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

  Elliptic Curve Digital Signature Algorithm
    Curve = K-163
    Hash Length = 160

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

================================================================

Private Key Generation

N is
            0004 00000000 00000000 00020108 A2E0CC0D 99F8A5EF


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

C is
                 7FF9959E 88692406 041273AB 70E00B88 EA18C9E5


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

D is
                 7FF9959E 88692406 041273AB 70E00B88 EA18C9E6


Q_x is
                 2CC266F6 D8373650 0418D2E0 0CE2D07C 2FF8F734


Q_y is
            0002 8553EA06 76C40D57 7DCFE525 9968B341 A1D33AF2


================================================================

Private Key Generation

N is
            0004 00000000 00000000 00020108 A2E0CC0D 99F8A5EF


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

C is
                 1E7EC8C9 8AB49FC1 4E1BC841 EBF61A0A D0961471


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

K is
                 1E7EC8C9 8AB49FC1 4E1BC841 EBF61A0A D0961472


================================================================

Signature Generation

msg is "Example of ECDSA with K-163"
Hash length = 160
D is
                 7FF9959E 88692406 041273AB 70E00B88 EA18C9E6


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

```
R_x is
            0007 18EF5EF3 76B8F530 1B5FD2A7 61989C41 7807A275


r(int) is 45268588399962317285010730840293109529346257050 94
E is
                590D17DF 8BF17246 EAF975B4 1864ABCC 7A747021


Kinv is
                39252C5D 41A93673 6CAE1413 DA889249 35F61B58


s(int) is 436976486904949861747941463411152135332914979 4237
---------------------------------------------------------------

Signature:
  R is
            0003 18EF5EF3 76B8F530 1B5DD19E BEB7D033 DE0EFC86


  S is
            0002 FD6B089A F933C881 D4B9FEB3 A550CBDE D50CD7BD


===============================================================

Signature Verification

msg is "Example of ECDSA with K-163"
Hash length = 160
Signature:
  R is
            0003 18EF5EF3 76B8F530 1B5DD19E BEB7D033 DE0EFC86


  S is
            0002 FD6B089A F933C881 D4B9FEB3 A550CBDE D50CD7BD


Public Key:
  Q_x is
                2CC266F6 D8373650 0418D2E0 0CE2D07C 2FF8F734


  Q_y is
            0002 8553EA06 76C40D57 7DCFE525 9968B341 A1D33AF2


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

E is
                590D17DF 8BF17246 EAF975B4 1864ABCC 7A747021


U1 is
            0003 32DD232E F2D65C09 309D52C7 BE1646D4 1FC9DE20


U2 is
            0003 D355DAD4 B1418780 A63A87DA FC06D38B FC287312


R_x is
            0007 18EF5EF3 76B8F530 1B5FD2A7 61989C41 7807A275
```

```
V is
            0003 18EF5EF3 76B8F530 1B5DD19E BEB7D033 DE0EFC86


R' is
            0003 18EF5EF3 76B8F530 1B5DD19E BEB7D033 DE0EFC86


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

Signature is verified


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

  Elliptic Curve Digital Signature Algorithm
    Curve = B-163
    Hash Length = 160

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

=============================================================

Private Key Generation

N is
            0004 00000000 00000000 000292FE 77E70C12 A4234C33


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

C is
            0003 48D138C2 DE9447BD 288FEED1 77222EE3 77FB7BE9


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

D is
            0003 48D138C2 DE9447BD 288FEED1 77222EE3 77FB7BEA


Q_x is
            0006 6B015C0B 72B0F81B 1ECBA6F5 8E7545D9 4744644C


Q_y is
                 BA6D4D62 419155B1 86A29784 F4AA4B8E 8E1E7F76


=============================================================

Private Key Generation

N is
            0004 00000000 00000000 000292FE 77E70C12 A4234C33


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

C is
                 8ED0F93F 7D492BB3 991847D0 E96F9CC3 947259A9


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

K is
```

8ED0F93F 7D492BB3 991847D0 E96F9CC3 947259AA

==========

Signature Generation

msg is "Example of ECDSA with B-163"
Hash length = 160
D is
0003 48D138C2 DE9447BD 288FEED1 77222EE3 77FB7BEA

R_x is
0007 60938A97 D88B30FD FB2CCE1A 4C59783A D0ED8FDE

r(int) is 493585830870191330854598333053045181980719777 4763
E is
728D59BB E028509D D5D2CE48 0F458E29 25232AC3

Kinv is
0003 6DC66491 68421137 3AAA8BD1 6024DD0A 12A8FF11

s(int) is 234343619976773062681397368240188957691231492 4924

Signature:
R is
0003 60938A97 D88B30FD FB2A3B1B D4726C28 2CCA43AB

S is
0001 9A7B5043 D93A13D7 14B4717F C0698E67 91CF7F7C

==========

Signature Verification

msg is "Example of ECDSA with B-163"
Hash length = 160
Signature:
R is
0003 60938A97 D88B30FD FB2A3B1B D4726C28 2CCA43AB

S is
0001 9A7B5043 D93A13D7 14B4717F C0698E67 91CF7F7C

Public Key:
Q_x is
0006 6B015C0B 72B0F81B 1ECBA6F5 8E7545D9 4744644C

Q_y is
BA6D4D62 419155B1 86A29784 F4AA4B8E 8E1E7F76

E is

```
                728D59BB E028509D D5D2CE48 0F458E29 25232AC3

U1 is
            0003 C4099DB2 41A80C80 7E02D81B E10955B2 EB2E5D8C

U2 is
            0001 60CCEDAB B7E3E767 A604D8B0 42A65751 708CC262

R_x is
            0007 60938A97 D88B30FD FB2CCE1A 4C59783A D0ED8FDE

V is
            0003 60938A97 D88B30FD FB2A3B1B D4726C28 2CCA43AB

R' is
            0003 60938A97 D88B30FD FB2A3B1B D4726C28 2CCA43AB

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

Signature is verified

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

  Elliptic Curve Digital Signature Algorithm
    Curve = K-233
    Hash Length = 224

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

================================================================

Private Key Generation

N is
                                                0080 00000000
        00000000 00000000 00069D5B B915BCD4 6EFB1AD5 F173ABDF

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

C is
                                                0001 90DA60FE
        3B179B96 611DB7C7 E5217C9A FF0AEE43 5782EBFB 2DFFF27E

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

K is
                                                0001 90DA60FE
        3B179B96 611DB7C7 E5217C9A FF0AEE43 5782EBFB 2DFFF27F

================================================================

Signature Generation

msg is "Example of ECDSA with K-233"
Hash length = 224
D is
                                                    8434613F
```

```
        4B799B4C 26E4D7AB 8E9481B0 4B09E648 C94AFFD1 4B611A20


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

R_x is
                                                01BE A7231662
        E6516F11 E37D59D5 00EAE71D 116E9B7B BCE5964B 88D4CC4D


r(int) is 168911828021030560517169377389207920186627501202122693337121777528235 2
E is
                                                    CB2314B2
        1E913F4D 345AF272 ED611F3E BA003880 56921DA8 A450F731


Kinv is
                                                0075 9A37371C
        026E261A DD7278B8 1EE15D18 E2B0D9BD 1A077AEB F96AA067


s(int) is 31547270105072343068622585060853237243251310833599563458799108700344 74
---------------------------------------------------------------

Signature:
  R is
                                                003E A7231662
        E6516F11 E37D59D5 00D70F09 E62D64FE 6FF445C9 B479C8B0


  S is
                                                0075 03EC8E63
        0386CE36 A6276F22 1BC8EE45 92CCA596 0A1EABE3 BD2A282A


===============================================================

Signature Verification

msg is "Example of ECDSA with K-233"
Hash length = 224
Signature:
  R is
                                                003E A7231662
        E6516F11 E37D59D5 00D70F09 E62D64FE 6FF445C9 B479C8B0


  S is
                                                0075 03EC8E63
        0386CE36 A6276F22 1BC8EE45 92CCA596 0A1EABE3 BD2A282A


Public Key:
  Q_x is
                                                017C 9DD766AE
        FBE4DE4B 15F46DB0 671DC4CA 0767ED51 ECEA9475 7D9C662E


  Q_y is
                                                01CD D7260848
        37AE73C1 1C27D605 C6EB2D5E 31482358 780305C2 522B151B


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

E is
                                                    CB2314B2
```

```
        1E913F4D 345AF272 ED611F3E BA003880 56921DA8 A450F731


U1 is
                                                0043 A8EA5148
        9B412B0A 1CA97865 A12491E8 E144159E 56CDC8BB E201D0D5


U2 is
                                                0036 D6AC76BC
        AC51707F 796E6FA1 CB649F7F D2C69AED 93D01AB7 C8AE35AA


R_x is
                                                01BE A7231662
        E6516F11 E37D59D5 00EAE71D 116E9B7B BCE5964B 88D4CC4D


V is
                                                003E A7231662
        E6516F11 E37D59D5 00D70F09 E62D64FE 6FF445C9 B479C8B0


R' is
                                                003E A7231662
        E6516F11 E37D59D5 00D70F09 E62D64FE 6FF445C9 B479C8B0


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

Signature is verified


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

  Elliptic Curve Digital Signature Algorithm
    Curve = B-233
    Hash Length = 224

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

=============================================================

Private Key Generation

N is
                                                0100 00000000
        00000000 00000000 0013E974 E72F8A69 22031D26 03CFE0D7


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

C is
                                                    8AF6D5A8
        E875977C 7D4BA1F6 11CF7B6D 70B26140 BF84A1CC 281F1B7A


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

D is
                                                    8AF6D5A8
        E875977C 7D4BA1F6 11CF7B6D 70B26140 BF84A1CC 281F1B7B


Q_x is
                                                01D3 AD52D68F
        8383F582 E2BA00F8 9CE16322 11EDC244 40C31798 E0C8ED40
```

```
Q_y is
                                                  006C 3B96CC0E
        6BC59355 A1294E22 DBF1D4B9 071C28DA 1389B6DE BE0E7F43


============================================================

Private Key Generation

N is
                                                  0100 00000000
        00000000 00000000 0013E974 E72F8A69 22031D26 03CFE0D7


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

C is
                                                    8A654829
        17BA18F1 E8B266A3 795B0A3A 09C439FA 6B611E37 123BAF71


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

K is
                                                    8A654829
        17BA18F1 E8B266A3 795B0A3A 09C439FA 6B611E37 123BAF72


============================================================

Signature Generation

msg is "Example of ECDSA with B-233"
Hash length = 224
D is
                                                    8AF6D5A8
        E875977C 7D4BA1F6 11CF7B6D 70B26140 BF84A1CC 281F1B7B


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

R_x is
                                                  0186 806715D9
        620F0A3E 62C1BA59 3D9817B6 DCB23DE8 5BF504C3 26629E63


r(int) is 362615523358434647301127290174911560787530418978383684953535910580980 4
E is
                                                    6A8389D3
        644C7FA9 0D7F57E6 049D0DD4 1B8E473C D296C71D 0FF232B3


Kinv is
                                                  0097 589E4B9B
        7C0F0C1E 58D2AC61 E8297D83 FE7D0017 2E64B7D0 DF207DD9


s(int) is 172770953230472512433035413720275843869066300017311966978215900354993 5
------------------------------------------------------------

Signature:
  R is
                                                  0086 806715D9
        620F0A3E 62C1BA59 3D842E41 F582B37F 39F1E79D 2292BD8C
```

```
  S is
                                                0040 15953986
        1BE6673C 0A3B2E49 F5F6C953 2B60130C 6FC78826 C9E900EF


============================================================

Signature Verification

msg is "Example of ECDSA with B-233"
Hash length = 224
Signature:
  R is
                                                0086 806715D9
        620F0A3E 62C1BA59 3D842E41 F582B37F 39F1E79D 2292BD8C


  S is
                                                0040 15953986
        1BE6673C 0A3B2E49 F5F6C953 2B60130C 6FC78826 C9E900EF


Public Key:
  Q_x is
                                                01D3 AD52D68F
        8383F582 E2BA00F8 9CE16322 11EDC244 40C31798 E0C8ED40


  Q_y is
                                                006C 3B96CC0E
        6BC59355 A1294E22 DBF1D4B9 071C28DA 1389B6DE BE0E7F43


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

E is
                                                    6A8389D3
        644C7FA9 0D7F57E6 049D0DD4 1B8E473C D296C71D 0FF232B3


U1 is
                                                0009 621ACB96
        BA987E23 54A4CA32 73C142BC 963CCE4C B84E17F4 A6A8A3E1


U2 is
                                                006F 64D0192B
        2965749D 0AC29C78 40245CC7 0BDB296F 7E71CFC5 9C069515


R_x is
                                                0186 806715D9
        620F0A3E 62C1BA59 3D9817B6 DCB23DE8 5BF504C3 26629E63


V is
                                                0086 806715D9
        620F0A3E 62C1BA59 3D842E41 F582B37F 39F1E79D 2292BD8C


R' is
                                                0086 806715D9
        620F0A3E 62C1BA59 3D842E41 F582B37F 39F1E79D 2292BD8C


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

```
Signature is verified


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

  Elliptic Curve Digital Signature Algorithm
    Curve = K-283
    Hash Length = 256

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

============================================================

Private Key Generation

N is
                                  01FFFFFF FFFFFFFF FFFFFFFF
        FFFFFFFF FFFFE9AE 2ED07577 265DFF7F 94451E06 1E163C61


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

C is
                                  00069E6D 19F7E454 A83664FF
        49208F60 38EAF842 E164DF42 D0F64948 FF9C94B0 14988328


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

D is
                                  00069E6D 19F7E454 A83664FF
        49208F60 38EAF842 E164DF42 D0F64948 FF9C94B0 14988329


Q_x is
                                  01B64A60 D4A36540 9635AAA2
        7E1708D9 0B839AFA 2D9820E1 2B79C3AF 1094B601 0AAEF5BE


Q_y is
                                  0334B5F3 0CA21756 BDE6D477
        38F2458F 56FBF6BD C76FCFB8 F3E59145 5F041A95 2EE87A8E


============================================================

Private Key Generation

N is
                                  01FFFFFF FFFFFFFF FFFFFFFF
        FFFFFFFF FFFFE9AE 2ED07577 265DFF7F 94451E06 1E163C61


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

C is
                                     E308 4442D66F A9A02C42
        890163E5 7EE33CA1 F4583C65 BCBDE927 81C7A3C8 3E89B772


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

K is
                                     E308 4442D66F A9A02C42
        890163E5 7EE33CA1 F4583C65 BCBDE927 81C7A3C8 3E89B773
```

```
============================================================

Signature Generation

msg is "Example of ECDSA with K-283"
Hash length = 256
D is
                                  00069E6D 19F7E454 A83664FF
        49208F60 38EAF842 E164DF42 D0F64948 FF9C94B0 14988329


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

R_x is
                                  07C973D5 8FD17A06 AA8F39D5
        EC42E0A6 B992F6CC 61F15756 5DD7036C 147D9005 400C1328


r(int) is 347140116251034137562323944383881095168284241287207993747866890549298446248326944307 7
E is
                                           184F9AEA 741E7668
        B8B5C72C 81617FA4 06892962 8F77BD2F 7A713A0A 09916B81


Kinv is
                                  0045D85F 04239846 DEB60444
        DA59F95C A0CA13FB 9C30B697 2E852E33 2E223067 143D174D


s(int) is 250655786031518189275263098458916896425696649087476506788284788624806507378659012409 7
------------------------------------------------------------

Signature:
  R is
                                  01C973D5 8FD17A06 AA8F39D5
        EC42E0A6 B99339C1 D57FF6F0 EABD04ED 57AE35F2 E5C95E05


  S is
                                  014A4ED0 2CBE4D76 ED5DDAA3
        4A9F2D73 90AF2DE3 27EDBC33 35119D3E 43CBB7FE 0384D841


============================================================

Signature Verification

msg is "Example of ECDSA with K-283"
Hash length = 256
Signature:
  R is
                                  01C973D5 8FD17A06 AA8F39D5
        EC42E0A6 B99339C1 D57FF6F0 EABD04ED 57AE35F2 E5C95E05


  S is
                                  014A4ED0 2CBE4D76 ED5DDAA3
        4A9F2D73 90AF2DE3 27EDBC33 35119D3E 43CBB7FE 0384D841


Public Key:
  Q_x is
                                  01B64A60 D4A36540 9635AAA2
        7E1708D9 0B839AFA 2D9820E1 2B79C3AF 1094B601 0AAEF5BE
```

```
  Q_y is
                                0334B5F3 0CA21756 BDE6D477
        38F2458F 56FBF6BD C76FCFB8 F3E59145 5F041A95 2EE87A8E


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

E is
                                         184F9AEA 741E7668
        B8B5C72C 81617FA4 06892962 8F77BD2F 7A713A0A 09916B81


U1 is
                                00195071 7A3BA3FE 8CC4677C
        5C6A1F9E C4C92A7D 405E39E1 33250ABC 8038A945 B86FBBB8


U2 is
                                00B8D9B4 2E8B8C1C 7B610132
        B88A9D3D DC8BEAE7 BD8A7E5F C94FC937 C46779BF 8E33CA2A


R_x is
                                07C973D5 8FD17A06 AA8F39D5
        EC42E0A6 B992F6CC 61F15756 5DD7036C 147D9005 400C1328


V is
                                01C973D5 8FD17A06 AA8F39D5
        EC42E0A6 B99339C1 D57FF6F0 EABD04ED 57AE35F2 E5C95E05


R' is
                                01C973D5 8FD17A06 AA8F39D5
        EC42E0A6 B99339C1 D57FF6F0 EABD04ED 57AE35F2 E5C95E05


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

Signature is verified


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

  Elliptic Curve Digital Signature Algorithm
    Curve = B-283
    Hash Length = 256

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

===============================================================

Private Key Generation

N is
                                03FFFFFF FFFFFFFF FFFFFFFF
        FFFFFFFF FFFFEF90 399660FC 938A9016 5B042A7C EFADB307


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

C is
                                010652D3 7B0A9DB6 4D4033AC
        6549CD1D F37E1EED E2612C23 63257C6A FF6C8CB5 DCB63647


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

D is
                                  010652D3 7B0A9DB6 4D4033AC
        6549CD1D F37E1EED E2612C23 63257C6A FF6C8CB5 DCB63648

Q_x is
                                  0390858E 9327A714 C74AF0C3
        ADEDF4E6 C75CAFDC C46507A4 9E415B13 8A094B6F 43E882AC

Q_y is
                                  00D4A65D 973CD150 A5221BED
        F872A4BA 207FF442 7DFFFD48 27C5BF16 9E719162 504D0631

==

Private Key Generation

N is
                                  03FFFFFF FFFFFFFF FFFFFFFF
        FFFFFFFF FFFFEF90 399660FC 938A9016 5B042A7C EFADB307

C is
                                  0100EC32 1393E6DD 6C4D47BE
        5AE189E5 E3540857 9D086217 8F94CCBB A3C4049A 4D88E296

K is
                                  0100EC32 1393E6DD 6C4D47BE
        5AE189E5 E3540857 9D086217 8F94CCBB A3C4049A 4D88E297

==

Signature Generation

msg is "Example of ECDSA with B-283"
Hash length = 256
D is
                                  010652D3 7B0A9DB6 4D4033AC
        6549CD1D F37E1EED E2612C23 63257C6A FF6C8CB5 DCB63648

R_x is
                                  077CB284 AC41E72E DA2A93EB
        8D6DFF58 620F6C69 D528DFE9 0D909AA5 CABC03A3 4E5D5A76

r(int) is 67742786977414206636875214464786924543620795990998866953565339605179366724434164222 55
E is
                                        F0BF4AEF 3F694EBD
        DE0A7944 5C897ADB 2430B918 77C772DA 9B7362CB 03AEA87F

Kinv is
                                  00AB6D18 AF222D8F DE7D9389
        4D4FAEEB 36ACCD4F B68EC95D 9E9BFF4C 08AFF3C6 31A67BE4

```
s(int) is 1240572480066211322672976019324920068198845924194402393411512731505068634362155794211
---------------------------------------------------------------

Signature:
  R is
                                  037CB284 AC41E72E DA2A93EB
        8D6DFF58 620F7CD9 9B927EEC 7A060A8F 6FB7D926 5EAFA76F


  S is
                                  00A37AC1 0AEBFC22 FC6E6EE2
        2E8F235E 3EEB0555 A0F0F9DA 92D9FFA7 34AD7679 56D27F23


===============================================================

Signature Verification

msg is "Example of ECDSA with B-283"
Hash length = 256
Signature:
  R is
                                  037CB284 AC41E72E DA2A93EB
        8D6DFF58 620F7CD9 9B927EEC 7A060A8F 6FB7D926 5EAFA76F


  S is
                                  00A37AC1 0AEBFC22 FC6E6EE2
        2E8F235E 3EEB0555 A0F0F9DA 92D9FFA7 34AD7679 56D27F23


Public Key:
  Q_x is
                                  0390858E 9327A714 C74AF0C3
        ADEDF4E6 C75CAFDC C46507A4 9E415B13 8A094B6F 43E882AC


  Q_y is
                                  00D4A65D 973CD150 A5221BED
        F872A4BA 207FF442 7DFFFD48 27C5BF16 9E719162 504D0631


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

E is
                                           F0BF4AEF 3F694EBD
        DE0A7944 5C897ADB 2430B918 77C772DA 9B7362CB 03AEA87F


U1 is
                                  01A9AF08 4B9E0457 4C178A2D
        00C97CFE 36F25D5F 834FCD70 44235A92 E89AC334 6C8C9AF3


U2 is
                                  00994904 2A40D761 3F3880CF
        CC3B3E9D 22EE9C13 0651CEE1 F263EFC8 81CF9A53 A564FBCE


R_x is
                                  077CB284 AC41E72E DA2A93EB
        8D6DFF58 620F6C69 D528DFE9 0D909AA5 CABC03A3 4E5D5A76


V is
                                  037CB284 AC41E72E DA2A93EB
```

```
        8D6DFF58 620F7CD9 9B927EEC 7A060A8F 6FB7D926 5EAFA76F


R' is
                                  037CB284 AC41E72E DA2A93EB
        8D6DFF58 620F7CD9 9B927EEC 7A060A8F 6FB7D926 5EAFA76F


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

Signature is verified


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

  Elliptic Curve Digital Signature Algorithm
    Curve = K-409
    Hash Length = 384

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

============================================================

Private Key Generation

N is
                                                    007FFFFF
        FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFE5F
        83B2D4EA 20400EC4 557D5ED3 E3E7CA5B 4B5C83B8 E01E5FCF


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

C is
                                                    00019F57
        89FE26E0 E700C69E 253E9F74 D76EAFB4 C979D0B1 584D4FE9
        8715D45B 7BAAA851 E02A1ECA ED8B9660 2CF611D8 A504BBD4


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

D is
                                                    00019F57
        89FE26E0 E700C69E 253E9F74 D76EAFB4 C979D0B1 584D4FE9
        8715D45B 7BAAA851 E02A1ECA ED8B9660 2CF611D8 A504BBD5


Q_x is
                                                    01270655
        90DF9265 FDFBA4ED 6EDF76A9 BC8CE880 B58B6F57 1A1AB62B
        A3401269 441F3B95 ECD09094 65022240 AE45C7B3 6A91DE58


Q_y is
                                                    003C8526
        8D926730 2090425B BC14C3D9 AE1C1CFC 78E0BFCC CFC1FB5D
        CA5B195C 6F8CFBE2 D85E4071 B71317AA 2B0B65C3 91F82502


============================================================

Private Key Generation

N is
                                                    007FFFFF
        FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFE5F
        83B2D4EA 20400EC4 557D5ED3 E3E7CA5B 4B5C83B8 E01E5FCF
```

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

C is
                                                    00015920
        48516CCD 793C7B86 3B00985F DBA71C3D 1EDF449F 667AC0D0
        5EF37D15 A94AD328 2F29F7E9 FD949187 2F931354 A1CCFA38


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

K is
                                                    00015920
        48516CCD 793C7B86 3B00985F DBA71C3D 1EDF449F 667AC0D0
        5EF37D15 A94AD328 2F29F7E9 FD949187 2F931354 A1CCFA39


===============================================================

Signature Generation

msg is "Example of ECDSA with K-409"
Hash length = 384
D is
                                                    00019F57
        89FE26E0 E700C69E 253E9F74 D76EAFB4 C979D0B1 584D4FE9
        8715D45B 7BAAA851 E02A1ECA ED8B9660 2CF611D8 A504BBD5


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

R_x is
                                                    00EF421A
        230AA8B4 71939A77 BF4F2C64 FC0B4CAA 39EDCD06 337A9115
        AF89DF72 5E3C748A E018320E 89D77ABC D3AA13A6 CCF10C34


r(int) is
287296502609903755047276062317671877380342987214246771450934811188142631858192434973293671444180485746280616241
641144101989
E is
        B18623FE 7D6B79C3 947651CF 64A06640 0F89DC98 9D07BFD8
        C1AAF75E 3C9B3D48 FC457204 168DE4ED 4ECA8E24 0E009B95


Kinv is
                                                    0064D066
        B74C9771 A843F341 A1853F05 20696AA5 7338C21C 4A839507
        B5EE65CB 98A7F87C 8E53037C 02980CF5 185300B7 09901D59


s(int) is
171388639085828986597824337788600168526139265051294280998358619335390078299394527527443716590351871100863295063
908700846115
---------------------------------------------------------------

Signature:
  R is
                                                    006F421A
        230AA8B4 71939A77 BF4F2C64 FC0B4CAA 39EDCD06 337A92B6
        2BD70A88 3DFC65C6 8A9AD33A A5EFB061 884D8FED ECD2AC65


  S is
                                                    00425F2F
        F9CBBF1B 9E3FC17C 4B663036 22D77490 47373CC9 F919758C
```

```
        D88420C4 CD0FDF14 B819A4AD A9961C3E 60950004 67C2F823


============================================================

Signature Verification

msg is "Example of ECDSA with K-409"
Hash length = 384
Signature:
  R is
                                                  006F421A
        230AA8B4 71939A77 BF4F2C64 FC0B4CAA 39EDCD06 337A92B6
        2BD70A88 3DFC65C6 8A9AD33A A5EFB061 884D8FED ECD2AC65


  S is
                                                  00425F2F
        F9CBBF1B 9E3FC17C 4B663036 22D77490 47373CC9 F919758C
        D88420C4 CD0FDF14 B819A4AD A9961C3E 60950004 67C2F823


Public Key:
  Q_x is
                                                  01270655
        90DF9265 FDFBA4ED 6EDF76A9 BC8CE880 B58B6F57 1A1AB62B
        A3401269 441F3B95 ECD09094 65022240 AE45C7B3 6A91DE58


  Q_y is
                                                  003C8526
        8D926730 2090425B BC14C3D9 AE1C1CFC 78E0BFCC CFC1FB5D
        CA5B195C 6F8CFBE2 D85E4071 B71317AA 2B0B65C3 91F82502


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

E is
        B18623FE 7D6B79C3 947651CF 64A06640 0F89DC98 9D07BFD8
        C1AAF75E 3C9B3D48 FC457204 168DE4ED 4ECA8E24 0E009B95


U1 is
                                                  007FC6BD
        B66A9D2A 23BF69D4 F96BB3E7 E24E365B 45D111C6 66747A42
        B39275ED 0BA4F286 6D3723DD 13851A45 208C8645 25D5F530


U2 is
                                                  0005E16D
        63457088 B1F3012E 844C852E 23C9F122 5AA569A8 83DE8A58
        28DDE309 17D23C4D 807A371A A1FC5DB2 5149ABBC D53F7558


R_x is
                                                  00EF421A
        230AA8B4 71939A77 BF4F2C64 FC0B4CAA 39EDCD06 337A9115
        AF89DF72 5E3C748A E018320E 89D77ABC D3AA13A6 CCF10C34


V is
                                                  006F421A
        230AA8B4 71939A77 BF4F2C64 FC0B4CAA 39EDCD06 337A92B6
        2BD70A88 3DFC65C6 8A9AD33A A5EFB061 884D8FED ECD2AC65


R' is
```

                                                    006F421A
        230AA8B4 71939A77 BF4F2C64 FC0B4CAA 39EDCD06 337A92B6
        2BD70A88 3DFC65C6 8A9AD33A A5EFB061 884D8FED ECD2AC65

Signature is verified

##

  Elliptic Curve Digital Signature Algorithm
    Curve = B-409
    Hash Length = 384

##

==

Private Key Generation

N is
                                                    01000000
        00000000 00000000 00000000 00000000 00000000 000001E2
        AAD6A612 F33307BE 5FA47C3C 9E052F83 8164CD37 D9A21173

C is
                                                      4AF8
        96DB379A BDF70C8F ADE9EBD2 8CD530F2 ECB336B4 DE84BD6E
        065EF56C 8C548C53 2D00FA55 CA8ACF3E 98ADBCA9 F78D241A

D is
                                                      4AF8
        96DB379A BDF70C8F ADE9EBD2 8CD530F2 ECB336B4 DE84BD6E
        065EF56C 8C548C53 2D00FA55 CA8ACF3E 98ADBCA9 F78D241B

Q_x is
                                                    01951C5E
        41607E93 17F247D4 9A389D0E 120F479D 47737543 098AE5E1
        BB62BD59 DE70E1C5 84AE655C 702D39DD 4F7883E1 876C4A9B

Q_y is
                                                    016B16B9
        8A3353D7 5BEB4D35 76C64568 BA381463 CF77D4AE B85218D2
        D546E7A1 EE3AB931 6D8C7DF0 0D155B78 91B2C0BF 4B5E942E

==

Private Key Generation

N is
                                                    01000000
        00000000 00000000 00000000 00000000 00000000 000001E2
        AAD6A612 F33307BE 5FA47C3C 9E052F83 8164CD37 D9A21173

```
C is
                                                          6A0B
        81D9320B 5C305D73 0B1C1E74 B03FAFB8 8A7EC355 990B75F9
        B70E8532 433296A3 2492CBA0 6F8583D5 B19C5B8C 5D6D07EB


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

K is
                                                          6A0B
        81D9320B 5C305D73 0B1C1E74 B03FAFB8 8A7EC355 990B75F9
        B70E8532 433296A3 2492CBA0 6F8583D5 B19C5B8C 5D6D07EC


=============================================================

Signature Generation

msg is "Example of ECDSA with B-409"
Hash length = 384
D is
                                                          4AF8
        96DB379A BDF70C8F ADE9EBD2 8CD530F2 ECB336B4 DE84BD6E
        065EF56C 8C548C53 2D00FA55 CA8ACF3E 98ADBCA9 F78D241B


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

R_x is
                                                    01F3E4DA
        3101C642 39D76831 995C0EC1 E56CE469 0C42DDD5 3DBF3EF7
        25D819DF 090B8632 F327499B 5B99C280 D7F410CD 7105C8DB


r(int) is
629795133852997848663164416330632008108488131029367711198400899015295569161990628452056613359116571349413663774
547185481576
E is
        4BBF1BC0 DDF9D3B7 BFE21FC6 8642B3E5 508CA6BA 4D365C1D
        00ABBFAB DB0F3EC2 B0BE995A E803DE47 D0880BF1 92649EDC


Kinv is
                                                    00A202EA
        455D0E1A 5EF09054 B39259C7 68DB76FF D1A77B62 81FC7056
        A4A23A10 12CDD604 E4D7993E 0D9EDD42 2DEFD782 C1225A1A


s(int) is
106353011790980050510402230388010919168837770971007460637281001297135413850335587267331709367101624723953375840
680931987115
-------------------------------------------------------------

Signature:
  R is
                                                    00F3E4DA
        3101C642 39D76831 995C0EC1 E56CE469 0C42DDD5 3DBF3D14
        7B0173CC 15D87E74 9382CD5E BD9492FD 568F4395 9763B768


  S is
                                                    00292FA9
        94DC6EA3 67236AD7 3956DBC1 EB62B877 9DF43816 54071415
        87E3FEED 883741CD F5542F25 5BEBC57B 9D0C87AD 403B8EAB


=============================================================
```

```
Signature Verification

msg is "Example of ECDSA with B-409"
Hash length = 384
Signature:
  R is
                                                    00F3E4DA
        3101C642 39D76831 995C0EC1 E56CE469 0C42DDD5 3DBF3D14
        7B0173CC 15D87E74 9382CD5E BD9492FD 568F4395 9763B768


  S is
                                                    00292FA9
        94DC6EA3 67236AD7 3956DBC1 EB62B877 9DF43816 54071415
        87E3FEED 883741CD F5542F25 5BEBC57B 9D0C87AD 403B8EAB


Public Key:
  Q_x is
                                                    01951C5E
        41607E93 17F247D4 9A389D0E 120F479D 47737543 098AE5E1
        BB62BD59 DE70E1C5 84AE655C 702D39DD 4F7883E1 876C4A9B


  Q_y is
                                                    016B16B9
        8A3353D7 5BEB4D35 76C64568 BA381463 CF77D4AE B85218D2
        D546E7A1 EE3AB931 6D8C7DF0 0D155B78 91B2C0BF 4B5E942E


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

E is
        4BBF1BC0 DDF9D3B7 BFE21FC6 8642B3E5 508CA6BA 4D365C1D
        00ABBFAB DB0F3EC2 B0BE995A E803DE47 D0880BF1 92649EDC


U1 is
                                                    0033D4F3
        CE2B7D4F 2548F54C 92420A8C 30E6B02D 768CBD6C A4AB020E
        88BE82EE FE4D58A9 B4DB2854 561EAD89 75E1A58F B45C2117


U2 is
                                                    00EB0671
        192B38CB C911CADE 604D9E04 8C7E660A F3C7085D 54839C1B
        7549691E 5F7FFFDA B4003ADE 05208775 D4A0287E 448740AF


R_x is
                                                    01F3E4DA
        3101C642 39D76831 995C0EC1 E56CE469 0C42DDD5 3DBF3EF7
        25D819DF 090B8632 F327499B 5B99C280 D7F410CD 7105C8DB


V is
                                                    00F3E4DA
        3101C642 39D76831 995C0EC1 E56CE469 0C42DDD5 3DBF3D14
        7B0173CC 15D87E74 9382CD5E BD9492FD 568F4395 9763B768


R' is
                                                    00F3E4DA
        3101C642 39D76831 995C0EC1 E56CE469 0C42DDD5 3DBF3D14
        7B0173CC 15D87E74 9382CD5E BD9492FD 568F4395 9763B768
```

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

Signature is verified


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

  Elliptic Curve Digital Signature Algorithm
    Curve = K-571
    Hash Length = 512

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

=============================================================

Private Key Generation

N is
        02000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 131850E1 F19A63E4 B391A8DB
        917F4138 B630D84B E5D63938 1E91DEB4 5CFE778F 637C1001


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

C is
        01042FDE 4D66E767 25E7957E 208A85CF 23BC0D5B 8D001B36
        AEAFB34A D1104004 CCF99AFD FABCA115 85A4EB52 63C87052
        CB05EF7F B39D9E5F 6CF495E9 DCE5840B 83FBC5FF 3AD8B2F2


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

D is
        01042FDE 4D66E767 25E7957E 208A85CF 23BC0D5B 8D001B36
        AEAFB34A D1104004 CCF99AFD FABCA115 85A4EB52 63C87052
        CB05EF7F B39D9E5F 6CF495E9 DCE5840B 83FBC5FF 3AD8B2F3


Q_x is
        04D9CFE0 A7338FEA 703E007F 5D10BABD 2DF3F319 B47DF1E2
        3C4F7E5A BF5014C1 390B78F1 17E6AF82 58A48F56 ACB9FAAC
        788530B5 CCDB1AB7 E9390EC5 DD7A39D5 EEAF6C41 BF50AC76


Q_y is
        064732C5 04F81DC5 F9B0E882 B6DA46E1 24E82413 58F07789
        6D25ECF0 28AD0E60 11993C85 E68741A0 7D7817C4 00CF94B1
        A3F524F4 8668B5B9 70972618 616DB436 2A769D16 CAC34BF0


=============================================================

Private Key Generation

N is
        02000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 131850E1 F19A63E4 B391A8DB
        917F4138 B630D84B E5D63938 1E91DEB4 5CFE778F 637C1001


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

C is
        0104063C 918DE620 00A3FD87 775D8D71 398722BD 153B8EA3
        3060349C 5FE6CF6C B4677957 E6BA50D3 C8A8B518 2B9CF962
```

```
        954A6BBB 5F7868B8 8E5778AA 62A0CF80 02BF19DA 3049FF50


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

K is
        0104063C 918DE620 00A3FD87 775D8D71 398722BD 153B8EA3
        3060349C 5FE6CF6C B4677957 E6BA50D3 C8A8B518 2B9CF962
        954A6BBB 5F7868B8 8E5778AA 62A0CF80 02BF19DA 3049FF51


===============================================================

Signature Generation

msg is "Example of ECDSA with K-571"
Hash length = 512
D is
        01042FDE 4D66E767 25E7957E 208A85CF 23BC0D5B 8D001B36
        AEAFB34A D1104004 CCF99AFD FABCA115 85A4EB52 63C87052
        CB05EF7F B39D9E5F 6CF495E9 DCE5840B 83FBC5FF 3AD8B2F3


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

R_x is
        0668758C 313FBF19 45F775D9 5B25866D BC8D001D 9C7EF4FF
        A53774E8 C68927A5 2707F034 CEBB3A71 2BE6D164 F2FFE189
        7B069F8F BAEC4650 B5372DDF A31CDECC FA785691 97CF50F1


r(int) is
3942249840777817941104967970902430132643106976942351331529293576152105911173110397896355536260608432131563292950907945266948460238476768669002612397025471525972220991981900
E is
                        46E30ABD D459269C F19AF769 00AF7131
        B4F63922 7414719E BEBE548C CD4026B7 5C1F5261 8547AA38
        21F29FCF 685E3364 0BD9E29F 7FE46817 627D4139 EEE411C6


Kinv is
        0075A02B EAEA5166 0A1D0505 3B173C9C 6DCCAEBA 80F72CA0
        8DEC3C32 E2A47CBC 5674998A D19FC77B 6615BFBE D482451A
        F7FD9B41 6B64B0E8 F8429449 FA9685F2 B9C8DC21 08544D98


s(int) is
9275826462470345361774197411576427373206616335911802279144015736222078185856359572652371895283193202640215239610002206044584984307125779998921944554154918225019945555510 41
---------------------------------------------------------------

Signature:
  R is
        0068758C 313FBF19 45F775D9 5B25866D BC8D001D 9C7EF4FF
        A53774E8 C68927A5 2707F034 957247CB 5717A5B6 D84AE6F6
        C688DBE5 9859BD6D 03B48237 476742AF E37CEFE3 6D5B20EE


  S is
        00F5C8E9 75A1DA26 B2E0ACD4 F486C4A4 231C1E29 EE8ECFA0
        3A697761 498F5D53 FF898AFC 16945975 D328D34A 8DCDC6D0
        613C73FE 4F516F56 85E23716 FE105ED3 472C3358 B5B4AD41


===============================================================

Signature Verification
```

```
msg is "Example of ECDSA with K-571"
Hash length = 512
Signature:
  R is
        0068758C 313FBF19 45F775D9 5B25866D BC8D001D 9C7EF4FF
        A53774E8 C68927A5 2707F034 957247CB 5717A5B6 D84AE6F6
        C688DBE5 9859BD6D 03B48237 476742AF E37CEFE3 6D5B20EE


  S is
        00F5C8E9 75A1DA26 B2E0ACD4 F486C4A4 231C1E29 EE8ECFA0
        3A697761 498F5D53 FF898AFC 16945975 D328D34A 8DCDC6D0
        613C73FE 4F516F56 85E23716 FE105ED3 472C3358 B5B4AD41


Public Key:
  Q_x is
        04D9CFE0 A7338FEA 703E007F 5D10BABD 2DF3F319 B47DF1E2
        3C4F7E5A BF5014C1 390B78F1 17E6AF82 58A48F56 ACB9FAAC
        788530B5 CCDB1AB7 E9390EC5 DD7A39D5 EEAF6C41 BF50AC76


  Q_y is
        064732C5 04F81DC5 F9B0E882 B6DA46E1 24E82413 58F07789
        6D25ECF0 28AD0E60 11993C85 E68741A0 7D7817C4 00CF94B1
        A3F524F4 8668B5B9 70972618 616DB436 2A769D16 CAC34BF0


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

E is
                        46E30ABD D459269C F19AF769 00AF7131
        B4F63922 7414719E BEBE548C CD4026B7 5C1F5261 8547AA38
        21F29FCF 685E3364 0BD9E29F 7FE46817 627D4139 EEE411C6


U1 is
        0121B1F8 919C4ED4 1D4676BC 6F417DBF 7F93C231 4C747966
        42D1B17D F4FD04C1 14AE2937 07913E2E BB65E173 D52C3678
        C8366EB3 C94E7B7E CEE53F6B 0B625AC6 2B924E3D 6B975FF3


U2 is
        01AFBF8D 1D315114 13EB6846 B32CED90 D38E515F F26CB833
        4EF61967 7794CC3B 92DA014E 9B0E39BF 49D8933D 3E998145
        59412861 2AECCBFC 7004D087 77FD90BC 197D13DC 6238BF0B


R_x is
        0068758C 313FBF19 45F775D9 5B25866D BC8D001D 9C7EF4FF
        A53774E8 C68927A5 2707F034 CEBB3A71 2BE6D164 F2FFE189
        7B069F8F BAEC4650 B5372DDF A31CDECC FA785691 97CF50F1


V is
        0068758C 313FBF19 45F775D9 5B25866D BC8D001D 9C7EF4FF
        A53774E8 C68927A5 2707F034 957247CB 5717A5B6 D84AE6F6
        C688DBE5 9859BD6D 03B48237 476742AF E37CEFE3 6D5B20EE


R' is
        0068758C 313FBF19 45F775D9 5B25866D BC8D001D 9C7EF4FF
        A53774E8 C68927A5 2707F034 957247CB 5717A5B6 D84AE6F6
        C688DBE5 9859BD6D 03B48237 476742AF E37CEFE3 6D5B20EE
```

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

Signature is verified


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

  Elliptic Curve Digital Signature Algorithm
    Curve = B-571
    Hash Length = 512

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

============================================================

Private Key Generation

N is
        03FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
        FFFFFFFF FFFFFFFF FFFFFFFF E661CE18 FF559873 08059B18
        6823851E C7DD9CA1 161DE93D 5174D66E 8382E9BB 2FE84E47


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

C is
        0003CCE3 2BA00DC3 A7EEFC9E B6F6CBFB 9C5F0E57 F532B7EE
        6826D4A7 5D0E756F D533900F 2CEA8CCC C50EE22C E079398D
        371EC4A2 EC45CC24 B8876066 78E9C674 53D0F5E7 68E9D751


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

D is
        0003CCE3 2BA00DC3 A7EEFC9E B6F6CBFB 9C5F0E57 F532B7EE
        6826D4A7 5D0E756F D533900F 2CEA8CCC C50EE22C E079398D
        371EC4A2 EC45CC24 B8876066 78E9C674 53D0F5E7 68E9D752


Q_x is
        00310EAD 2BEF3DDB 84F9FC17 77A7EE17 9FFCB77A AB497BDC
        00E29059 7A5FCE30 6FE419D2 F1F208E5 48505165 26DB8E03
        B0519BEF 60E3A3CC 8198FBCA 8C469ACF E46AB70D 5C31874F


Q_y is
        0373CE6E A68F55D1 501D5203 ACA03C5A B709A337 A8E03B03
        838F47C0 6762065F BDD08A10 2A08C42F F1760145 BE54D860
        6D326EA2 2A54DF03 4FAC3098 8049820B EBA2B0AF 9F6404B3


============================================================

Private Key Generation

N is
        03FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
        FFFFFFFF FFFFFFFF FFFFFFFF E661CE18 FF559873 08059B18
        6823851E C7DD9CA1 161DE93D 5174D66E 8382E9BB 2FE84E47


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

C is
        01062FF6 D95C49AC 610CB9AF 9900D59C 288669C3 626306DB
        7EB7F119 499BA1D5 4CB6BE88 8758CAAD A6995267 5CC0CD49
        99176879 BC302A7E 2A5118DF C7D538DA 114CCAC2 BAF9AD07
```

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

K is
        01062FF6 D95C49AC 610CB9AF 9900D59C 288669C3 626306DB
        7EB7F119 499BA1D5 4CB6BE88 8758CAAD A6995267 5CC0CD49
        99176879 BC302A7E 2A5118DF C7D538DA 114CCAC2 BAF9AD08


=============================================================

Signature Generation

msg is "Example of ECDSA with B-571"
Hash length = 512
D is
        0003CCE3 2BA00DC3 A7EEFC9E B6F6CBFB 9C5F0E57 F532B7EE
        6826D4A7 5D0E756F D533900F 2CEA8CCC C50EE22C E079398D
        371EC4A2 EC45CC24 B8876066 78E9C674 53D0F5E7 68E9D752


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

R_x is
        00E17447 E422A2C0 08519035 4AC14921 0C1137A9 2C10F9B1
        4D225E65 10DA76B1 9EF44D39 390DD9D8 08C9DFBA E67D9CF0
        E7BE79A9 E72FA8FA 1DFE89F4 3FB6D093 A6CEB30E 136EABA3


r(int) is
850855762239502026591058023510563289273348857487181767834743944602362175979470988825265490247148142789747022832
891719663177918797433599028444576028042439884754109942639523
E is
                        60EDEF7D A1D9D35A 77D1DA44 1EBB6345
        4501F2BB 1AF8A4C4 9D281298 E5F4D4E6 B7E9BCE4 B66B2512
        BF590288 B57915BF D3AED2C2 604A5C57 4107DF67 4FAF9779


Kinv is
        028C3AE1 2BD7922B 837FE050 66136BB4 5EDA0337 D39E31C3
        D4B9164C 93F17FD7 549471EB 0385FCCE A8768DD6 E5925ADF
        1D188882 6FF6AECC 48F3DB39 905D46A6 44EB2F0C 3A3DCBBD


s(int) is
371005865765721334746413249075321341103084481747665324048935832930246035334494733931256416306196179464892337407
155249561524652370280994639556574699020735912775043796334024
-------------------------------------------------------------

Signature:
  R is
        00E17447 E422A2C0 08519035 4AC14921 0C1137A9 2C10F9B1
        4D225E65 10DA76B1 9EF44D39 390DD9D8 08C9DFBA E67D9CF0
        E7BE79A9 E72FA8FA 1DFE89F4 3FB6D093 A6CEB30E 136EABA3


  S is
        00624E85 2C7B6A06 1B4B39A9 07B51820 0FED380F D692C9AE
        147C5250 F4852434 AFA24A1C A5062C48 E5FC217F B689AB3A
        7266B552 2F176F32 A5CEA22D 6BF2820D 349E4193 BCEE75C8


=============================================================

Signature Verification
```

```
msg is "Example of ECDSA with B-571"
Hash length = 512
Signature:
  R is
        00E17447 E422A2C0 08519035 4AC14921 0C1137A9 2C10F9B1
        4D225E65 10DA76B1 9EF44D39 390DD9D8 08C9DFBA E67D9CF0
        E7BE79A9 E72FA8FA 1DFE89F4 3FB6D093 A6CEB30E 136EABA3


  S is
        00624E85 2C7B6A06 1B4B39A9 07B51820 0FED380F D692C9AE
        147C5250 F4852434 AFA24A1C A5062C48 E5FC217F B689AB3A
        7266B552 2F176F32 A5CEA22D 6BF2820D 349E4193 BCEE75C8


Public Key:
  Q_x is
        00310EAD 2BEF3DDB 84F9FC17 77A7EE17 9FFCB77A AB497BDC
        00E29059 7A5FCE30 6FE419D2 F1F208E5 48505165 26DB8E03
        B0519BEF 60E3A3CC 8198FBCA 8C469ACF E46AB70D 5C31874F


  Q_y is
        0373CE6E A68F55D1 501D5203 ACA03C5A B709A337 A8E03B03
        838F47C0 6762065F BDD08A10 2A08C42F F1760145 BE54D860
        6D326EA2 2A54DF03 4FAC3098 8049820B EBA2B0AF 9F6404B3


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

E is
                          60EDEF7D A1D9D35A 77D1DA44 1EBB6345
        4501F2BB 1AF8A4C4 9D281298 E5F4D4E6 B7E9BCE4 B66B2512
        BF590288 B57915BF D3AED2C2 604A5C57 4107DF67 4FAF9779


U1 is
        01A73BE1 676983C3 B1583A85 04C46E29 0AC2FFC3 FD7866E6
        242AE2A3 DC40F362 E2B79917 3698175F 7F094E9F A06EE09B
        3AA7D284 549B8FCF 4671051B 829AA38E F59D066B 3554DE19


U2 is
        010DF449 E4FB5760 79A7D63A 59F000DA 5E24DA78 00FA29BF
        321084ED 549834B1 ED95E5BA F48FD658 30F2BD09 57B6F709
        DAC14AF9 0BE29993 FE428BD7 DF93206C C9ED9296 230B8657


R_x is
        00E17447 E422A2C0 08519035 4AC14921 0C1137A9 2C10F9B1
        4D225E65 10DA76B1 9EF44D39 390DD9D8 08C9DFBA E67D9CF0
        E7BE79A9 E72FA8FA 1DFE89F4 3FB6D093 A6CEB30E 136EABA3


V is
        00E17447 E422A2C0 08519035 4AC14921 0C1137A9 2C10F9B1
        4D225E65 10DA76B1 9EF44D39 390DD9D8 08C9DFBA E67D9CF0
        E7BE79A9 E72FA8FA 1DFE89F4 3FB6D093 A6CEB30E 136EABA3


R' is
        00E17447 E422A2C0 08519035 4AC14921 0C1137A9 2C10F9B1
        4D225E65 10DA76B1 9EF44D39 390DD9D8 08C9DFBA E67D9CF0
        E7BE79A9 E72FA8FA 1DFE89F4 3FB6D093 A6CEB30E 136EABA3


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

Signature is verified