

Samples to illustrate the proper truncation of SHAKE outputs for output lengths that are not multiples of 8-bits.

All samples below use SHAKE128 with a 0-bit input message (the “empty” or “null” message).

Note – Only the final byte changes to accommodate the convention established in FIPS 202 for the hex representation of the final bits of a truncated bit string.

Output length = 4096

Output val is

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 76 7B E1 FD A6 94 19 DF
B9 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C C0 D4 C9
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 69 2D 86 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 5B 70 B8 3F
28 01 F2 F4 B3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED C0 96
31 B1 09 58 F4 64 D8 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
```

```
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B 6F
```

Output length = 4095

Output val is

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 76 7B E1 FD A6 94 19 DF
B9 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C C0 D4 C9
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 69 2D 86 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 5B 70 B8 3F
28 01 F2 F4 B3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED C0 96
31 B1 09 58 F4 64 D8 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
```

```
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B 6F
```

Output length = 4094

Output val is

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 76 7B E1 FD A6 94 19 DF
B9 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C C0 D4 C9
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 69 2D 86 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 5B 70 B8 3F
28 01 F2 F4 B3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED C0 96
31 B1 09 58 F4 64 D8 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
```

43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B 2F

Output length = 4093

Output val is

7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 76 7B E1 FD A6 94 19 DF
B9 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C C0 D4 C9
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 69 2D 86 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 5B 70 B8 3F
28 01 F2 F4 B3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED C0 96
31 B1 09 58 F4 64 D8 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B 0F

Output length = 4092

Output val is

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 76 7B E1 FD A6 94 19 DF
B9 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C C0 D4 C9
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 69 2D 86 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 5B 70 B8 3F
28 01 F2 F4 B3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED C0 96
31 B1 09 58 F4 64 D8 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B 0F
```

Output length = 4091

Output val is

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 76 7B E1 FD A6 94 19 DF
B9 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C C0 D4 C9
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 69 2D 86 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 5B 70 B8 3F
28 01 F2 F4 B3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED C0 96
31 B1 09 58 F4 64 D8 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B 07
```

Output length = 4090

Output val is

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
```

```
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 76 7B E1 FD A6 94 19 DF
B9 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C C0 D4 C9
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 69 2D 86 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 5B 70 B8 3F
28 01 F2 F4 B3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED C0 96
31 B1 09 58 F4 64 D8 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B 03
```

Output length = 4089

Output val is

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
```

```
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 76 7B E1 FD A6 94 19 DF
B9 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C C0 D4 C9
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 69 2D 86 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 5B 70 B8 3F
28 01 F2 F4 B3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED C0 96
31 B1 09 58 F4 64 D8 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B 01
```

Output length = 4088

Output val is

```
7F 9C 2B A4 E8 8F 82 7D 61 60 45 50 76 05 85 3E
D7 3B 80 93 F6 EF BC 88 EB 1A 6E AC FA 66 EF 26
3C B1 EE A9 88 00 4B 93 10 3C FB 0A EE FD 2A 68
6E 01 FA 4A 58 E8 A3 63 9C A8 A1 E3 F9 AE 57 E2
35 B8 CC 87 3C 23 DC 62 B8 D2 60 16 9A FA 2F 75
AB 91 6A 58 D9 74 91 88 35 D2 5E 6A 43 50 85 B2
BA DF D6 DF AA C3 59 A5 EF BB 7B CC 4B 59 D5 38
DF 9A 04 30 2E 10 C8 BC 1C BF 1A 0B 3A 51 20 EA
```


17 CD A7 CF AD 76 5F 56 23 47 4D 36 8C CC A8 AF
00 07 CD 9F 5E 4C 84 9F 16 7A 58 0B 14 AA BD EF
AE E7 EE F4 7C B0 FC A9 76 7B E1 FD A6 94 19 DF
B9 27 E9 DF 07 34 8B 19 66 91 AB AE B5 80 B3 2D
EF 58 53 8B 8D 23 F8 77 32 EA 63 B0 2B 4F A0 F4
87 33 60 E2 84 19 28 CD 60 DD 4C EE 8C C0 D4 C9
22 A9 61 88 D0 32 67 5C 8A C8 50 93 3C 7A FF 15
33 B9 4C 83 4A DB B6 9C 61 15 BA D4 69 2D 86 19
F9 0B 0C DF 8A 7B 9C 26 40 29 AC 18 5B 70 B8 3F
28 01 F2 F4 B3 F7 0C 59 3E A3 AE EB 61 3A 7F 1B
1D E3 3F D7 50 81 F5 92 30 5F 2E 45 26 ED C0 96
31 B1 09 58 F4 64 D8 89 F3 1B A0 10 25 0F DA 7F
13 68 EC 29 67 FC 84 EF 2A E9 AF F2 68 E0 B1 70
0A FF C6 82 0B 52 3A 3D 91 71 35 F2 DF F2 EE 06
BF E7 2B 31 24 72 1D 4A 26 C0 4E 53 A7 5E 30 E7
3A 7A 9C 4A 95 D9 1C 55 D4 95 E9 F5 1D D0 B5 E9
D8 3C 6D 5E 8C E8 03 AA 62 B8 D6 54 DB 53 D0 9B
8D CF F2 73 CD FE B5 73 FA D8 BC D4 55 78 BE C2
E7 70 D0 1E FD E8 6E 72 1A 3F 7C 6C CE 27 5D AB
E6 E2 14 3F 1A F1 8D A7 EF DD C4 C7 B7 0B 5E 34
5D B9 3C C9 36 BE A3 23 49 1C CB 38 A3 88 F5 46
A9 FF 00 DD 4E 13 00 B9 B2 15 3D 20 41 D2 05 B4
43 E4 1B 45 A6 53 F2 A5 C4 49 2C 1A DD 54 45 12
DD A2 52 98 33 46 2B 71 A4 1A 45 BE 97 29 0B