C97AE3 D6545183
        1E3AA40B 3D5875FA 1E091A6A 73F97510 867B41F2 FC143568
        875D4929 9180BB7F 9A8EF55D 2474B888 F696087A EC61AE48


    w_i is
                           345DFCFC F7D18E29 CF66DE2C 0615AF35
        A6C9218C E1EF2DA9 4C865A47 7A64FAC3 9D21D344 F19F8344
        53C68BC1 5FD929B2 B9B32D71 0E145F08 DA0FBD5E 0924061C


    W is
                                              557C2284 16B46E30
        A3E703F6 A5270130 7003615D 0DFCD1D4 F5E1F147 BAB4461F
        4AF69FE4 13AAA932 F537BA0B BEF93FA0 BA6EE187 8B86312A
        E9259DEC 73D73F27 345DFCFC F7D18E29 CF66DE2C 0615AF35
        A6C9218C E1EF2DA9 4C865A47 7A64FAC3 9D21D344 F19F8344
        53C68BC1 5FD929B2 B9B32D71 0E145F08 DA0FBD5E 0924061C


  returned_bits is
                                              557C2284 16B46E30
        A3E703F6 A5270130 7003615D 0DFCD1D4 F5E1F147 BAB4461F
        4AF69FE4 13AAA932 F537BA0B BEF93FA0 BA6EE187 8B86312A
        E9259DEC 73D73F27 345DFCFC F7D18E29 CF66DE2C 0615AF35
        A6C9218C E1EF2DA9 4C865A47 7A64FAC3 9D21D344 F19F8344
        53C68BC1 5FD929B2 B9B32D71 0E145F08 DA0FBD5E 0924061C


---------------------------

  Update V

    0x03||V is
                           03F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 6E244CC6 FF2B5779 15C97AE3 D6545183
        1E3AA40B 3D5875FA 1E091A6A 73F97510 867B41F2 FC143568
```

```
        875D4929 9180BB7F 9A8EF55D 2474B888 F696087A EC61AE47


    H is
                            58EB8BE5 2DA8F5EC 0D2DDCF9 B0FF4F6C
        3445EDCC FC8549EF DAC23C18 C5186B2B 0AB36AC6 89C6A2B1
        A7C06102 8BD219DE 86891787 9EE72862 8E008E8B 5F193920


  Updated values

  V is
                              FDD840 FE092F63 5FE4C247 1040C76B
        DFCA1790 F98DF63D 92692289 5F9A75EE AF1627BF A83C4D7D
        1C00B5BD 33D09A5E 403E1181 6071AE0F 46F9EABE BBF5EA94
        C98208D6 CD828183 9AF0DC99 16BA20EA 00F19494 BEEDED2B
        CD75217B B18C41E0 1710E168 20BD6E81 8FC0159E 3D1D029E


  reseed_counter is
                                                  0000 00000003


rnd_val is
                                               557C2284 16B46E30
        A3E703F6 A5270130 7003615D 0DFCD1D4 F5E1F147 BAB4461F
        4AF69FE4 13AAA932 F537BA0B BEF93FA0 BA6EE187 8B86312A
        E9259DEC 73D73F27 345DFCFC F7D18E29 CF66DE2C 0615AF35
        A6C9218C E1EF2DA9 4C865A47 7A64FAC3 9D21D344 F19F8344
        53C68BC1 5FD929B2 B9B32D71 0E145F08 DA0FBD5E 0924061C


##############################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
```

```
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                         808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                         C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                       20212223 24252627 28292A2B 2C2D2E2F


PersonalizationString =
                         404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                         606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


AdditionalInput2 =
                         A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                             404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                        010000
    03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
                      E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


temp =
                      E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
                          80B87195 7508538D 2D87A4A3 B5728ADB
        4191974A 384F323D 2E585869 5C152F99 D0E8CF4C B41BC2A6
        12955B4C 4838B9FB EB00568D 36F727E1 742FF774 E8542A4B


    temp =
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


  V is
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
```

```
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    Hash(counter||no_of_bits_to_return||input_string) is
                            0C193DBC 1942C121 C63513ED 95ECA91C
        62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
        421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


    temp =
                            0C193DBC 1942C121 C63513ED 95ECA91C
        62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
        421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    Hash(counter||no_of_bits_to_return||input_string) is
                            0176FE93 A4C199A2 258615DD A840AE6F
        C2E7DB39 1315119E 57774F94 396C81F5 F8D4835D 618D960B
        297E97F1 A21B35E3 E450A877 4819D918 961DFC01 FFC73630


    temp =
                              0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


C is
                            0C193D BC1942C1 21C63513 ED95ECA9
```

```
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


--------------------------

  Process additional_input

    0x02||V||additional_input is
                                              02E5A5 C585D6A9
        E11C5858 1F3514EE 19A7048C F096A3E9 B139D9C0 A2C06793
        10414073 C104E2F6 F8A37C7C 666E11FF 443933AB A1CFAD4C
        620CDFF5 DA8C0860 CEEE80B8 71957508 538D2D87 A4A3B572
        8ADB4191 974A384F 323D2E58 58695C15 2F99D0E8 CF4CB41B
        C2A61295 5B4C4838 B9606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    w=Hash(0x02||V||additional_input) is
                          45751730 26074982 F90C7520 DCB4E495
        C5560C97 F73D6910 A6DD9382 06980B1B 59811FF1 2923D007
        9CBCA198 7ADA2DBB D41C17E6 6D8CBA09 1EA4006D 10B606BE
```

```
    V is
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 7EA8C2D1 F5B495E5 05EC6AFB 68BD4564
        B3D6C509 8CB27164 340B1B26 AA4D7DA6 34C2B188 735C1F39
        D9EAF9F0 E43642EB 6DED00B5 BA40D5CB C4B695C8 5CFE3F77


---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 7EA8C2D1 F5B495E5 05EC6AFB 68BD4564
        B3D6C509 8CB27164 340B1B26 AA4D7DA6 34C2B188 735C1F39
        D9EAF9F0 E43642EB 6DED00B5 BA40D5CB C4B695C8 5CFE3F77


    w_i is
                           DA126CF9 5C6BF97E 2F731F21 37A907AC
        C70FD7AC 9EBACD1C 6E31C740 29B052E3 AABC48F3 B00993F2
        B2381F76 50A55322 A968C86E 05DE88E6 367F6EF8 9A601DB4


    W is
                           DA126CF9 5C6BF97E 2F731F21 37A907AC
        C70FD7AC 9EBACD1C 6E31C740 29B052E3 AABC48F3 B00993F2
        B2381F76 50A55322 A968C86E 05DE88E6 367F6EF8 9A601DB4


    ------------

    i = 2

    data is
                            E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
```

```
        A37C7C66 6E11FF44 7EA8C2D1 F5B495E5 05EC6AFB 68BD4564
        B3D6C509 8CB27164 340B1B26 AA4D7DA6 34C2B188 735C1F39
        D9EAF9F0 E43642EB 6DED00B5 BA40D5CB C4B695C8 5CFE3F78


    w_i is
                         342E9086 C7AC13B5 E56C32E9 E668040B
        73847893 C5BFD38A 1CF44F34 8B4EEE4C D68ADB7E 7B8C837F
        19BC4F90 2761F7CF F24AB1D7 04FD11C4 E929D855 3753B55D


    W is
                                           DA126CF9 5C6BF97E
        2F731F21 37A907AC C70FD7AC 9EBACD1C 6E31C740 29B052E3
        AABC48F3 B00993F2 B2381F76 50A55322 A968C86E 05DE88E6
        367F6EF8 9A601DB4 342E9086 C7AC13B5 E56C32E9 E668040B
        73847893 C5BFD38A 1CF44F34 8B4EEE4C D68ADB7E 7B8C837F
        19BC4F90 2761F7CF F24AB1D7 04FD11C4 E929D855 3753B55D


  returned_bits is
                                           DA126CF9 5C6BF97E
        2F731F21 37A907AC C70FD7AC 9EBACD1C 6E31C740 29B052E3
        AABC48F3 B00993F2 B2381F76 50A55322 A968C86E 05DE88E6
        367F6EF8 9A601DB4 342E9086 C7AC13B5 E56C32E9 E668040B
        73847893 C5BFD38A 1CF44F34 8B4EEE4C D68ADB7E 7B8C837F
        19BC4F90 2761F7CF F24AB1D7 04FD11C4 E929D855 3753B55D


---------------------------

  Update V

    0x03||V is
                         03E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 7EA8C2D1 F5B495E5 05EC6AFB 68BD4564
        B3D6C509 8CB27164 340B1B26 AA4D7DA6 34C2B188 735C1F39
        D9EAF9F0 E43642EB 6DED00B5 BA40D5CB C4B695C8 5CFE3F77


    H is
                         C9F3F96E 42CF0833 F5230A54 B1846C4C
        07E4282C 2851B4A5 91561F87 062D7A87 0016631E 18E3B559
        256B7E72 D0E2B60F DF2912BE BE24D3B0 9E2F4334 10A7E1F7
```

```
  Updated values

  V is
                            F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 C1CAF515 6C20FEC3 1F120831 4EE3FB56
        32BC6434 48A8E7A3 6786C0C3 8E2338DB A49BFC81 C552E9A4
        9DADEFB3 4952657D 430EE7F7 D5C73712 6E0F5794 5F483CA4


  reseed_counter is
                                                0000 00000002


rnd_val is
                                              DA126CF9 5C6BF97E
        2F731F21 37A907AC C70FD7AC 9EBACD1C 6E31C740 29B052E3
        AABC48F3 B00993F2 B2381F76 50A55322 A968C86E 05DE88E6
        367F6EF8 9A601DB4 342E9086 C7AC13B5 E56C32E9 E668040B
        73847893 C5BFD38A 1CF44F34 8B4EEE4C D68ADB7E 7B8C837F
        19BC4F90 2761F7CF F24AB1D7 04FD11C4 E929D855 3753B55D


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


--------------------------

  Process additional_input
```

0x02||V||additional_input is

02F1BF 0341EFEC
A23E1E8D 3322AADA C2C36752 40C818EF F7662171 96100104
7F782B4D C0568FA2 3ADFBE99 11D0F14C D1C1CAF5 156C20FE
C31F1208 314EE3FB 5632BC64 3448A8E7 A36786C0 C38E2338
DBA49BFC 81C552E9 A49DADEF B3495265 7D430EE7 F7D5C737
126E0F57 945F483C A4A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

w=Hash(0x02||V||additional_input) is

144F2001 03C8A031 4B9926FF C2B70B97
494663C9 A27EEC51 A44E9281 6BC1BB05 22FE594A AFE4574D
AC175FFD 3320DB34 C7D1AD98 3A94C970 740F7C27 F178D3EE

V is

F1BF03 41EFECA2 3E1E8D33 22AADAC2
C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
DFBE9911 D0F14CD1 D61A1516 6FE99EF4 6AAB2F31 119B06ED
7C02C7FD EB27D3F5 0BD55344 F9E4F3E0 C79A55CC 753740F2
49C54FB0 7C7340B2 0AE09590 105C0082 E21ED3BC 50C11092

Hashgen

requested_no_of_bits = 1024

---

i = 1

data is

F1BF03 41EFECA2 3E1E8D33 22AADAC2
C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
DFBE9911 D0F14CD1 D61A1516 6FE99EF4 6AAB2F31 119B06ED
7C02C7FD EB27D3F5 0BD55344 F9E4F3E0 C79A55CC 753740F2
49C54FB0 7C7340B2 0AE09590 105C0082 E21ED3BC 50C11092

w_i is

```
                      400B977C E8A2BB6A 84C6FD1C F9014596
    85ABF540 8CFF4588 CEDF52E2 D2DC300A A9B4FAED 8CD0161C
    2172B1FD 26925319 5883D6EB F21020F2 C20E5F2C 81AE60C8


  W is
                      400B977C E8A2BB6A 84C6FD1C F9014596
    85ABF540 8CFF4588 CEDF52E2 D2DC300A A9B4FAED 8CD0161C
    2172B1FD 26925319 5883D6EB F21020F2 C20E5F2C 81AE60C8


  ------------

  i = 2

  data is
                        F1BF03 41EFECA2 3E1E8D33 22AADAC2
    C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
    DFBE9911 D0F14CD1 D61A1516 6FE99EF4 6AAB2F31 119B06ED
    7C02C7FD EB27D3F5 0BD55344 F9E4F3E0 C79A55CC 753740F2
    49C54FB0 7C7340B2 0AE09590 105C0082 E21ED3BC 50C11093


  w_i is
                      595B834A 229B1F5B 726C1125 717E6207
    8886EF38 E61E3270 7AD5F811 6C6393DF B6E7C7AE 0E8E92BB
    D7E0C3D0 4BBA02F5 169F2F56 9A581589 15FEE4C9 D28D45DB


  W is
                                        400B977C E8A2BB6A
    84C6FD1C F9014596 85ABF540 8CFF4588 CEDF52E2 D2DC300A
    A9B4FAED 8CD0161C 2172B1FD 26925319 5883D6EB F21020F2
    C20E5F2C 81AE60C8 595B834A 229B1F5B 726C1125 717E6207
    8886EF38 E61E3270 7AD5F811 6C6393DF B6E7C7AE 0E8E92BB
    D7E0C3D0 4BBA02F5 169F2F56 9A581589 15FEE4C9 D28D45DB


returned_bits is
                                        400B977C E8A2BB6A
    84C6FD1C F9014596 85ABF540 8CFF4588 CEDF52E2 D2DC300A
    A9B4FAED 8CD0161C 2172B1FD 26925319 5883D6EB F21020F2
    C20E5F2C 81AE60C8 595B834A 229B1F5B 726C1125 717E6207
    8886EF38 E61E3270 7AD5F811 6C6393DF B6E7C7AE 0E8E92BB
    D7E0C3D0 4BBA02F5 169F2F56 9A581589 15FEE4C9 D28D45DB
```

```
---------------------------

  Update V

    0x03||V is
                          03F1BF03 41EFECA2 3E1E8D33 22AADAC2
        C3675240 C818EFF7 66217196 1001047F 782B4DC0 568FA23A
        DFBE9911 D0F14CD1 D61A1516 6FE99EF4 6AAB2F31 119B06ED
        7C02C7FD EB27D3F5 0BD55344 F9E4F3E0 C79A55CC 753740F2
        49C54FB0 7C7340B2 0AE09590 105C0082 E21ED3BC 50C11092


    H is
                          AF6B255D F26B42E3 135836C5 FF96BDB5
        5D6642FA D8346A99 27BA263E 0478B510 1FBC8FFA 358E930C
        CE1DE3F0 CA627639 B9A936F7 EEE22574 27C4B8CE E193F4C0


  Updated values

  V is
                            FDD840 FE092F63 5FE4C247 1040C76B
        DFCA1790 F98DF63D 92692289 5F9A75EE AF1627BF A83C4D7D
        1C00B5BD 33D09A5E FEB37349 95F24281 A205F8D8 45D40E48
        506A81F7 57010027 D5B4FF98 DC05E99F 5719CDA1 E3D8E910
        B63AAAF0 DB0F236D BA82A10B 5C9FB38D 150D0B23 23F72089


  reseed_counter is
                                                0000 00000003


rnd_val is
                                              400B977C E8A2BB6A
        84C6FD1C F9014596 85ABF540 8CFF4588 CEDF52E2 D2DC300A
        A9B4FAED 8CD0161C 2172B1FD 26925319 5883D6EB F21020F2
        C20E5F2C 81AE60C8 595B834A 229B1F5B 726C1125 717E6207
        8886EF38 E61E3270 7AD5F811 6C6393DF B6E7C7AE 0E8E92BB
        D7E0C3D0 4BBA02F5 169F2F56 9A581589 15FEE4C9 D28D45DB


################################################################

Hash_DRBG
```

```
    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                           000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                           000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
```

```
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                            20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                    01000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
                            152D908B 0EDF7253 D5D19F0A F96518D3
        AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
        BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A
```

```
    temp =
                          152D908B 0EDF7253 D5D19F0A F96518D3
        AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
        BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                   02000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
                          D466C1D9 AC010D21 B28CD9FD 124DF56D
        4D3B75B9 604827B3 CF49928E C4DA204F C374888E 278C0319
        DB45E1FD 3BCAD38C C355D2D6 55C1D606 60AEA6D6 BBE4E7C1


    temp =
                            152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


  V is
                            152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


--------------------------

  Hash_df - Generate C - Step 4
```

```
0x00||V is
                      00152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


Hash(counter||no_of_bits_to_return||input_string) is
                      2B22189F 32CB92C1 508BC343 69B8C37F
    D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
    10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


temp =
                      2B22189F 32CB92C1 508BC343 69B8C37F
    D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
    10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                           051F8441 D411B910 71605B9A 44B6643E
        67225358 2AE3148F 4A57E8FD A8E81155 108E4AFC C0E939BF
        D95FAB62 E8B1E4FD BDA34B60 C9220A37 EC6BD096 A6DAE159


    temp =
                             2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


  C is
                             2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


-----------------------------------------------------------------

First call to Generate

*****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

Generate FAILED: Reseed is required
-----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                             808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
  additional_input <empty>

--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                 01152D 908B0EDF
        7253D5D1 9F0AF965 18D3AD33 F2EF3151 A0C956D9 D3EE6DC0
        8B70F1EB 75982501 CE67BB72 94F1BC43 B322DCD2 5C146721
        2CAB0CD5 E6954C5B 6F6AD466 C1D9AC01 0D21B28C D9FD124D
        F56D4D3B 75B96048 27B3CF49 928EC4DA 204FC374 888E278C
        0319DB45 E1FD3BCA D3808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                 01000003 7801152D 908B0EDF
        7253D5D1 9F0AF965 18D3AD33 F2EF3151 A0C956D9 D3EE6DC0
        8B70F1EB 75982501 CE67BB72 94F1BC43 B322DCD2 5C146721
        2CAB0CD5 E6954C5B 6F6AD466 C1D9AC01 0D21B28C D9FD124D
        F56D4D3B 75B96048 27B3CF49 928EC4DA 204FC374 888E278C
        0319DB45 E1FD3BCA D3808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    Hash(counter||no_of_bits_to_return||input_string) is
                          17CE08BA 0E4651EA DF0FC284 53E6FB22
        268D86FC 36726062 9EEB49F1 3078D76D A5D5FB23 B8ED59BC
        101FE6D1 16EE9EE8 9A05CCB3 F636E348 1A82B307 79B8A687


    temp =
```

```
                        17CE08BA 0E4651EA DF0FC284 53E6FB22
        268D86FC 36726062 9EEB49F1 3078D76D A5D5FB23 B8ED59BC
        101FE6D1 16EE9EE8 9A05CCB3 F636E348 1A82B307 79B8A687


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                   02000003 7801152D 908B0EDF
        7253D5D1 9F0AF965 18D3AD33 F2EF3151 A0C956D9 D3EE6DC0
        8B70F1EB 75982501 CE67BB72 94F1BC43 B322DCD2 5C146721
        2CAB0CD5 E6954C5B 6F6AD466 C1D9AC01 0D21B28C D9FD124D
        F56D4D3B 75B96048 27B3CF49 928EC4DA 204FC374 888E278C
        0319DB45 E1FD3BCA D3808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    Hash(counter||no_of_bits_to_return||input_string) is
                        69E3C22C CD045AC3 1040FDBE 6CED62C2
        89607123 9A203F90 65DADAE6 51D56694 E76EC358 BBD4E673
        08A9A921 C6B71923 97235978 5AE5EE19 ECDB5D35 87552BC4


    temp =
                          17CE08 BA0E4651 EADF0FC2 8453E6FB
        22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
        BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
        8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
        9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


  V is
                          17CE08 BA0E4651 EADF0FC2 8453E6FB
        22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
        BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
        8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
        9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


--------------------------
```

```
Hash_df - Generate C - Step 4

  0x00||V is
                        0017CE08 BA0E4651 EADF0FC2 8453E6FB
      22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
      BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
      8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
      9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


  no_of_bits_to_return = 888

  ------------

  i = 1

  counter||no_of_bits_to_return||input_string is
            01 00000378 0017CE08 BA0E4651 EADF0FC2 8453E6FB
      22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
      BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
      8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
      9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


  Hash(counter||no_of_bits_to_return||input_string) is
                        4B0CA37A 6183A4D3 B14843C0 C8D603FD
      BC738838 A93506BB C567FD4F 8B54F665 0CB04697 A5380BFE
      108BFCB0 4195F953 3A87E871 74769A7D 24E97D26 27416E7F


  temp =
                        4B0CA37A 6183A4D3 B14843C0 C8D603FD
      BC738838 A93506BB C567FD4F 8B54F665 0CB04697 A5380BFE
      108BFCB0 4195F953 3A87E871 74769A7D 24E97D26 27416E7F


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
            02 00000378 0017CE08 BA0E4651 EADF0FC2 8453E6FB
      22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
      BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
      8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
      9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                          B974D8B5 F1C1D7A2 4ADFED81 E2382AE9
        089FF637 76DAF544 0661405E 13A67D43 6BABF056 22D9BC9A
        A7B9D848 862F6858 93B94E18 D4FEDB4E C3A87782 D47CE6CA


    temp =
                            4B0CA3 7A6183A4 D3B14843 C0C8D603
        FDBC7388 38A93506 BBC567FD 4F8B54F6 650CB046 97A5380B
        FE108BFC B04195F9 533A87E8 7174769A 7D24E97D 2627416E
        7FB974D8 B5F1C1D7 A24ADFED 81E2382A E9089FF6 3776DAF5
        44066140 5E13A67D 436BABF0 5622D9BC 9AA7B9D8 48862F68


  C is
                            4B0CA3 7A6183A4 D3B14843 C0C8D603
        FDBC7388 38A93506 BBC567FD 4F8B54F6 650CB046 97A5380B
        FE108BFC B04195F9 533A87E8 7174769A 7D24E97D 2627416E
        7FB974D8 B5F1C1D7 A24ADFED 81E2382A E9089FF6 3776DAF5
        44066140 5E13A67D 436BABF0 5622D9BC 9AA7B9D8 48862F68


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            17CE08 BA0E4651 EADF0FC2 8453E6FB
        22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
        BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
```

```
        8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
        9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


    w_i is
                           F93CA685 5590A77F 07354097 E90E0266
        48B6115D F008FFED BD9D9811 F54E8286 EF00FDD6 BA1E58DF
        2535E3FB DD9A9BA3 754A97F3 6EE83322 1582060A 1F37FCE4


    W is
                           F93CA685 5590A77F 07354097 E90E0266
        48B6115D F008FFED BD9D9811 F54E8286 EF00FDD6 BA1E58DF
        2535E3FB DD9A9BA3 754A97F3 6EE83322 1582060A 1F37FCE4


    ------------

    i = 2

    data is
                             17CE08 BA0E4651 EADF0FC2 8453E6FB
        22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
        BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
        8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
        9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B71A


    w_i is
                           EE882663 6B28EAD5 89593F4C A8B64738
        8F24EB3F 0A347969 68D21BDE E6F81FD5 DF93536F 935937B8
        025EC8CB F57DDB0C 61F2E414 63CC1516 D657DA28 29C6BF90


    W is
                                               F93CA685 5590A77F
        07354097 E90E0266 48B6115D F008FFED BD9D9811 F54E8286
        EF00FDD6 BA1E58DF 2535E3FB DD9A9BA3 754A97F3 6EE83322
        1582060A 1F37FCE4 EE882663 6B28EAD5 89593F4C A8B64738
        8F24EB3F 0A347969 68D21BDE E6F81FD5 DF93536F 935937B8
        025EC8CB F57DDB0C 61F2E414 63CC1516 D657DA28 29C6BF90


returned_bits is
                                               F93CA685 5590A77F
        07354097 E90E0266 48B6115D F008FFED BD9D9811 F54E8286
```

```
        EF00FDD6 BA1E58DF 2535E3FB DD9A9BA3 754A97F3 6EE83322
        1582060A 1F37FCE4 EE882663 6B28EAD5 89593F4C A8B64738
        8F24EB3F 0A347969 68D21BDE E6F81FD5 DF93536F 935937B8
        025EC8CB F57DDB0C 61F2E414 63CC1516 D657DA28 29C6BF90


--------------------------

  Update V

    0x03||V is
                         0317CE08 BA0E4651 EADF0FC2 8453E6FB
        22268D86 FC367260 629EEB49 F13078D7 6DA5D5FB 23B8ED59
        BC101FE6 D116EE9E E89A05CC B3F636E3 481A82B3 0779B8A6
        8769E3C2 2CCD045A C31040FD BE6CED62 C2896071 239A203F
        9065DADA E651D566 94E76EC3 58BBD4E6 7308A9A9 21C6B719


    H is
                         9947CEAD BF7B9EFF B4167AA7 7DEEEF78
        AB54762F BDDA12AF A034B7A3 0B837D85 5954FE7C 7C89A480
        CDFB25CE 69CD76B8 07D1095C 1C6018D7 FC0152D8 9E063488


  Updated values

  V is
                           62DAAC 346FC9F6 BE905806 451CBCFF
        1FE3010F 34DFA767 1E645347 40BBCDCD D2B28641 BB5E2565
        BA20ABE3 81588498 D51C5C62 E4E64C7D 7955E6D7 AB8FE98D
        B277CECA A098D8E2 058FD88E 4BD2A313 04E6FEE3 D79A9FB5
        A26761E9 AE32F29B E024240F CB3EC77B 09B1B65A 08531B0A


  reseed_counter is
                                                0000 00000002


rnd_val is
                                             F93CA685 5590A77F
        07354097 E90E0266 48B6115D F008FFED BD9D9811 F54E8286
        EF00FDD6 BA1E58DF 2535E3FB DD9A9BA3 754A97F3 6EE83322
        1582060A 1F37FCE4 EE882663 6B28EAD5 89593F4C A8B64738
        8F24EB3F 0A347969 68D21BDE E6F81FD5 DF93536F 935937B8
        025EC8CB F57DDB0C 61F2E414 63CC1516 D657DA28 29C6BF90
```

```
-------------------------------------------------------------

Second call to Generate

*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

Generate FAILED: Reseed is required
-------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                              0162DA AC346FC9
        F6BE9058 06451CBC FF1FE301 0F34DFA7 671E6453 4740BBCD
        CDD2B286 41BB5E25 65BA20AB E3815884 98D51C5C 62E4E64C
        7D7955E6 D7AB8FE9 8DB277CE CAA098D8 E2058FD8 8E4BD2A3
        1304E6FE E3D79A9F B5A26761 E9AE32F2 9BE02424 0FCB3EC7
        7B09B1B6 5A08531B 0AC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    no_of_bits_to_return = 888
```

```
------------

i = 1

counter||no_of_bits_to_return||input_string is
                                01000003 780162DA AC346FC9
    F6BE9058 06451CBC FF1FE301 0F34DFA7 671E6453 4740BBCD
    CDD2B286 41BB5E25 65BA20AB E3815884 98D51C5C 62E4E64C
    7D7955E6 D7AB8FE9 8DB277CE CAA098D8 E2058FD8 8E4BD2A3
    1304E6FE E3D79A9F B5A26761 E9AE32F2 9BE02424 0FCB3EC7
    7B09B1B6 5A08531B 0AC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Hash(counter||no_of_bits_to_return||input_string) is
                        26F8B3C0 A59D2E12 74CA61F9 D896F8F9
    0AE012FE 512AA300 72DD2BAA 5BCE6F16 BF9398BC 247FE40F
    76079262 EEC76476 2CB5B8CF 738ED7C7 249EC615 CA579D68


temp =
                        26F8B3C0 A59D2E12 74CA61F9 D896F8F9
    0AE012FE 512AA300 72DD2BAA 5BCE6F16 BF9398BC 247FE40F
    76079262 EEC76476 2CB5B8CF 738ED7C7 249EC615 CA579D68


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                02000003 780162DA AC346FC9
    F6BE9058 06451CBC FF1FE301 0F34DFA7 671E6453 4740BBCD
    CDD2B286 41BB5E25 65BA20AB E3815884 98D51C5C 62E4E64C
    7D7955E6 D7AB8FE9 8DB277CE CAA098D8 E2058FD8 8E4BD2A3
    1304E6FE E3D79A9F B5A26761 E9AE32F2 9BE02424 0FCB3EC7
    7B09B1B6 5A08531B 0AC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                          107F58B6 1187B19B A9FB47F9 06F1698D
        5B0F3967 D7E7D97C 6D6F25C7 5FC403C1 C6E05077 0951F57F
        997DFDB1 F6B6506D E75F9D00 953ED240 28C8DE4D C22ADD87


    temp =
                            26F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


  V is
                            26F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          0026F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 0026F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
```

```
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


    Hash(counter||no_of_bits_to_return||input_string) is
                           E35403EB 642047D2 4B2913A6 A064EC86
        3D44541A 951BD377 04EEEC2A C67FB0B3 9968ED22 5646700F
        24FA3A0A 7C42F941 1840ED9E 067D5AE9 F54A7E20 4E5AEB6C


    temp =
                           E35403EB 642047D2 4B2913A6 A064EC86
        3D44541A 951BD377 04EEEC2A C67FB0B3 9968ED22 5646700F
        24FA3A0A 7C42F941 1840ED9E 067D5AE9 F54A7E20 4E5AEB6C


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 0026F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


    Hash(counter||no_of_bits_to_return||input_string) is
                           47BC945E 0C7B6F91 8B4BAA5D 3EED85CC
        20B0EE1D 46BF14C1 3D189703 69EF6C55 A8AB988D 7E3F356F
        2E328856 E356FDEE 3D2976E3 CB55E90C 61FB3FBF BA296DB4


    temp =
                             E35403 EB642047 D24B2913 A6A064EC
        863D4454 1A951BD3 7704EEEC 2AC67FB0 B39968ED 22564670
        0F24FA3A 0A7C42F9 411840ED 9E067D5A E9F54A7E 204E5AEB
        6C47BC94 5E0C7B6F 918B4BAA 5D3EED85 CC20B0EE 1D46BF14
        C13D1897 0369EF6C 55A8AB98 8D7E3F35 6F2E3288 56E356FD


C is
                             E35403 EB642047 D24B2913 A6A064EC
        863D4454 1A951BD3 7704EEEC 2AC67FB0 B39968ED 22564670
        0F24FA3A 0A7C42F9 411840ED 9E067D5A E9F54A7E 204E5AEB
        6C47BC94 5E0C7B6F 918B4BAA 5D3EED85 CC20B0EE 1D46BF14
```

```
        C13D1897 0369EF6C 55A8AB98 8D7E3F35 6F2E3288 56E356FD


************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            26F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


    w_i is
                          4817618F 48C60FB1 CE5BFBDA 0CAF4591
        882A31F6 EE3FE0F7 8779992A 06EC60F3 7FB9A8D6 108C231F
        0A927754 B0599FA4 FA27A4E2 5E065EF0 3085B892 979DC0E7


    W is
                          4817618F 48C60FB1 CE5BFBDA 0CAF4591
        882A31F6 EE3FE0F7 8779992A 06EC60F3 7FB9A8D6 108C231F
        0A927754 B0599FA4 FA27A4E2 5E065EF0 3085B892 979DC0E7


    ------------

    i = 2

    data is
```

```
                          26F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B651


    w_i is
                         A1080883 CAEBFDFD 3665A8F2 D061C521
        F7D6E3DA 2AF8B97B 6B43B6EC 831AF515 070A83BB B9AC95ED
        4EF49B75 6A2377A5 F0833D84 7E27A88D DB0C2CE4 AD782E7B


    W is
                                             4817618F 48C60FB1
        CE5BFBDA 0CAF4591 882A31F6 EE3FE0F7 8779992A 06EC60F3
        7FB9A8D6 108C231F 0A927754 B0599FA4 FA27A4E2 5E065EF0
        3085B892 979DC0E7 A1080883 CAEBFDFD 3665A8F2 D061C521
        F7D6E3DA 2AF8B97B 6B43B6EC 831AF515 070A83BB B9AC95ED
        4EF49B75 6A2377A5 F0833D84 7E27A88D DB0C2CE4 AD782E7B


  returned_bits is
                                             4817618F 48C60FB1
        CE5BFBDA 0CAF4591 882A31F6 EE3FE0F7 8779992A 06EC60F3
        7FB9A8D6 108C231F 0A927754 B0599FA4 FA27A4E2 5E065EF0
        3085B892 979DC0E7 A1080883 CAEBFDFD 3665A8F2 D061C521
        F7D6E3DA 2AF8B97B 6B43B6EC 831AF515 070A83BB B9AC95ED
        4EF49B75 6A2377A5 F0833D84 7E27A88D DB0C2CE4 AD782E7B


---------------------------

  Update V

    0x03||V is
                         0326F8B3 C0A59D2E 1274CA61 F9D896F8
        F90AE012 FE512AA3 0072DD2B AA5BCE6F 16BF9398 BC247FE4
        0F760792 62EEC764 762CB5B8 CF738ED7 C7249EC6 15CA579D
        68107F58 B61187B1 9BA9FB47 F906F169 8D5B0F39 67D7E7D9
        7C6D6F25 C75FC403 C1C6E050 770951F5 7F997DFD B1F6B650


    H is
                         7F116A9A 5EE60219 CB56CF14 EA153D77
        D31DD052 0D1D8407 79B39FD8 3750B4F3 76BE499E 43F66A07
```

```
        63E03D8D 39F32DA9 1BB2A0CF 1D4D97A5 FDB1B238 5DED4D0B


  Updated values

  V is
                           0A4CB7 AC09BD75 E4BFF375 A078FBE5
        7F482467 18E64676 7777CC17 D5224E1F CA58FC85 DE7AC654
        1E9B01CC 6D6B0A5E 36566140 CC600E4C 7C70B859 202DF000
        A7760C3F 213B8728 A6E8E6CA 8D9693E2 D03A09C5 C91510F5
        A18AC54A 04BCE119 33222CB8 21D528D0 EC7962BE 66C75A59


  reseed_counter is
                                                0000 00000002


rnd_val is
                                             4817618F 48C60FB1
        CE5BFBDA 0CAF4591 882A31F6 EE3FE0F7 8779992A 06EC60F3
        7FB9A8D6 108C231F 0A927754 B0599FA4 FA27A4E2 5E065EF0
        3085B892 979DC0E7 A1080883 CAEBFDFD 3665A8F2 D061C521
        F7D6E3DA 2AF8B97B 6B43B6EC 831AF515 070A83BB B9AC95ED
        4EF49B75 6A2377A5 F0833D84 7E27A88D DB0C2CE4 AD782E7B


##############################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                           000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                           20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##############################################################

**************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
```

```
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                    01000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
                           152D908B 0EDF7253 D5D19F0A F96518D3
        AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
        BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


    temp =
```

```
                        152D908B 0EDF7253 D5D19F0A F96518D3
        AD33F2EF 3151A0C9 56D9D3EE 6DC08B70 F1EB7598 2501CE67
        BB7294F1 BC43B322 DCD25C14 67212CAB 0CD5E695 4C5B6F6A


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
                                   02000003 78000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
                           D466C1D9 AC010D21 B28CD9FD 124DF56D
        4D3B75B9 604827B3 CF49928E C4DA204F C374888E 278C0319
        DB45E1FD 3BCAD38C C355D2D6 55C1D606 60AEA6D6 BBE4E7C1


    temp =
                             152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


  V is
                             152D90 8B0EDF72 53D5D19F 0AF96518
        D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
        67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
        6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
        B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           00152D90 8B0EDF72 53D5D19F 0AF96518
```

```
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


Hash(counter||no_of_bits_to_return||input_string) is
                     2B22189F 32CB92C1 508BC343 69B8C37F
    D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
    10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


temp =
                     2B22189F 32CB92C1 508BC343 69B8C37F
    D9593FD9 EC56B559 844E605D 67B4A586 2F1C7B75 3F68DF75
    10BE1F64 A7AAB557 9821195F FF0357CC 5464CAC5 D07655D6


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00152D90 8B0EDF72 53D5D19F 0AF96518
    D3AD33F2 EF3151A0 C956D9D3 EE6DC08B 70F1EB75 982501CE
    67BB7294 F1BC43B3 22DCD25C 1467212C AB0CD5E6 954C5B6F
    6AD466C1 D9AC010D 21B28CD9 FD124DF5 6D4D3B75 B9604827
    B3CF4992 8EC4DA20 4FC37488 8E278C03 19DB45E1 FD3BCAD3


Hash(counter||no_of_bits_to_return||input_string) is
                     051F8441 D411B910 71605B9A 44B6643E
```

```
        67225358 2AE3148F 4A57E8FD A8E81155 108E4AFC C0E939BF
        D95FAB62 E8B1E4FD BDA34B60 C9220A37 EC6BD096 A6DAE159


    temp =
                           2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


  C is
                           2B2218 9F32CB92 C1508BC3 4369B8C3
        7FD9593F D9EC56B5 59844E60 5D67B4A5 862F1C7B 753F68DF
        7510BE1F 64A7AAB5 57982119 5FFF0357 CC5464CA C5D07655
        D6051F84 41D411B9 1071605B 9A44B664 3E672253 582AE314
        8F4A57E8 FDA8E811 55108E4A FCC0E939 BFD95FAB 62E8B1E4


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


----------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0115 2D908B0E DF7253D5 D19F0AF9 6518D3AD 33F2EF31
        51A0C956 D9D3EE6D C08B70F1 EB759825 01CE67BB 7294F1BC
        43B322DC D25C1467 212CAB0C D5E6954C 5B6F6AD4 66C1D9AC
        010D21B2 8CD9FD12 4DF56D4D 3B75B960 4827B3CF 49928EC4
        DA204FC3 74888E27 8C0319DB 45E1FD3B CAD38081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        03780115 2D908B0E DF7253D5 D19F0AF9 6518D3AD 33F2EF31
        51A0C956 D9D3EE6D C08B70F1 EB759825 01CE67BB 7294F1BC
        43B322DC D25C1467 212CAB0C D5E6954C 5B6F6AD4 66C1D9AC
        010D21B2 8CD9FD12 4DF56D4D 3B75B960 4827B3CF 49928EC4
```

```
    DA204FC3 74888E27 8C0319DB 45E1FD3B CAD38081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
                      E027DDFE D6A43806 62480926 0DA6610E
    27531429 5772E9B2 3B44BB5F EAE132FB 6E6B69EA 539D3699
    192CD0A3 9D869CCD BEA14C8C CD3E4A54 D1777BD7 E6C7301D


temp =
                      E027DDFE D6A43806 62480926 0DA6610E
    27531429 5772E9B2 3B44BB5F EAE132FB 6E6B69EA 539D3699
    192CD0A3 9D869CCD BEA14C8C CD3E4A54 D1777BD7 E6C7301D


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    03780115 2D908B0E DF7253D5 D19F0AF9 6518D3AD 33F2EF31
    51A0C956 D9D3EE6D C08B70F1 EB759825 01CE67BB 7294F1BC
    43B322DC D25C1467 212CAB0C D5E6954C 5B6F6AD4 66C1D9AC
    010D21B2 8CD9FD12 4DF56D4D 3B75B960 4827B3CF 49928EC4
    DA204FC3 74888E27 8C0319DB 45E1FD3B CAD38081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                          E1BD13FD 14135A06 878D0E14 56BEDE0F
        9C155E5D 4BC6FC5E 53263EEB E7FC1DA9 2342A29A C9E0EEEE
        BAF1BE2F 043DB8A2 F0009B69 9051F360 D881C2DC B8198588


    temp =
                            E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


  V is
                            E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8
```

```
  Hash(counter||no_of_bits_to_return||input_string) is
                       006B8A26 5897C2B3 7B02C787 66692916
      B0E0839A 7F778736 0D5F2A08 F9C380CD 083ADBE1 A758EA52
      FF0672B2 3F5976B1 1225D0BA 3D990E2C 198F7CAC 3EA6ECAD


  temp =
                       006B8A26 5897C2B3 7B02C787 66692916
      B0E0839A 7F778736 0D5F2A08 F9C380CD 083ADBE1 A758EA52
      FF0672B2 3F5976B1 1225D0BA 3D990E2C 198F7CAC 3EA6ECAD


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
            02 00000378 00E027DD FED6A438 06624809 260DA661
      0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
      99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
      1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
      5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


  Hash(counter||no_of_bits_to_return||input_string) is
                       35D7E097 B14DA223 67788C5E 5F6CB178
      D3F5EF2D 58751980 F8706DA8 6E078431 0AE61865 25FAA503
      8A9312BA 5040A72D 7BCE3632 6382B5EE EB173EAA ED1E7857


  temp =
                         006B8A 265897C2 B37B02C7 87666929
      16B0E083 9A7F7787 360D5F2A 08F9C380 CD083ADB E1A758EA
      52FF0672 B23F5976 B11225D0 BA3D990E 2C198F7C AC3EA6EC
      AD35D7E0 97B14DA2 2367788C 5E5F6CB1 78D3F5EF 2D587519
      80F8706D A86E0784 310AE618 6525FAA5 038A9312 BA5040A7


C is
                         006B8A 265897C2 B37B02C7 87666929
      16B0E083 9A7F7787 360D5F2A 08F9C380 CD083ADB E1A758EA
      52FF0672 B23F5976 B11225D0 BA3D990E 2C198F7C AC3EA6EC
      AD35D7E0 97B14DA2 2367788C 5E5F6CB1 78D3F5EF 2D587519
      80F8706D A86E0784 310AE618 6525FAA5 038A9312 BA5040A7
```

```
***************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                           E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


    w_i is
                          0455DD4A D7DBACB2 410BE58D F7248D76
        5A4547AB AEE1743B 0BCAD37E BD06DA7C F7CE5E22 16E52532
        7E9E2005 EBEF2CE5 3BD733B1 8128627D 3FD61530 89373AF2


    W is
                          0455DD4A D7DBACB2 410BE58D F7248D76
        5A4547AB AEE1743B 0BCAD37E BD06DA7C F7CE5E22 16E52532
        7E9E2005 EBEF2CE5 3BD733B1 8128627D 3FD61530 89373AF2


    ------------

    i = 2

    data is
                           E027DD FED6A438 06624809 260DA661
```

```
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB9


    w_i is
                             606A1584 646A0EA4 88BFEF45 228699A0
        89CEA8AE C44502D8 6D9591F3 552C688B 7F7B45FC B0C3C2B9
        43C1CD8A 6FC63DF4 D81C3DA5 43C9CF28 43855EA8 4E4F959C


    W is
                                              0455DD4A D7DBACB2
        410BE58D F7248D76 5A4547AB AEE1743B 0BCAD37E BD06DA7C
        F7CE5E22 16E52532 7E9E2005 EBEF2CE5 3BD733B1 8128627D
        3FD61530 89373AF2 606A1584 646A0EA4 88BFEF45 228699A0
        89CEA8AE C44502D8 6D9591F3 552C688B 7F7B45FC B0C3C2B9
        43C1CD8A 6FC63DF4 D81C3DA5 43C9CF28 43855EA8 4E4F959C


  returned_bits is
                                              0455DD4A D7DBACB2
        410BE58D F7248D76 5A4547AB AEE1743B 0BCAD37E BD06DA7C
        F7CE5E22 16E52532 7E9E2005 EBEF2CE5 3BD733B1 8128627D
        3FD61530 89373AF2 606A1584 646A0EA4 88BFEF45 228699A0
        89CEA8AE C44502D8 6D9591F3 552C688B 7F7B45FC B0C3C2B9
        43C1CD8A 6FC63DF4 D81C3DA5 43C9CF28 43855EA8 4E4F959C


--------------------------

  Update V

    0x03||V is
                             03E027DD FED6A438 06624809 260DA661
        0E275314 295772E9 B23B44BB 5FEAE132 FB6E6B69 EA539D36
        99192CD0 A39D869C CDBEA14C 8CCD3E4A 54D1777B D7E6C730
        1DE1BD13 FD14135A 06878D0E 1456BEDE 0F9C155E 5D4BC6FC
        5E53263E EBE7FC1D A92342A2 9AC9E0EE EEBAF1BE 2F043DB8


    H is
                             FEA33CEC E4551052 A5620E9F F9CE37B0
        93C77E97 BDBBD15E 358C8A42 CE1D47DC FC587048 90D8ECD8
        86703CE6 334C5D2B 9093A57D E6E85638 5A96E601 1F73F8AA
```

```
  Updated values

  V is
                            E09368 252F3BFA B9DD4AD0 AD740F8A
        24D83397 C3D6EA70 E848A3E5 68E4A4B3 C876A645 CBFAF620
        EC183343 55DCE014 7D74040A 2B5FE7AB 264D1598 7DF3A5CD
        5EDF138C 5281325A 5F7B8FDD 40D3736C 84C87B96 1B7D28EE
        65BBD392 C7A260CD 6AC1CE38 E6D831CC 4CDC6AD2 08C8770A


  reseed_counter is
                                                0000 00000002


rnd_val is
                                               0455DD4A D7DBACB2
        410BE58D F7248D76 5A4547AB AEE1743B 0BCAD37E BD06DA7C
        F7CE5E22 16E52532 7E9E2005 EBEF2CE5 3BD733B1 8128627D
        3FD61530 89373AF2 606A1584 646A0EA4 88BFEF45 228699A0
        89CEA8AE C44502D8 6D9591F3 552C688B 7F7B45FC B0C3C2B9
        43C1CD8A 6FC63DF4 D81C3DA5 43C9CF28 43855EA8 4E4F959C


----------------------------------------------------------------

Second call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
----------------------------------------------------------------
```

Hash_DRBG_Reseed_algorithm

  entropy_input
                          C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

  additional_input
                          A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01E0 9368252F 3BFAB9DD 4AD0AD74 0F8A24D8 3397C3D6
        EA70E848 A3E568E4 A4B3C876 A645CBFA F620EC18 334355DC
        E0147D74 040A2B5F E7AB264D 15987DF3 A5CD5EDF 138C5281
        325A5F7B 8FDD40D3 736C84C8 7B961B7D 28EE65BB D392C7A2
        60CD6AC1 CE38E6D8 31CC4CDC 6AD208C8 770AC0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

    no_of_bits_to_return = 888

    ----

    i = 1

    counter||no_of_bits_to_return||input_string is

                                                        010000
    037801E0 9368252F 3BFAB9DD 4AD0AD74 0F8A24D8 3397C3D6
    EA70E848 A3E568E4 A4B3C876 A645CBFA F620EC18 334355DC
    E0147D74 040A2B5F E7AB264D 15987DF3 A5CD5EDF 138C5281
    325A5F7B 8FDD40D3 736C84C8 7B961B7D 28EE65BB D392C7A2
    60CD6AC1 CE38E6D8 31CC4CDC 6AD208C8 770AC0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

Hash(counter||no_of_bits_to_return||input_string) is
                        FED11DEE 23C9EB92 D1D700B2 E41A74C9
    31FAC151 E1A405CC C786043D 5828D57E 40132987 BD791906
    E19D29BE A6C99FDF CF342F6B 4112165B BEC738FD 296465F9

temp =
                        FED11DEE 23C9EB92 D1D700B2 E41A74C9
    31FAC151 E1A405CC C786043D 5828D57E 40132987 BD791906
    E19D29BE A6C99FDF CF342F6B 4112165B BEC738FD 296465F9

----

i = 2

counter||no_of_bits_to_return||input_string is
                                                        020000
    037801E0 9368252F 3BFAB9DD 4AD0AD74 0F8A24D8 3397C3D6
    EA70E848 A3E568E4 A4B3C876 A645CBFA F620EC18 334355DC
    E0147D74 040A2B5F E7AB264D 15987DF3 A5CD5EDF 138C5281
    325A5F7B 8FDD40D3 736C84C8 7B961B7D 28EE65BB D392C7A2
    60CD6AC1 CE38E6D8 31CC4CDC 6AD208C8 770AC0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6

```
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    Hash(counter||no_of_bits_to_return||input_string) is
                           53607D77 80E07836 D3CF926B 4575368D
        2891F587 9804CCBE 4414F228 BD0FBBDF 89378390 1DA7536E
        C301B2EB AC27DA53 82919EFF 3675946B 4CE8EB63 6C2BC483


    temp =
                             FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


  V is
                             FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           00FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
```

```
          01 00000378 00FED11D EE23C9EB 92D1D700 B2E41A74
      C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
      06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
      F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
      BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


   Hash(counter||no_of_bits_to_return||input_string) is
                        5B0257EF F0741C93 45764EE4 D2D630BE
      02725A7F 0AFD9873 2BB98E9F C7CB759A 57830B67 0F22F97D
      7CC91247 AA8F7458 DC72B067 01C9CE4B BBFCCCE9 B44B43AF


   temp =
                        5B0257EF F0741C93 45764EE4 D2D630BE
      02725A7F 0AFD9873 2BB98E9F C7CB759A 57830B67 0F22F97D
      7CC91247 AA8F7458 DC72B067 01C9CE4B BBFCCCE9 B44B43AF


   ------------

   i = 2

   counter||no_of_bits_to_return||input_string is
             02 00000378 00FED11D EE23C9EB 92D1D700 B2E41A74
      C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
      06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
      F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
      BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


   Hash(counter||no_of_bits_to_return||input_string) is
                        E891AF3C 8B4D3730 C877550D 41F944A6
      D18919A5 22F668CD 9AFBE283 E42A2C85 D95BA607 F3635B1F
      A473EA1D AB14476B 082C537E 965D206E D75165A3 299B56FB


   temp =
                          5B0257 EFF0741C 9345764E E4D2D630
      BE02725A 7F0AFD98 732BB98E 9FC7CB75 9A57830B 670F22F9
      7D7CC912 47AA8F74 58DC72B0 6701C9CE 4BBBFCCC E9B44B43
      AFE891AF 3C8B4D37 30C87755 0D41F944 A6D18919 A522F668
      CD9AFBE2 83E42A2C 85D95BA6 07F3635B 1FA473EA 1DAB1447


C is
```

```
                          5B0257 EFF0741C 9345764E E4D2D630
        BE02725A 7F0AFD98 732BB98E 9FC7CB75 9A57830B 670F22F9
        7D7CC912 47AA8F74 58DC72B0 6701C9CE 4BBBFCCC E9B44B43
        AFE891AF 3C8B4D37 30C87755 0D41F944 A6D18919 A522F668
        CD9AFBE2 83E42A2C 85D95BA6 07F3635B 1FA473EA 1DAB1447


************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                          FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA


    w_i is
                         C047D46D 7F614E4E 4A7952C7 9A451F8F
        7ACA3799 67E2977C 401C626A 2ED70D74 A6366057 9A354115
        BC8C8C8C C3AEA305 0686A0CF CDB6FA9C F78D4C21 65BAF851


    W is
                         C047D46D 7F614E4E 4A7952C7 9A451F8F
        7ACA3799 67E2977C 401C626A 2ED70D74 A6366057 9A354115
        BC8C8C8C C3AEA305 0686A0CF CDB6FA9C F78D4C21 65BAF851


    ------------
```

```
    i = 2

    data is
                             FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DB


    w_i is
                           C6F9B1CD 16A2E14C 15C6DAAC 56C16E75
        FC84A14D 58B41622 E88B0F1B 1995587F D8BAA999 CBA98025
        4C8AB9A9 691DF7B8 4D88B639 A9A3106D EABEB637 48B99C09


    W is
                                               C047D46D 7F614E4E
        4A7952C7 9A451F8F 7ACA3799 67E2977C 401C626A 2ED70D74
        A6366057 9A354115 BC8C8C8C C3AEA305 0686A0CF CDB6FA9C
        F78D4C21 65BAF851 C6F9B1CD 16A2E14C 15C6DAAC 56C16E75
        FC84A14D 58B41622 E88B0F1B 1995587F D8BAA999 CBA98025
        4C8AB9A9 691DF7B8 4D88B639 A9A3106D EABEB637 48B99C09


  returned_bits is
                                               C047D46D 7F614E4E
        4A7952C7 9A451F8F 7ACA3799 67E2977C 401C626A 2ED70D74
        A6366057 9A354115 BC8C8C8C C3AEA305 0686A0CF CDB6FA9C
        F78D4C21 65BAF851 C6F9B1CD 16A2E14C 15C6DAAC 56C16E75
        FC84A14D 58B41622 E88B0F1B 1995587F D8BAA999 CBA98025
        4C8AB9A9 691DF7B8 4D88B639 A9A3106D EABEB637 48B99C09


---------------------------

  Update V

    0x03||V is
                           03FED11D EE23C9EB 92D1D700 B2E41A74
        C931FAC1 51E1A405 CCC78604 3D5828D5 7E401329 87BD7919
        06E19D29 BEA6C99F DFCF342F 6B411216 5BBEC738 FD296465
        F953607D 7780E078 36D3CF92 6B457536 8D2891F5 879804CC
        BE4414F2 28BD0FBB DF893783 901DA753 6EC301B2 EBAC27DA
```

```
    H is
                          11F64E29 6D412BE7 B8B5F5D6 86844A6D
        6660FC31 DA53314D A4DD6D8A E87B2BA5 D03A7172 BE903116
        CA50EFEE 37E6582E ACDB7E3B 13BC60EA 7D6E8907 E1215603


  Updated values

  V is
                            59D375 DE143E08 26174D4F 97B6F0A5
        87346D1B D0ECA19E 3FF33F92 DD1FF44B 18979634 EECC9C12
        845E663C 06515914 4AA1F509 3F8407CC 6030B9DC 6D61FA17
        0F9CEE5E 8E5F5EFD 0C79B472 61029A21 04348C81 EB4B2C4C
        563000C2 E4879217 123E1164 ABCD6B99 0BD5FEA4 EA789225


  reseed_counter is
                                                 0000 00000002


rnd_val is
                                               C047D46D 7F614E4E
        4A7952C7 9A451F8F 7ACA3799 67E2977C 401C626A 2ED70D74
        A6366057 9A354115 BC8C8C8C C3AEA305 0686A0CF CDB6FA9C
        F78D4C21 65BAF851 C6F9B1CD 16A2E14C 15C6DAAC 56C16E75
        FC84A14D 58B41622 E88B0F1B 1995587F D8BAA999 CBA98025
        4C8AB9A9 691DF7B8 4D88B639 A9A3106D EABEB637 48B99C09


################################################################

Hash_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E
```

```
    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

################################################################

****************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
```

```
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                             404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
                     E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


temp =
                     E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
                     80B87195 7508538D 2D87A4A3 B5728ADB
    4191974A 384F323D 2E585869 5C152F99 D0E8CF4C B41BC2A6
    12955B4C 4838B9FB EB00568D 36F727E1 742FF774 E8542A4B


temp =
                       E5A5C5 85D6A9E1 1C58581F 3514EE19
    A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
    A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
    EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
    3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9
```

```
  V is
                           E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


----------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                          00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    Hash(counter||no_of_bits_to_return||input_string) is
                          0C193DBC 1942C121 C63513ED 95ECA91C
        62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
        421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


    temp =
                          0C193DBC 1942C121 C63513ED 95ECA91C
        62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
        421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577
```

```
    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


    Hash(counter||no_of_bits_to_return||input_string) is
                          0176FE93 A4C199A2 258615DD A840AE6F
        C2E7DB39 1315119E 57774F94 396C81F5 F8D4835D 618D960B
        297E97F1 A21B35E3 E450A877 4819D918 961DFC01 FFC73630


    temp =
                            0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


  C is
                            0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


------------------------------------------------------------

First call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024
```

```
  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
                                                 01E5A5 C585D6A9
        E11C5858 1F3514EE 19A7048C F096A3E9 B139D9C0 A2C06793
        10414073 C104E2F6 F8A37C7C 666E11FF 443933AB A1CFAD4C
        620CDFF5 DA8C0860 CEEE80B8 71957508 538D2D87 A4A3B572
        8ADB4191 974A384F 323D2E58 58695C15 2F99D0E8 CF4CB41B
        C2A61295 5B4C4838 B9808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                  01000003 7801E5A5 C585D6A9
        E11C5858 1F3514EE 19A7048C F096A3E9 B139D9C0 A2C06793
        10414073 C104E2F6 F8A37C7C 666E11FF 443933AB A1CFAD4C
        620CDFF5 DA8C0860 CEEE80B8 71957508 538D2D87 A4A3B572
        8ADB4191 974A384F 323D2E58 58695C15 2F99D0E8 CF4CB41B
```

```
    C2A61295 5B4C4838 B9808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


Hash(counter||no_of_bits_to_return||input_string) is
                      90710EB6 88DF0184 891E9AE5 B0996022
    A3CA8E79 D7769CE7 5B00BAF2 E6D6EAB7 761DC6FB 1E76DB71
    77737E44 41F0AF58 6138E43C A81E70D2 3F71DD61 CCF5FA8D


temp =
                      90710EB6 88DF0184 891E9AE5 B0996022
    A3CA8E79 D7769CE7 5B00BAF2 E6D6EAB7 761DC6FB 1E76DB71
    77737E44 41F0AF58 6138E43C A81E70D2 3F71DD61 CCF5FA8D


------------

i = 2

counter||no_of_bits_to_return||input_string is
                               02000003 7801E5A5 C585D6A9
    E11C5858 1F3514EE 19A7048C F096A3E9 B139D9C0 A2C06793
    10414073 C104E2F6 F8A37C7C 666E11FF 443933AB A1CFAD4C
    620CDFF5 DA8C0860 CEEE80B8 71957508 538D2D87 A4A3B572
    8ADB4191 974A384F 323D2E58 58695C15 2F99D0E8 CF4CB41B
    C2A61295 5B4C4838 B9808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


Hash(counter||no_of_bits_to_return||input_string) is
                      46829AC7 E211C76E 9391E914 9A96C5F0
    FC5239BE BDB5CD05 F22E0B8D A207A408 C44975D7 F1894EC2
    3A47A047 B8657C9E 50FDDFE3 0B1D6523 C96ABD2F 39547413


temp =
                        90710E B688DF01 84891E9A E5B09960
    22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
    7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
```

```
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


  V is
                            90710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           0090710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 0090710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


    Hash(counter||no_of_bits_to_return||input_string) is
                           458CFE66 103B99E5 F76853E8 AD6B7D35
        EDEAED91 4B58D2A4 8FDC6735 959CC6BE 0CA35FFF 9E90B25D
        825B1399 7453576C 2640B98F D6EC56DA 2D0384DE 71C5C73E


    temp =
                           458CFE66 103B99E5 F76853E8 AD6B7D35
```

```
        EDEAED91 4B58D2A4 8FDC6735 959CC6BE 0CA35FFF 9E90B25D
        825B1399 7453576C 2640B98F D6EC56DA 2D0384DE 71C5C73E


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 0090710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


    Hash(counter||no_of_bits_to_return||input_string) is
                           A74A55CD 25DDE339 128FE35F D5BFB9FF
        FFC9A246 25A1ECD4 517EC083 ADB5D61B 2ADF04CE 914C4486
        5E0A96FC FF9CAD70 0FF4902F 07B21CC2 402F9894 ABFD9F78


    temp =
                             458CFE 66103B99 E5F76853 E8AD6B7D
        35EDEAED 914B58D2 A48FDC67 35959CC6 BE0CA35F FF9E90B2
        5D825B13 99745357 6C2640B9 8FD6EC56 DA2D0384 DE71C5C7
        3EA74A55 CD25DDE3 39128FE3 5FD5BFB9 FFFFC9A2 4625A1EC
        D4517EC0 83ADB5D6 1B2ADF04 CE914C44 865E0A96 FCFF9CAD


  C is
                             458CFE 66103B99 E5F76853 E8AD6B7D
        35EDEAED 914B58D2 A48FDC67 35959CC6 BE0CA35F FF9E90B2
        5D825B13 99745357 6C2640B9 8FD6EC56 DA2D0384 DE71C5C7
        3EA74A55 CD25DDE3 39128FE3 5FD5BFB9 FFFFC9A2 4625A1EC
        D4517EC0 83ADB5D6 1B2ADF04 CE914C44 865E0A96 FCFF9CAD


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>
```

```
---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            90710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


    w_i is
                          22EB93A6 7911DA73 85D9180C 78127DE1
        A04FF713 114C07C9 C615F7CC 5EF72744 A2DDCD7C 3CB85E65
        DED8EF5F 240FBDCB EBBDE2BA AC8ECF7D CBC8AC33 3E54607A


    W is
                          22EB93A6 7911DA73 85D9180C 78127DE1
        A04FF713 114C07C9 C615F7CC 5EF72744 A2DDCD7C 3CB85E65
        DED8EF5F 240FBDCB EBBDE2BA AC8ECF7D CBC8AC33 3E54607A


    ------------

    i = 2

    data is
                            90710E B688DF01 84891E9A E5B09960
        22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
        7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
        8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
        05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657D


    w_i is
                          D41DC495 D83DF72A 05EF55B1 27C1441C
        9A0EFFDA 2C7954DB 6C2D0434 2EB812E5 E0B11D6C 395F41ED
        A2702ECE 5BA479E2 DFA18F95 30974926 36C12FE3 0CE5C968
```

```
  W is
                                              22EB93A6 7911DA73
       85D9180C 78127DE1 A04FF713 114C07C9 C615F7CC 5EF72744
       A2DDCD7C 3CB85E65 DED8EF5F 240FBDCB EBBDE2BA AC8ECF7D
       CBC8AC33 3E54607A D41DC495 D83DF72A 05EF55B1 27C1441C
       9A0EFFDA 2C7954DB 6C2D0434 2EB812E5 E0B11D6C 395F41ED
       A2702ECE 5BA479E2 DFA18F95 30974926 36C12FE3 0CE5C968


  returned_bits is
                                              22EB93A6 7911DA73
       85D9180C 78127DE1 A04FF713 114C07C9 C615F7CC 5EF72744
       A2DDCD7C 3CB85E65 DED8EF5F 240FBDCB EBBDE2BA AC8ECF7D
       CBC8AC33 3E54607A D41DC495 D83DF72A 05EF55B1 27C1441C
       9A0EFFDA 2C7954DB 6C2D0434 2EB812E5 E0B11D6C 395F41ED
       A2702ECE 5BA479E2 DFA18F95 30974926 36C12FE3 0CE5C968


---------------------------

  Update V

    0x03||V is
                          0390710E B688DF01 84891E9A E5B09960
       22A3CA8E 79D7769C E75B00BA F2E6D6EA B7761DC6 FB1E76DB
       7177737E 4441F0AF 586138E4 3CA81E70 D23F71DD 61CCF5FA
       8D46829A C7E211C7 6E9391E9 149A96C5 F0FC5239 BEBDB5CD
       05F22E0B 8DA207A4 08C44975 D7F1894E C23A47A0 47B8657C


    H is
                          DE0335C1 4096439E 3FA51263 D05A0A38
       290A1B62 938F241B 39364DA5 21AD1132 EF54EE5B 2D9B8206
       AF5F7051 283BB5CB 28EE232C 4F216171 E2DEA414 78400EFE


  Updated values

  V is
                            D5FE0D 1C991A9B 6A8086EE CE5E04DD
       5891B57C 0B22CF6F 8BEADD22 287C73B1 7582C126 FABD078D
       CEF9CE91 DDB64407 A28AAF5F 0D154E65 EC1187C6 1098C5F9
       F4F7E853 289713C5 E0DC6F71 961D67B2 E0510A37 327ED9C0
       89A31D1D 398B7345 4CDD4BA6 F5A43705 2B76F64B BCF81128
```

```
  reseed_counter is
                                                  0000 00000002


rnd_val is
                                                22EB93A6 7911DA73
        85D9180C 78127DE1 A04FF713 114C07C9 C615F7CC 5EF72744
        A2DDCD7C 3CB85E65 DED8EF5F 240FBDCB EBBDE2BA AC8ECF7D
        CBC8AC33 3E54607A D41DC495 D83DF72A 05EF55B1 27C1441C
        9A0EFFDA 2C7954DB 6C2D0434 2EB812E5 E0B11D6C 395F41ED
        A2702ECE 5BA479E2 DFA18F95 30974926 36C12FE3 0CE5C968


------------------------------------------------------------

Second call to Generate

************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

Generate FAILED: Reseed is required
------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input <empty>

---------------------------

  Hash_df - Generate seed(which is V) - Step 2
```

```
seed_material is
                                                01D5FE 0D1C991A
    9B6A8086 EECE5E04 DD5891B5 7C0B22CF 6F8BEADD 22287C73
    B17582C1 26FABD07 8DCEF9CE 91DDB644 07A28AAF 5F0D154E
    65EC1187 C61098C5 F9F4F7E8 53289713 C5E0DC6F 71961D67
    B2E0510A 37327ED9 C089A31D 1D398B73 454CDD4B A6F5A437
    052B76F6 4BBCF811 28C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                 01000003 7801D5FE 0D1C991A
    9B6A8086 EECE5E04 DD5891B5 7C0B22CF 6F8BEADD 22287C73
    B17582C1 26FABD07 8DCEF9CE 91DDB644 07A28AAF 5F0D154E
    65EC1187 C61098C5 F9F4F7E8 53289713 C5E0DC6F 71961D67
    B2E0510A 37327ED9 C089A31D 1D398B73 454CDD4B A6F5A437
    052B76F6 4BBCF811 28C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Hash(counter||no_of_bits_to_return||input_string) is
                       53AA08A1 A34FCCBD 82A0817A F3C88C35
    49BCDFCB DFBC1D74 08B137E5 0B3ABA20 0D1524B5 BCA3138F
    77C45377 B501948B 2A4C5AD5 1BE5F99E 9AE264A3 2AEFE040


temp =
                       53AA08A1 A34FCCBD 82A0817A F3C88C35
    49BCDFCB DFBC1D74 08B137E5 0B3ABA20 0D1524B5 BCA3138F
    77C45377 B501948B 2A4C5AD5 1BE5F99E 9AE264A3 2AEFE040


------------
```

```
    i = 2

    counter||no_of_bits_to_return||input_string is
                                  02000003 7801D5FE 0D1C991A
        9B6A8086 EECE5E04 DD5891B5 7C0B22CF 6F8BEADD 22287C73
        B17582C1 26FABD07 8DCEF9CE 91DDB644 07A28AAF 5F0D154E
        65EC1187 C61098C5 F9F4F7E8 53289713 C5E0DC6F 71961D67
        B2E0510A 37327ED9 C089A31D 1D398B73 454CDD4B A6F5A437
        052B76F6 4BBCF811 28C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Hash(counter||no_of_bits_to_return||input_string) is
                           39A298BE 17D00D28 8868EA39 7B9CF3F3
        FC352224 74AB0B61 15E44543 4AAB903B 4611A783 0734A7AF
        5A36DDE2 3C45BDEC 2B2ACB7D 047D5246 3537076A 0A6FF410


    temp =
                             53AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
        6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


  V is
                             53AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
        6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


--------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           0053AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
```

```
    6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 0053AA08 A1A34FCC BD82A081 7AF3C88C
    3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
    8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
    4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
    6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


Hash(counter||no_of_bits_to_return||input_string) is
                     C0D57BB6 D50B2114 4F2FFFEC 22B980F1
    0317AD7C A1814A87 CE8000B1 6C56D396 9F54F093 201CC480
    85360AA0 DAB042C8 8ED611B9 615748A4 9A73869C 3C0052CC


temp =
                     C0D57BB6 D50B2114 4F2FFFEC 22B980F1
    0317AD7C A1814A87 CE8000B1 6C56D396 9F54F093 201CC480
    85360AA0 DAB042C8 8ED611B9 615748A4 9A73869C 3C0052CC


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 0053AA08 A1A34FCC BD82A081 7AF3C88C
    3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
    8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
    4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
    6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


Hash(counter||no_of_bits_to_return||input_string) is
                     B6390CA9 72DE5FD8 51C4D013 8172E71B
    47EE2D77 A622962B 7A47E3E6 8FE8C5C7 4D809631 DA6D8F45
    E235F725 903499A3 676CD633 AC73AFFC C895889E 4CD7E12E
```

```
    temp =
                            C0D57B B6D50B21 144F2FFF EC22B980
        F10317AD 7CA1814A 87CE8000 B16C56D3 969F54F0 93201CC4
        8085360A A0DAB042 C88ED611 B9615748 A49A7386 9C3C0052
        CCB6390C A972DE5F D851C4D0 138172E7 1B47EE2D 77A62296
        2B7A47E3 E68FE8C5 C74D8096 31DA6D8F 45E235F7 25903499


  C is
                            C0D57B B6D50B21 144F2FFF EC22B980
        F10317AD 7CA1814A 87CE8000 B16C56D3 969F54F0 93201CC4
        8085360A A0DAB042 C88ED611 B9615748 A49A7386 9C3C0052
        CCB6390C A972DE5F D851C4D0 138172E7 1B47EE2D 77A62296
        2B7A47E3 E68FE8C5 C74D8096 31DA6D8F 45E235F7 25903499


**************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

----------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            53AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
        6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


    w_i is
                           E66698CF BF1B3F2E 919C0303 6E584EAA
        81CF1C66 66240AF0 5F706370 43733954 D8A1E5A6 6A04C53C
```

```
        6900FDC1 45D4A3A8 0A31F586 8ACE9AC9 4E14E205 1F624A05


    W is
                            E66698CF BF1B3F2E 919C0303 6E584EAA
        81CF1C66 66240AF0 5F706370 43733954 D8A1E5A6 6A04C53C
        6900FDC1 45D4A3A8 0A31F586 8ACE9AC9 4E14E205 1F624A05


    ------------

    i = 2

    data is
                              53AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
        6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BE


    w_i is
                            EEA1F8B6 84AA5410 BCE315E7 6EA07C71
        5D6F3473 1320FF0D CF78D795 E6EFA2DF 92B98BE6 36CDFBA2
        9008DD39 2112AEC2 02F2E481 CB9D83F9 87FEA69C D1B368BB


    W is
                                                E66698CF BF1B3F2E
        919C0303 6E584EAA 81CF1C66 66240AF0 5F706370 43733954
        D8A1E5A6 6A04C53C 6900FDC1 45D4A3A8 0A31F586 8ACE9AC9
        4E14E205 1F624A05 EEA1F8B6 84AA5410 BCE315E7 6EA07C71
        5D6F3473 1320FF0D CF78D795 E6EFA2DF 92B98BE6 36CDFBA2
        9008DD39 2112AEC2 02F2E481 CB9D83F9 87FEA69C D1B368BB


  returned_bits is
                                                E66698CF BF1B3F2E
        919C0303 6E584EAA 81CF1C66 66240AF0 5F706370 43733954
        D8A1E5A6 6A04C53C 6900FDC1 45D4A3A8 0A31F586 8ACE9AC9
        4E14E205 1F624A05 EEA1F8B6 84AA5410 BCE315E7 6EA07C71
        5D6F3473 1320FF0D CF78D795 E6EFA2DF 92B98BE6 36CDFBA2
        9008DD39 2112AEC2 02F2E481 CB9D83F9 87FEA69C D1B368BB


--------------------------
```

```
  Update V

    0x03||V is
                          0353AA08 A1A34FCC BD82A081 7AF3C88C
        3549BCDF CBDFBC1D 7408B137 E50B3ABA 200D1524 B5BCA313
        8F77C453 77B50194 8B2A4C5A D51BE5F9 9E9AE264 A32AEFE0
        4039A298 BE17D00D 288868EA 397B9CF3 F3FC3522 2474AB0B
        6115E445 434AAB90 3B4611A7 830734A7 AF5A36DD E23C45BD


    H is
                          9570EF86 9B34C000 8DFC9B32 5EB45FB7
        F4B68DF6 244CA3C5 49A08912 7263A47D A717A227 4105C9E8
        87C48A0D C5FD6557 269EAA07 20C14DB4 69FEE6AF 34355EC0


  Updated values

  V is
                            147F84 58785AED D1D1D081 6716820D
        264CD48D 48813D67 FBD73138 9677918D B6AC6A15 48DCBFD8
        0FFCFA5E 188FB1D7 E92A11F3 29B1FD42 D131F11D 9E1B4FEB
        01A6699B 8BD75232 4A7AB6CC BF60B458 B65BC576 DD20978A
        1454B636 EFD7F9AD 29323C44 D5A2EFEB 5F3B5384 3C01D917


  reseed_counter is
                                                0000 00000002


rnd_val is
                                              E66698CF BF1B3F2E
        919C0303 6E584EAA 81CF1C66 66240AF0 5F706370 43733954
        D8A1E5A6 6A04C53C 6900FDC1 45D4A3A8 0A31F586 8ACE9AC9
        4E14E205 1F624A05 EEA1F8B6 84AA5410 BCE315E7 6EA07C71
        5D6F3473 1320FF0D CF78D795 E6EFA2DF 92B98BE6 36CDFBA2
        9008DD39 2112AEC2 02F2E481 CB9D83F9 87FEA69C D1B368BB


################################################################

Hash_DRBG

    Requested Security Strength = 256
```

```
Requested Hash Algorithm = SHA-512

prediction_resistance_flag = "ENABLED"
EntropyInput =
                          000102 03040506 0708090A 0B0C0D0E
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
    3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                          808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                          C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                        20212223 24252627 28292A2B 2C2D2E2F


PersonalizationString =
                          404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                          606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##############################################################

**************************************************************

Hash_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
```

```
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
                                                      010000
    03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


Hash(counter||no_of_bits_to_return||input_string) is
                      E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


temp =
                      E5A5C585 D6A9E11C 58581F35 14EE19A7
    048CF096 A3E9B139 D9C0A2C0 67931041 4073C104 E2F6F8A3
    7C7C666E 11FF4439 33ABA1CF AD4C620C DFF5DA8C 0860CEEE


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
```

```
        03780001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    Hash(counter||no_of_bits_to_return||input_string) is
                            80B87195 7508538D 2D87A4A3 B5728ADB
        4191974A 384F323D 2E585869 5C152F99 D0E8CF4C B41BC2A6
        12955B4C 4838B9FB EB00568D 36F727E1 742FF774 E8542A4B


    temp =
                              E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


  V is
                              E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                            00E5A5C5 85D6A9E1 1C58581F 3514EE19
        A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
        A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
        EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
        3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9
```

```
no_of_bits_to_return = 888

------------

i = 1

counter||no_of_bits_to_return||input_string is
          01 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
    A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
    A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
    EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
    3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


Hash(counter||no_of_bits_to_return||input_string) is
                      0C193DBC 1942C121 C63513ED 95ECA91C
    62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
    421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


temp =
                      0C193DBC 1942C121 C63513ED 95ECA91C
    62C55031 7506462C 47B0F34F 99716F36 EAD9FF51 ACAB423C
    421CAB62 DF4D8C79 2E38D533 9D60AA24 0292E134 A249A577


------------

i = 2

counter||no_of_bits_to_return||input_string is
          02 00000378 00E5A5C5 85D6A9E1 1C58581F 3514EE19
    A7048CF0 96A3E9B1 39D9C0A2 C0679310 414073C1 04E2F6F8
    A37C7C66 6E11FF44 3933ABA1 CFAD4C62 0CDFF5DA 8C0860CE
    EE80B871 95750853 8D2D87A4 A3B5728A DB419197 4A384F32
    3D2E5858 695C152F 99D0E8CF 4CB41BC2 A612955B 4C4838B9


Hash(counter||no_of_bits_to_return||input_string) is
                      0176FE93 A4C199A2 258615DD A840AE6F
    C2E7DB39 1315119E 57774F94 396C81F5 F8D4835D 618D960B
    297E97F1 A21B35E3 E450A877 4819D918 961DFC01 FFC73630


temp =
                        0C193D BC1942C1 21C63513 ED95ECA9
```

```
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


  C is
                            0C193D BC1942C1 21C63513 ED95ECA9
        1C62C550 31750646 2C47B0F3 4F99716F 36EAD9FF 51ACAB42
        3C421CAB 62DF4D8C 792E38D5 339D60AA 240292E1 34A249A5
        770176FE 93A4C199 A2258615 DDA840AE 6FC2E7DB 39131511
        9E57774F 94396C81 F5F8D483 5D618D96 0B297E97 F1A21B35


----------------------------------------------------------------

First call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  additional_input
```

```
                          606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


----------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            01E5 A5C585D6 A9E11C58 581F3514 EE19A704 8CF096A3
        E9B139D9 C0A2C067 93104140 73C104E2 F6F8A37C 7C666E11
        FF443933 ABA1CFAD 4C620CDF F5DA8C08 60CEEE80 B8719575
        08538D2D 87A4A3B5 728ADB41 91974A38 4F323D2E 5858695C
        152F99D0 E8CF4CB4 1BC2A612 955B4C48 38B98081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                        010000
        037801E5 A5C585D6 A9E11C58 581F3514 EE19A704 8CF096A3
        E9B139D9 C0A2C067 93104140 73C104E2 F6F8A37C 7C666E11
        FF443933 ABA1CFAD 4C620CDF F5DA8C08 60CEEE80 B8719575
        08538D2D 87A4A3B5 728ADB41 91974A38 4F323D2E 5858695C
        152F99D0 E8CF4CB4 1BC2A612 955B4C48 38B98081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
```

```
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
                      04F0F3B8 9552F8C0 006FE2BA 33D069A4
    08885EB0 AE9A9618 F8381C83 2B8A6FD8 1FFFFF52 5C4BD7E2
    E3EDE6ED 7AC02DED 66DFBFA0 50134D3B 1A828DA2 D4818482


temp =
                      04F0F3B8 9552F8C0 006FE2BA 33D069A4
    08885EB0 AE9A9618 F8381C83 2B8A6FD8 1FFFFF52 5C4BD7E2
    E3EDE6ED 7AC02DED 66DFBFA0 50134D3B 1A828DA2 D4818482


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    037801E5 A5C585D6 A9E11C58 581F3514 EE19A704 8CF096A3
    E9B139D9 C0A2C067 93104140 73C104E2 F6F8A37C 7C666E11
    FF443933 ABA1CFAD 4C620CDF F5DA8C08 60CEEE80 B8719575
    08538D2D 87A4A3B5 728ADB41 91974A38 4F323D2E 5858695C
    152F99D0 E8CF4CB4 1BC2A612 955B4C48 38B98081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Hash(counter||no_of_bits_to_return||input_string) is
                      6BDA0EED A45C794A 18B04CED 7E8AFAAE
    88B743FE 0833735F C59704C4 3252DAC6 76A4C91B 8D3E78DC
    41782C01 96D73DFD 11C631F3 7B382D42 D0F77A4A A040E727
```

```
    temp =
                            04F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


  V is
                            04F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                           0004F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 0004F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


    Hash(counter||no_of_bits_to_return||input_string) is
                           76878CDA 0362CAD7 DB3F3D92 17093D29
        602FF901 5D2D87A1 8EE4B2F2 88947D33 4565E066 F7E104AC
        DDBC773B 1486541E D12488D3 B70FCD34 AE68F5AD 78464189
```

```
    temp =
                          76878CDA 0362CAD7 DB3F3D92 17093D29
        602FF901 5D2D87A1 8EE4B2F2 88947D33 4565E066 F7E104AC
        DDBC773B 1486541E D12488D3 B70FCD34 AE68F5AD 78464189


    ------------

    i = 2

    counter||no_of_bits_to_return||input_string is
              02 00000378 0004F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


    Hash(counter||no_of_bits_to_return||input_string) is
                          A8053FAF A58CA32F EA5C4F5C 7F3AEF74
        D699AD57 13E64377 430E4528 E54B6EE6 CE4DB441 907CA52A
        3F90A768 7AA90E89 4E60E54B C1E4E3E5 101AD0F5 CC8DD1E0


    temp =
                            76878C DA0362CA D7DB3F3D 9217093D
        29602FF9 015D2D87 A18EE4B2 F288947D 334565E0 66F7E104
        ACDDBC77 3B148654 1ED12488 D3B70FCD 34AE68F5 AD784641
        89A8053F AFA58CA3 2FEA5C4F 5C7F3AEF 74D699AD 5713E643
        77430E45 28E54B6E E6CE4DB4 41907CA5 2A3F90A7 687AA90E


  C is
                            76878C DA0362CA D7DB3F3D 9217093D
        29602FF9 015D2D87 A18EE4B2 F288947D 334565E0 66F7E104
        ACDDBC77 3B148654 1ED12488 D3B70FCD 34AE68F5 AD784641
        89A8053F AFA58CA3 2FEA5C4F 5C7F3AEF 74D699AD 5713E643
        77430E45 28E54B6E E6CE4DB4 41907CA5 2A3F90A7 687AA90E


**************************************************************

Hash_DRBG_Generate_algorithm
```

```
  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                           04F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


    w_i is
                          7596A763 72308BD5 A5613439 934678B3
        5521A94D 81ABFE63 A21ACF61 ABB88B61 E86A12C3 7F308F2B
        BBE32BE4 B38D03AE 80838649 4D70EF52 E9E1365D D18B7784


    W is
                          7596A763 72308BD5 A5613439 934678B3
        5521A94D 81ABFE63 A21ACF61 ABB88B61 E86A12C3 7F308F2B
        BBE32BE4 B38D03AE 80838649 4D70EF52 E9E1365D D18B7784


    ------------

    i = 2

    data is
                           04F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73E
```

```
    w_i is
                          CAB826F3 1D47579E 4D57F69D 8BF3152B
        95741946 CEBE5857 1DF58ED3 9980D9AF 44E69F01 E8989759
        8E401711 01A0E330 2838E0AD 9E849C01 988993CF 9F6E5263


    W is
                                               7596A763 72308BD5
        A5613439 934678B3 5521A94D 81ABFE63 A21ACF61 ABB88B61
        E86A12C3 7F308F2B BBE32BE4 B38D03AE 80838649 4D70EF52
        E9E1365D D18B7784 CAB826F3 1D47579E 4D57F69D 8BF3152B
        95741946 CEBE5857 1DF58ED3 9980D9AF 44E69F01 E8989759
        8E401711 01A0E330 2838E0AD 9E849C01 988993CF 9F6E5263


  returned_bits is
                                               7596A763 72308BD5
        A5613439 934678B3 5521A94D 81ABFE63 A21ACF61 ABB88B61
        E86A12C3 7F308F2B BBE32BE4 B38D03AE 80838649 4D70EF52
        E9E1365D D18B7784 CAB826F3 1D47579E 4D57F69D 8BF3152B
        95741946 CEBE5857 1DF58ED3 9980D9AF 44E69F01 E8989759
        8E401711 01A0E330 2838E0AD 9E849C01 988993CF 9F6E5263


--------------------------

  Update V

    0x03||V is
                          0304F0F3 B89552F8 C0006FE2 BA33D069
        A408885E B0AE9A96 18F8381C 832B8A6F D81FFFFF 525C4BD7
        E2E3EDE6 ED7AC02D ED66DFBF A050134D 3B1A828D A2D48184
        826BDA0E EDA45C79 4A18B04C ED7E8AFA AE88B743 FE083373
        5FC59704 C43252DA C676A4C9 1B8D3E78 DC41782C 0196D73D


    H is
                          570B7582 C7A57D2D 0D1631DD 208A507A
        9B9BE4AE 3676F474 C31F49B0 AE96CD64 33D19AEB 51584CEA
        F532A3C7 9E0C7208 17510AAB 6AF67458 9AB9180B 51620620


  Updated values

  V is
                             7B7880 9298B5C3 97DBAF20 4C4AD9A6
```

```
        CD68B857 B20BC81D BA871CCF 75B41EED 0B6565DF B9542CDC
        8FC1AA5E 288F4682 634379CB 3BACA047 7CDF1D60 70D71840
        A7AFC3FC D3C0DD91 3D22564C F894934E 5730EBDC A67466A1
        CC3B4911 8B241051 C495FD28 C8142F76 A13A20DE BB73866C


  reseed_counter is
                                                0000 00000002


rnd_val is
                                             7596A763 72308BD5
        A5613439 934678B3 5521A94D 81ABFE63 A21ACF61 ABB88B61
        E86A12C3 7F308F2B BBE32BE4 B38D03AE 80838649 4D70EF52
        E9E1365D D18B7784 CAB826F3 1D47579E 4D57F69D 8BF3152B
        95741946 CEBE5857 1DF58ED3 9980D9AF 44E69F01 E8989759
        8E401711 01A0E330 2838E0AD 9E849C01 988993CF 9F6E5263


----------------------------------------------------------------

Second call to Generate

****************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
----------------------------------------------------------------

Hash_DRBG_Reseed_algorithm

  entropy_input
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
```

```
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  additional_input
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


--------------------------

  Hash_df - Generate seed(which is V) - Step 2

    seed_material is
            017B 78809298 B5C397DB AF204C4A D9A6CD68 B857B20B
        C81DBA87 1CCF75B4 1EED0B65 65DFB954 2CDC8FC1 AA5E288F
        46826343 79CB3BAC A0477CDF 1D6070D7 1840A7AF C3FCD3C0
        DD913D22 564CF894 934E5730 EBDCA674 66A1CC3B 49118B24
        1051C495 FD28C814 2F76A13A 20DEBB73 866CC0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                          010000
        0378017B 78809298 B5C397DB AF204C4A D9A6CD68 B857B20B
        C81DBA87 1CCF75B4 1EED0B65 65DFB954 2CDC8FC1 AA5E288F
        46826343 79CB3BAC A0477CDF 1D6070D7 1840A7AF C3FCD3C0
        DD913D22 564CF894 934E5730 EBDCA674 66A1CC3B 49118B24
        1051C495 FD28C814 2F76A13A 20DEBB73 866CC0C1 C2C3C4C5
```

```
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Hash(counter||no_of_bits_to_return||input_string) is
                    913CA013 D788EAD1 4EDFA1A5 7857414B
    1D68E30D 85930C99 4EC8DEEE 1B2F7E74 4CAC3288 A442A4CD
    55A41FD1 A0B265B4 90812D90 00FFCC62 82474D78 8DFB3781


temp =
                    913CA013 D788EAD1 4EDFA1A5 7857414B
    1D68E30D 85930C99 4EC8DEEE 1B2F7E74 4CAC3288 A442A4CD
    55A41FD1 A0B265B4 90812D90 00FFCC62 82474D78 8DFB3781


------------

i = 2

counter||no_of_bits_to_return||input_string is
                                                      020000
    0378017B 78809298 B5C397DB AF204C4A D9A6CD68 B857B20B
    C81DBA87 1CCF75B4 1EED0B65 65DFB954 2CDC8FC1 AA5E288F
    46826343 79CB3BAC A0477CDF 1D6070D7 1840A7AF C3FCD3C0
    DD913D22 564CF894 934E5730 EBDCA674 66A1CC3B 49118B24
    1051C495 FD28C814 2F76A13A 20DEBB73 866CC0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Hash(counter||no_of_bits_to_return||input_string) is
```

```
                        E7F19451 0674954D 9E49CEAC 2FD98109
        E08BEBBF FBBBA78C 16FEB723 64F49334 6BB916DB 78563AAD
        BD51A07D 55315AFB 4612F770 B4936987 47C3EC71 9C7BF6C0


    temp =
                          913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


  V is
                          913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


---------------------------

  Hash_df - Generate C - Step 4

    0x00||V is
                        00913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


    no_of_bits_to_return = 888

    ------------

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000378 00913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A
```

```
  Hash(counter||no_of_bits_to_return||input_string) is
                        9FA80ADB 6DC1CD99 3C00413B A974350B
      49725E33 4A188BEB 0A992B22 5C49DE64 CFE92B47 8B7589B6
      0649255A 304CA2EB 11BF7BB7 9021A86B A4F7BCD9 3679B8F7


  temp =
                        9FA80ADB 6DC1CD99 3C00413B A974350B
      49725E33 4A188BEB 0A992B22 5C49DE64 CFE92B47 8B7589B6
      0649255A 304CA2EB 11BF7BB7 9021A86B A4F7BCD9 3679B8F7


  ------------

  i = 2

  counter||no_of_bits_to_return||input_string is
            02 00000378 00913CA0 13D788EA D14EDFA1 A5785741
      4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
      CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
      81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
      8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


  Hash(counter||no_of_bits_to_return||input_string) is
                        356ED503 70D4A92A 84F44891 788408BE
      D41B4F3C 71B4FD1F 90D1480E 506B96A4 180D945C E02C4369
      876C3994 CA9463D6 887B6B27 457709FF FFCA9CE8 CE90D484


  temp =
                          9FA80A DB6DC1CD 993C0041 3BA97435
      0B49725E 334A188B EB0A992B 225C49DE 64CFE92B 478B7589
      B6064925 5A304CA2 EB11BF7B B79021A8 6BA4F7BC D93679B8
      F7356ED5 0370D4A9 2A84F448 91788408 BED41B4F 3C71B4FD
      1F90D148 0E506B96 A4180D94 5CE02C43 69876C39 94CA9463


C is
                          9FA80A DB6DC1CD 993C0041 3BA97435
      0B49725E 334A188B EB0A992B 225C49DE 64CFE92B 478B7589
      B6064925 5A304CA2 EB11BF7B B79021A8 6BA4F7BC D93679B8
      F7356ED5 0370D4A9 2A84F448 91788408 BED41B4F 3C71B4FD
      1F90D148 0E506B96 A4180D94 5CE02C43 69876C39 94CA9463
```

```
*************************************************************

Hash_DRBG_Generate_algorithm

  requested_number_of_bits = 1024

  additional_input <empty>

---------------------------

  Hashgen

    requested_no_of_bits  = 1024

    ------------

    i = 1

    data is
                            913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


    w_i is
                          DBE5EE36 FCD85301 303E1C36 17C1AC5E
        23C08885 D0BEFAAD 0C85A0D8 9F85B9F1 6ECE3D88 A24EB965
        04F2F13E FA704962 1782F5DE 2C416A0D 294CCFE5 3545C4E3


    W is
                          DBE5EE36 FCD85301 303E1C36 17C1AC5E
        23C08885 D0BEFAAD 0C85A0D8 9F85B9F1 6ECE3D88 A24EB965
        04F2F13E FA704962 1782F5DE 2C416A0D 294CCFE5 3545C4E3


    ------------

    i = 2

    data is
                            913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
```

```
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315B


    w_i is
                         09C48E1E 285A2B82 9A574B72 B3C2FBE1
        34D01E37 06B486F2 401B9820 E17298A3 42666918 E15B8462
        87F8C5AF 2D96B20F AF3D0BB3 92E15F4A 06CDB0DE CD1B6AD7


    W is
                                           DBE5EE36 FCD85301
        303E1C36 17C1AC5E 23C08885 D0BEFAAD 0C85A0D8 9F85B9F1
        6ECE3D88 A24EB965 04F2F13E FA704962 1782F5DE 2C416A0D
        294CCFE5 3545C4E3 09C48E1E 285A2B82 9A574B72 B3C2FBE1
        34D01E37 06B486F2 401B9820 E17298A3 42666918 E15B8462
        87F8C5AF 2D96B20F AF3D0BB3 92E15F4A 06CDB0DE CD1B6AD7


  returned_bits is
                                           DBE5EE36 FCD85301
        303E1C36 17C1AC5E 23C08885 D0BEFAAD 0C85A0D8 9F85B9F1
        6ECE3D88 A24EB965 04F2F13E FA704962 1782F5DE 2C416A0D
        294CCFE5 3545C4E3 09C48E1E 285A2B82 9A574B72 B3C2FBE1
        34D01E37 06B486F2 401B9820 E17298A3 42666918 E15B8462
        87F8C5AF 2D96B20F AF3D0BB3 92E15F4A 06CDB0DE CD1B6AD7


---------------------------

  Update V

    0x03||V is
                         03913CA0 13D788EA D14EDFA1 A5785741
        4B1D68E3 0D85930C 994EC8DE EE1B2F7E 744CAC32 88A442A4
        CD55A41F D1A0B265 B490812D 9000FFCC 6282474D 788DFB37
        81E7F194 51067495 4D9E49CE AC2FD981 09E08BEB BFFBBBA7
        8C16FEB7 2364F493 346BB916 DB78563A ADBD51A0 7D55315A


    H is
                         73FD2839 3EFADC11 1ADBC674 E19D8341
        76345539 6AC56861 F86260C7 4918A450 5D41B9D7 5FC254C0
        2EE70292 ED511374 3F2C179A A23149FC 18F27654 98319719
```

Updated values

V is

```
                          30E4AA EF454AB8 6A8ADFE2 E121CB76
       5666DB41 40CFAB98 8459620A 1077795C D91C955D D02FB82E
       835BED45 2BD0FF09 139F68E2 868BFD85 E903057F 3361F831
       EF51B5A2 BF3CB1A0 70859EDE 86C101DA 25F66112 5C2FC564
       DA8ED292 1F06739E 17AFDE45 DA89CC7A 3037342E AA515CD7
```

reseed_counter is

```
                                                0000 00000002
```

rnd_val is

```
                                           DBE5EE36 FCD85301
       303E1C36 17C1AC5E 23C08885 D0BEFAAD 0C85A0D8 9F85B9F1
       6ECE3D88 A24EB965 04F2F13E FA704962 1782F5DE 2C416A0D
       294CCFE5 3545C4E3 09C48E1E 285A2B82 9A574B72 B3C2FBE1
       34D01E37 06B486F2 401B9820 E17298A3 42666918 E15B8462
       87F8C5AF 2D96B20F AF3D0BB3 92E15F4A 06CDB0DE CD1B6AD7
```