##
SHA-3 Derived Functions
cSHAKE
KMAC
TupleHash
ParallelHash
##

cSHAKE:
Sample #1

Security Strength: 128-bits

Length of data is 32-bits
Data is
00 01 02 03

Requested output length is 256-bits

N is
(empty string)

S (as a character string) is
"Email Signature"

Encoded N
01 00
Encoded S
01 78 45 6D 61 69 6C 20 53 69 67 6E 61 74 75 72
65
bytepad data
01 A8 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

About to Absorb data
State (in bytes)
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Data to be absorbed

01 A8 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Xor'd state (in bytes)

01 A8 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

After Permutation

19 4C CD 05 8B 2A 83 D6 02 29 DC 69 84 D1 4F 15
8B 69 4F A4 BD 39 B2 1F 84 FB 06 C8 CB C6 7B 84
2D EF 9E 2B DB F0 F8 E1 BD 14 EA CC DC 58 26 84
62 4B 41 B6 4A 08 51 06 81 79 FD FB CA DB 73 1E
17 59 36 47 ED 96 C6 E3 5C DA 77 06 97 54 F5 F8
25 66 42 92 C6 79 78 FC B7 BD 58 31 ED 10 76 A6
FD 14 F3 4F FF AB 28 72 96 60 AB 82 DF 4A FD FF
81 EF 67 1C 91 81 E5 C6 EB 82 27 F6 A0 72 C8 E2
91 78 28 2E E5 A9 E6 83 92 5E 97 C5 F1 5F 71 68
23 B8 E1 05 6C 7D C8 46 14 94 7E 4A 31 EC E0 0D
8B 1E DA B4 78 74 0E 82 41 78 E7 C2 80 65 C0 C5
CC 84 74 9C AD 7F C3 C6 0D E7 27 61 8B 56 FE 3A
F0 03 FD D5 AB 02 54 28

about to call last of the absorb phase

About to Absorb data
State (in bytes)

```
19 4C CD 05 8B 2A 83 D6 02 29 DC 69 84 D1 4F 15
8B 69 4F A4 BD 39 B2 1F 84 FB 06 C8 CB C6 7B 84
2D EF 9E 2B DB F0 F8 E1 BD 14 EA CC DC 58 26 84
62 4B 41 B6 4A 08 51 06 81 79 FD FB CA DB 73 1E
17 59 36 47 ED 96 C6 E3 5C DA 77 06 97 54 F5 F8
25 66 42 92 C6 79 78 FC B7 BD 58 31 ED 10 76 A6
FD 14 F3 4F FF AB 28 72 96 60 AB 82 DF 4A FD FF
81 EF 67 1C 91 81 E5 C6 EB 82 27 F6 A0 72 C8 E2
91 78 28 2E E5 A9 E6 83 92 5E 97 C5 F1 5F 71 68
23 B8 E1 05 6C 7D C8 46 14 94 7E 4A 31 EC E0 0D
8B 1E DA B4 78 74 0E 82 41 78 E7 C2 80 65 C0 C5
CC 84 74 9C AD 7F C3 C6 0D E7 27 61 8B 56 FE 3A
F0 03 FD D5 AB 02 54 28
```

Data to be absorbed

```
00 01 02 03 04 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

Xor'd state (in bytes)

```
19 4D CF 06 8F 2A 83 D6 02 29 DC 69 84 D1 4F 15
8B 69 4F A4 BD 39 B2 1F 84 FB 06 C8 CB C6 7B 84
2D EF 9E 2B DB F0 F8 E1 BD 14 EA CC DC 58 26 84
62 4B 41 B6 4A 08 51 06 81 79 FD FB CA DB 73 1E
17 59 36 47 ED 96 C6 E3 5C DA 77 06 97 54 F5 F8
25 66 42 92 C6 79 78 FC B7 BD 58 31 ED 10 76 A6
FD 14 F3 4F FF AB 28 72 96 60 AB 82 DF 4A FD FF
81 EF 67 1C 91 81 E5 C6 EB 82 27 F6 A0 72 C8 E2
91 78 28 2E E5 A9 E6 83 92 5E 97 C5 F1 5F 71 68
23 B8 E1 05 6C 7D C8 46 14 94 7E 4A 31 EC E0 0D
8B 1E DA B4 78 74 0E 02 41 78 E7 C2 80 65 C0 C5
CC 84 74 9C AD 7F C3 C6 0D E7 27 61 8B 56 FE 3A
F0 03 FD D5 AB 02 54 28
```

After Permutation

```
C1 C3 69 25 B6 40 9A 04 F1 B5 04 FC BC A9 D8 2B
40 17 27 7C B5 ED 2B 20 65 FC 1D 38 14 D5 AA F5
9C BC E8 30 07 9C 45 2A BD EB 87 53 66 A4 9E BF
E7 5B 89 EF 17 39 6E 34 89 8E 90 48 30 B0 E1 36
F1 92 CC 06 2B D2 E1 16 A0 7F E6 EB 9B 4F C9 BA
```

25 4D 7D BF 6E C9 86 0C 5B A3 86 86 EA 29 4D D7
72 C1 FA D2 0E 42 14 AA D5 39 4A 26 71 01 E4 C9
D0 9C E8 02 81 DB 7E 91 70 D6 05 2A BE 6E 5A 93
57 13 E2 C6 23 65 F5 9C 9A 7D F5 A9 8E 40 40 FF
70 E8 50 60 10 7F 59 6A CD BF 87 6E 67 8D 73 F2
D4 49 43 02 22 62 19 AC 0A 9F EE D4 41 8D 72 DA
7A C8 E5 06 32 0B 71 FA 26 81 02 FA 03 70 B8 A5
1D F4 E0 26 4E 12 23 DB

Outval is

C1 C3 69 25 B6 40 9A 04 F1 B5 04 FC BC A9 D8 2B
40 17 27 7C B5 ED 2B 20 65 FC 1D 38 14 D5 AA F5

==========

cSHAKE:

Sample #2

Security Strength: 128-bits

Length of data is 1600-bits

Data is

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F
50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F
70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
80 81 82 83 84 85 86 87 88 89 8A 8B 8C 8D 8E 8F
90 91 92 93 94 95 96 97 98 99 9A 9B 9C 9D 9E 9F
A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC AD AE AF
B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB BC BD BE BF
C0 C1 C2 C3 C4 C5 C6 C7

Requested output length is 256-bits

N is

(empty string)

S (as a character string) is

"Email Signature"

Encoded N

01 00

Encoded S

01 78 45 6D 61 69 6C 20 53 69 67 6E 61 74 75 72
65

bytepad data

01 A8 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

About to Absorb data

State (in bytes)

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Data to be absorbed

01 A8 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Xor'd state (in bytes)

01 A8 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

After Permutation
19 4C CD 05 8B 2A 83 D6 02 29 DC 69 84 D1 4F 15
8B 69 4F A4 BD 39 B2 1F 84 FB 06 C8 CB C6 7B 84
2D EF 9E 2B DB F0 F8 E1 BD 14 EA CC DC 58 26 84
62 4B 41 B6 4A 08 51 06 81 79 FD FB CA DB 73 1E
17 59 36 47 ED 96 C6 E3 5C DA 77 06 97 54 F5 F8
25 66 42 92 C6 79 78 FC B7 BD 58 31 ED 10 76 A6
FD 14 F3 4F FF AB 28 72 96 60 AB 82 DF 4A FD FF
81 EF 67 1C 91 81 E5 C6 EB 82 27 F6 A0 72 C8 E2
91 78 28 2E E5 A9 E6 83 92 5E 97 C5 F1 5F 71 68
23 B8 E1 05 6C 7D C8 46 14 94 7E 4A 31 EC E0 0D
8B 1E DA B4 78 74 0E 82 41 78 E7 C2 80 65 C0 C5
CC 84 74 9C AD 7F C3 C6 0D E7 27 61 8B 56 FE 3A
F0 03 FD D5 AB 02 54 28

About to Absorb data
State (in bytes)
19 4C CD 05 8B 2A 83 D6 02 29 DC 69 84 D1 4F 15
8B 69 4F A4 BD 39 B2 1F 84 FB 06 C8 CB C6 7B 84
2D EF 9E 2B DB F0 F8 E1 BD 14 EA CC DC 58 26 84
62 4B 41 B6 4A 08 51 06 81 79 FD FB CA DB 73 1E
17 59 36 47 ED 96 C6 E3 5C DA 77 06 97 54 F5 F8
25 66 42 92 C6 79 78 FC B7 BD 58 31 ED 10 76 A6
FD 14 F3 4F FF AB 28 72 96 60 AB 82 DF 4A FD FF
81 EF 67 1C 91 81 E5 C6 EB 82 27 F6 A0 72 C8 E2
91 78 28 2E E5 A9 E6 83 92 5E 97 C5 F1 5F 71 68
23 B8 E1 05 6C 7D C8 46 14 94 7E 4A 31 EC E0 0D
8B 1E DA B4 78 74 0E 82 41 78 E7 C2 80 65 C0 C5
CC 84 74 9C AD 7F C3 C6 0D E7 27 61 8B 56 FE 3A
F0 03 FD D5 AB 02 54 28
Data to be absorbed
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F
50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F
70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
80 81 82 83 84 85 86 87 88 89 8A 8B 8C 8D 8E 8F
90 91 92 93 94 95 96 97 98 99 9A 9B 9C 9D 9E 9F
A0 A1 A2 A3 A4 A5 A6 A7 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
Xor'd state (in bytes)
19 4D CF 06 8F 2F 85 D1 0A 20 D6 62 88 DC 41 1A
9B 78 5D B7 A9 2C A4 08 9C E2 1C D3 D7 DB 65 9B
0D CE BC 08 FF D5 DE C6 95 3D C0 E7 F0 75 08 AB

52 7A 73 85 7E 3D 67 31 B9 40 C7 C0 F6 E6 4D 21
57 18 74 04 A9 D3 80 A4 14 93 3D 4D DB 19 BB B7
75 37 10 C1 92 2C 2E AB EF E4 02 6A B1 4D 28 F9
9D 75 91 2C 9B CE 4E 15 FE 09 C1 E9 B3 27 93 90
F1 9E 15 6F E5 F4 93 B1 93 FB 5D 8D DC 0F B6 9D
11 F9 AA AD 61 2C 60 04 1A D7 1D 4E 7D D2 FF E7
B3 29 73 96 F8 E8 5E D1 8C 0D E4 D1 AD 71 7E 92
2B BF 78 17 DC D1 A8 25 41 78 E7 C2 80 65 C0 C5
CC 84 74 9C AD 7F C3 C6 0D E7 27 61 8B 56 FE 3A
F0 03 FD D5 AB 02 54 28

After Permutation
21 9E E1 B0 D0 45 45 C1 83 58 52 03 59 FE D6 31
FE EC 7E 89 A1 A0 6F DF 44 82 CD FF 46 0F 12 78
DD F1 06 C3 5D C3 EE 15 19 D3 6F 53 78 5A C8 79
F5 B0 67 A7 91 C9 01 C6 30 94 D5 CB 68 8A DC A8
92 2F 9D AB AC AB AF 3D 6F 0D 49 33 E6 30 B7 66
C1 ED A7 83 EB 47 E0 BA A8 BA BC 1C C3 D5 5D 7B
07 02 21 03 75 5D 49 58 10 BC 04 91 4F 2C 93 2F
E2 73 D0 51 0E 8B 38 A9 4F 4A 66 4D 5A 03 DC 16
64 72 87 D1 B4 D6 33 49 26 9E EC 36 ED 6B 43 99
EF 49 F5 E0 8A AA C4 12 B0 50 99 0A 78 83 F9 D2
67 C1 69 43 83 55 CE 2A 3B AE 84 E3 1D 34 DD 48
B1 40 66 1A BE 38 A8 A1 1D 30 ED B9 61 97 D9 A6
60 BC CC 6F 05 34 FB F9
about to call last of the absorb phase

About to Absorb data
State (in bytes)
21 9E E1 B0 D0 45 45 C1 83 58 52 03 59 FE D6 31
FE EC 7E 89 A1 A0 6F DF 44 82 CD FF 46 0F 12 78
DD F1 06 C3 5D C3 EE 15 19 D3 6F 53 78 5A C8 79
F5 B0 67 A7 91 C9 01 C6 30 94 D5 CB 68 8A DC A8
92 2F 9D AB AC AB AF 3D 6F 0D 49 33 E6 30 B7 66
C1 ED A7 83 EB 47 E0 BA A8 BA BC 1C C3 D5 5D 7B
07 02 21 03 75 5D 49 58 10 BC 04 91 4F 2C 93 2F
E2 73 D0 51 0E 8B 38 A9 4F 4A 66 4D 5A 03 DC 16
64 72 87 D1 B4 D6 33 49 26 9E EC 36 ED 6B 43 99
EF 49 F5 E0 8A AA C4 12 B0 50 99 0A 78 83 F9 D2
67 C1 69 43 83 55 CE 2A 3B AE 84 E3 1D 34 DD 48
B1 40 66 1A BE 38 A8 A1 1D 30 ED B9 61 97 D9 A6
60 BC CC 6F 05 34 FB F9
Data to be absorbed
A8 A9 AA AB AC AD AE AF B0 B1 B2 B3 B4 B5 B6 B7
B8 B9 BA BB BC BD BE BF C0 C1 C2 C3 C4 C5 C6 C7
04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00

Xor'd state (in bytes)

89 37 4B 1B 7C E8 EB 6E 33 E9 E0 B0 ED 4B 60 86
46 55 C4 32 1D 1D D1 60 84 43 0F 3C 82 CA D4 BF
D9 F1 06 C3 5D C3 EE 15 19 D3 6F 53 78 5A C8 79
F5 B0 67 A7 91 C9 01 C6 30 94 D5 CB 68 8A DC A8
92 2F 9D AB AC AB AF 3D 6F 0D 49 33 E6 30 B7 66
C1 ED A7 83 EB 47 E0 BA A8 BA BC 1C C3 D5 5D 7B
07 02 21 03 75 5D 49 58 10 BC 04 91 4F 2C 93 2F
E2 73 D0 51 0E 8B 38 A9 4F 4A 66 4D 5A 03 DC 16
64 72 87 D1 B4 D6 33 49 26 9E EC 36 ED 6B 43 99
EF 49 F5 E0 8A AA C4 12 B0 50 99 0A 78 83 F9 D2
67 C1 69 43 83 55 CE AA 3B AE 84 E3 1D 34 DD 48
B1 40 66 1A BE 38 A8 A1 1D 30 ED B9 61 97 D9 A6
60 BC CC 6F 05 34 FB F9

After Permutation

C5 22 1D 50 E4 F8 22 D9 6A 2E 88 81 A9 61 42 0F
29 4B 7B 24 FE 3D 20 94 BA ED 2C 65 24 CC 16 6B
6A FA 37 64 99 E3 CB CB B4 CF 61 FE 4D 06 34 73
BB E5 69 50 04 A7 DF 73 24 1B 37 E7 15 6C 7D 95
2C B5 50 0A 6C 23 BF 76 AC 00 96 44 EC C6 15 B5
7C 2E 4B 26 FF 84 94 9F 80 C6 EC 25 96 26 AE F8
DE FA FE 66 57 E2 77 2D 27 72 2E 43 E1 AD 9F 67
CE AE 6A FA 2C 0F 92 77 35 EC 89 AF 89 A7 CB E9
EB 05 95 3B AE 79 08 04 79 7C DC 0A F1 FA 0D 9D
59 15 73 43 65 97 E6 AC C1 D7 1F 3C 44 5A 30 0C
1A 17 A6 E9 2A 25 D5 B9 FD 3C 7E 67 BE 02 40 E1
80 01 E4 65 7E 7C 1D 34 ED 54 6F 20 72 ED 02 2E
CD 76 36 87 69 18 59 04

Outval is

C5 22 1D 50 E4 F8 22 D9 6A 2E 88 81 A9 61 42 0F
29 4B 7B 24 FE 3D 20 94 BA ED 2C 65 24 CC 16 6B

==========

cSHAKE:

Sample #3

Security Strength: 256-bits

Length of data is 32-bits

Data is

00 01 02 03

Requested output length is 512-bits

N is

(empty string)

S (as a character string) is

"Email Signature"

Encoded N

01 00

Encoded S

01 78 45 6D 61 69 6C 20 53 69 67 6E 61 74 75 72
65

bytepad data

01 88 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

About to Absorb data

State (in bytes)

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Data to be absorbed

01 88 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Xor'd state (in bytes)

```
01 88 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

After Permutation

```
EF 16 AA 15 D8 D1 21 7D 44 4F ED CC 2A BB 44 07
89 53 75 39 4D 77 26 0E E4 06 5F 70 EB D5 42 89
28 E8 B7 14 5B 60 3D 7A D9 37 D5 2E 8E B3 1C B5
17 E1 58 EB EB 30 3A C8 68 CA FC 51 0C 55 C9 48
E5 51 C0 14 09 26 82 29 F6 DD 15 30 1C FD D5 2E
A4 BD 15 9F C3 B7 8E 4E 72 EE 8A B6 EC 5C BE AF
04 24 92 67 64 17 4B 4D A5 0A 50 D0 70 C5 94 13
CA C4 58 01 88 87 1F DF B2 E8 66 54 BC 8C EA 1B
61 3C 70 70 F7 B7 9D DA 4F A6 58 28 9F A9 70 52
B2 28 93 C6 64 5A 2F 23 52 CE C9 8D 25 92 3C 56
E6 CC 4B F0 FF 4C E7 71 16 64 40 27 36 B0 19 1E
03 51 A2 B3 68 D9 4F 0A FE 5D A3 E2 D8 CE DA 6C
DE 8C 48 E9 44 E8 40 01
```

about to call last of the absorb phase

About to Absorb data

State (in bytes)

```
EF 16 AA 15 D8 D1 21 7D 44 4F ED CC 2A BB 44 07
89 53 75 39 4D 77 26 0E E4 06 5F 70 EB D5 42 89
28 E8 B7 14 5B 60 3D 7A D9 37 D5 2E 8E B3 1C B5
17 E1 58 EB EB 30 3A C8 68 CA FC 51 0C 55 C9 48
E5 51 C0 14 09 26 82 29 F6 DD 15 30 1C FD D5 2E
A4 BD 15 9F C3 B7 8E 4E 72 EE 8A B6 EC 5C BE AF
04 24 92 67 64 17 4B 4D A5 0A 50 D0 70 C5 94 13
CA C4 58 01 88 87 1F DF B2 E8 66 54 BC 8C EA 1B
61 3C 70 70 F7 B7 9D DA 4F A6 58 28 9F A9 70 52
B2 28 93 C6 64 5A 2F 23 52 CE C9 8D 25 92 3C 56
E6 CC 4B F0 FF 4C E7 71 16 64 40 27 36 B0 19 1E
03 51 A2 B3 68 D9 4F 0A FE 5D A3 E2 D8 CE DA 6C
DE 8C 48 E9 44 E8 40 01
```

Data to be absorbed

```
00 01 02 03 04 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Xor'd state (in bytes)

EF 17 A8 16 DC D1 21 7D 44 4F ED CC 2A BB 44 07
89 53 75 39 4D 77 26 0E E4 06 5F 70 EB D5 42 89
28 E8 B7 14 5B 60 3D 7A D9 37 D5 2E 8E B3 1C B5
17 E1 58 EB EB 30 3A C8 68 CA FC 51 0C 55 C9 48
E5 51 C0 14 09 26 82 29 F6 DD 15 30 1C FD D5 2E
A4 BD 15 9F C3 B7 8E 4E 72 EE 8A B6 EC 5C BE AF
04 24 92 67 64 17 4B 4D A5 0A 50 D0 70 C5 94 13
CA C4 58 01 88 87 1F DF B2 E8 66 54 BC 8C EA 1B
61 3C 70 70 F7 B7 9D 5A 4F A6 58 28 9F A9 70 52
B2 28 93 C6 64 5A 2F 23 52 CE C9 8D 25 92 3C 56
E6 CC 4B F0 FF 4C E7 71 16 64 40 27 36 B0 19 1E
03 51 A2 B3 68 D9 4F 0A FE 5D A3 E2 D8 CE DA 6C
DE 8C 48 E9 44 E8 40 01

After Permutation

D0 08 82 8E 2B 80 AC 9D 22 18 FF EE 1D 07 0C 48
B8 E4 C8 7B FF 32 C9 69 9D 5B 68 96 EE E0 ED D1
64 02 0E 2B E0 56 08 58 D9 C0 0C 03 7E 34 A9 69
37 C5 61 A7 4C 41 2B B4 C7 46 46 95 27 28 1C 8C
7B DF 2D 26 91 9F B4 65 D4 85 37 83 9C B9 22 CB
A3 38 8D 3A B3 46 65 6D FA 59 8E 4E 26 F6 35 97
49 16 A2 56 C0 01 12 C0 04 55 F3 A1 DE 46 76 82
F8 6F FD C3 A6 D0 96 B4 2C 5D 0E 68 FF 63 A4 49
40 69 2F 42 D6 84 F1 C1 A7 B8 98 6B FD 52 6D ED
5C 12 2A 36 C7 DB C8 CD A7 C2 BB F5 DA 17 C5 1A
3E B9 DB A9 A0 37 92 32 4C A1 00 69 EE 7B 13 E1
7D 84 9E 69 97 50 EE E3 A3 91 31 2F 58 DF 2A 82
F0 FF 68 51 38 0D 6B 61

Outval is

D0 08 82 8E 2B 80 AC 9D 22 18 FF EE 1D 07 0C 48
B8 E4 C8 7B FF 32 C9 69 9D 5B 68 96 EE E0 ED D1
64 02 0E 2B E0 56 08 58 D9 C0 0C 03 7E 34 A9 69
37 C5 61 A7 4C 41 2B B4 C7 46 46 95 27 28 1C 8C

==========

cSHAKE:

Sample #4

Security Strength: 256-bits

Length of data is 1600-bits
Data is

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F
50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F
70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
80 81 82 83 84 85 86 87 88 89 8A 8B 8C 8D 8E 8F
90 91 92 93 94 95 96 97 98 99 9A 9B 9C 9D 9E 9F
A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC AD AE AF
B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB BC BD BE BF
C0 C1 C2 C3 C4 C5 C6 C7

Requested output length is 512-bits

N is

(empty string)

S (as a character string) is

"Email Signature"

Encoded N

01 00

Encoded S

01 78 45 6D 61 69 6C 20 53 69 67 6E 61 74 75 72
65

bytepad data

01 88 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

About to Absorb data

State (in bytes)

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Data to be absorbed

01 88 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Xor'd state (in bytes)

01 88 01 00 01 78 45 6D 61 69 6C 20 53 69 67 6E
61 74 75 72 65 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

After Permutation

EF 16 AA 15 D8 D1 21 7D 44 4F ED CC 2A BB 44 07
89 53 75 39 4D 77 26 0E E4 06 5F 70 EB D5 42 89
28 E8 B7 14 5B 60 3D 7A D9 37 D5 2E 8E B3 1C B5
17 E1 58 EB EB 30 3A C8 68 CA FC 51 0C 55 C9 48
E5 51 C0 14 09 26 82 29 F6 DD 15 30 1C FD D5 2E
A4 BD 15 9F C3 B7 8E 4E 72 EE 8A B6 EC 5C BE AF
04 24 92 67 64 17 4B 4D A5 0A 50 D0 70 C5 94 13
CA C4 58 01 88 87 1F DF B2 E8 66 54 BC 8C EA 1B
61 3C 70 70 F7 B7 9D DA 4F A6 58 28 9F A9 70 52
B2 28 93 C6 64 5A 2F 23 52 CE C9 8D 25 92 3C 56
E6 CC 4B F0 FF 4C E7 71 16 64 40 27 36 B0 19 1E
03 51 A2 B3 68 D9 4F 0A FE 5D A3 E2 D8 CE DA 6C
DE 8C 48 E9 44 E8 40 01

About to Absorb data

State (in bytes)

EF 16 AA 15 D8 D1 21 7D 44 4F ED CC 2A BB 44 07

89 53 75 39 4D 77 26 0E E4 06 5F 70 EB D5 42 89
28 E8 B7 14 5B 60 3D 7A D9 37 D5 2E 8E B3 1C B5
17 E1 58 EB EB 30 3A C8 68 CA FC 51 0C 55 C9 48
E5 51 C0 14 09 26 82 29 F6 DD 15 30 1C FD D5 2E
A4 BD 15 9F C3 B7 8E 4E 72 EE 8A B6 EC 5C BE AF
04 24 92 67 64 17 4B 4D A5 0A 50 D0 70 C5 94 13
CA C4 58 01 88 87 1F DF B2 E8 66 54 BC 8C EA 1B
61 3C 70 70 F7 B7 9D DA 4F A6 58 28 9F A9 70 52
B2 28 93 C6 64 5A 2F 23 52 CE C9 8D 25 92 3C 56
E6 CC 4B F0 FF 4C E7 71 16 64 40 27 36 B0 19 1E
03 51 A2 B3 68 D9 4F 0A FE 5D A3 E2 D8 CE DA 6C
DE 8C 48 E9 44 E8 40 01

Data to be absorbed

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F
50 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F
60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F
70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F
80 81 82 83 84 85 86 87 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Xor'd state (in bytes)

EF 17 A8 16 DC D4 27 7A 4C 46 E7 C7 26 B6 4A 08
99 42 67 2A 59 62 30 19 FC 1F 45 6B F7 C8 5C 96
08 C9 95 37 7F 45 1B 5D F1 1E FF 05 A2 9E 32 9A
27 D0 6A D8 DF 05 0C FF 50 F3 C6 6A 30 68 F7 77
A5 10 82 57 4D 63 C4 6E BE 94 5F 7B 50 B0 9B 61
F4 EC 47 CC 97 E2 D8 19 2A B7 D0 ED B0 01 E0 F0
64 45 F0 04 00 72 2D 2A CD 63 3A BB 1C A8 FA 7C
BA B5 2A 72 FC F2 69 A8 CA 91 1C 2F C0 F1 94 64
E1 BD F2 F3 73 32 1B 5D 4F A6 58 28 9F A9 70 52
B2 28 93 C6 64 5A 2F 23 52 CE C9 8D 25 92 3C 56
E6 CC 4B F0 FF 4C E7 71 16 64 40 27 36 B0 19 1E
03 51 A2 B3 68 D9 4F 0A FE 5D A3 E2 D8 CE DA 6C
DE 8C 48 E9 44 E8 40 01

After Permutation

3B D1 F7 83 1E 44 C4 88 D9 BC D1 56 06 A2 DF 05
DC 80 2A 1E D3 04 0A 50 53 97 59 CF 78 A3 30 FC
0A 18 73 37 7F 07 5B 35 C2 CE 6A 81 6B D6 F6 9B
63 DB 63 53 6B F3 3E B0 5D C3 CF 95 C1 CA D5 37
1D 40 DE 51 DE D9 C9 DC FB BD EA 7A 4C 89 DD 1C
FA D1 48 11 C9 90 D2 14 6E 73 A9 B9 72 3E 5D 5E
D8 E8 49 D3 9F F6 85 24 D9 29 99 0D B4 FF 5C 2B
91 13 FA D1 11 2A D6 E9 D3 FE 70 AF F0 63 6F 09
4C F9 D4 E6 A7 A9 D4 F6 D8 67 11 52 9B C5 8B DD

E3 51 49 95 19 9B 1C DE 5F D6 E8 D9 FC 91 AE D9
F7 A1 9F E5 BE E6 D6 EE 7E DD 1D AC FE 1B CF 40
56 07 A2 1F 88 0E 61 A6 59 F4 C1 4E 09 C8 66 23
E2 62 94 5A 3B 11 B6 49
about to call last of the absorb phase

About to Absorb data
State (in bytes)
3B D1 F7 83 1E 44 C4 88 D9 BC D1 56 06 A2 DF 05
DC 80 2A 1E D3 04 0A 50 53 97 59 CF 78 A3 30 FC
0A 18 73 37 7F 07 5B 35 C2 CE 6A 81 6B D6 F6 9B
63 DB 63 53 6B F3 3E B0 5D C3 CF 95 C1 CA D5 37
1D 40 DE 51 DE D9 C9 DC FB BD EA 7A 4C 89 DD 1C
FA D1 48 11 C9 90 D2 14 6E 73 A9 B9 72 3E 5D 5E
D8 E8 49 D3 9F F6 85 24 D9 29 99 0D B4 FF 5C 2B
91 13 FA D1 11 2A D6 E9 D3 FE 70 AF F0 63 6F 09
4C F9 D4 E6 A7 A9 D4 F6 D8 67 11 52 9B C5 8B DD
E3 51 49 95 19 9B 1C DE 5F D6 E8 D9 FC 91 AE D9
F7 A1 9F E5 BE E6 D6 EE 7E DD 1D AC FE 1B CF 40
56 07 A2 1F 88 0E 61 A6 59 F4 C1 4E 09 C8 66 23
E2 62 94 5A 3B 11 B6 49
Data to be absorbed
88 89 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97
98 99 9A 9B 9C 9D 9E 9F A0 A1 A2 A3 A4 A5 A6 A7
A8 A9 AA AB AC AD AE AF B0 B1 B2 B3 B4 B5 B6 B7
B8 B9 BA BB BC BD BE BF C0 C1 C2 C3 C4 C5 C6 C7
04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00
Xor'd state (in bytes)
B3 58 7D 08 92 C9 4A 07 49 2D 43 C5 92 37 49 92
44 19 B0 85 4F 99 94 CF F3 36 FB 6C DC 06 96 5B
A2 B1 D9 9C D3 AA F5 9A 72 7F D8 32 DF 63 40 2C
DB 62 D9 E8 D7 4E 80 0F 9D 02 0D 56 05 0F 13 F0
19 40 DE 51 DE D9 C9 DC FB BD EA 7A 4C 89 DD 1C
FA D1 48 11 C9 90 D2 14 6E 73 A9 B9 72 3E 5D 5E
D8 E8 49 D3 9F F6 85 24 D9 29 99 0D B4 FF 5C 2B
91 13 FA D1 11 2A D6 E9 D3 FE 70 AF F0 63 6F 09
4C F9 D4 E6 A7 A9 D4 76 D8 67 11 52 9B C5 8B DD
E3 51 49 95 19 9B 1C DE 5F D6 E8 D9 FC 91 AE D9
F7 A1 9F E5 BE E6 D6 EE 7E DD 1D AC FE 1B CF 40
56 07 A2 1F 88 0E 61 A6 59 F4 C1 4E 09 C8 66 23
E2 62 94 5A 3B 11 B6 49

After Permutation

07 DC 27 B1 1E 51 FB AC 75 BC 7B 3C 1D 98 3E 8B
4B 85 FB 1D EF AF 21 89 12 AC 86 43 02 73 09 17
27 F4 2B 17 ED 1D F6 3E 8E C1 18 F0 4B 23 63 3C
1D FB 15 74 C8 FB 55 CB 45 DA 8E 25 AF B0 92 BB
DA 60 4F E5 C6 AC 1C DD 07 35 EF 81 67 D7 97 E8
87 03 DC 78 F3 38 98 D4 53 53 FF 59 FC ED 67 02
AF 2B 64 09 9F 50 46 1C D5 A7 87 CE DF CA 60 C0
3E 6C EC 10 8A 0F 01 F0 26 09 09 7C E6 45 54 19
7E DB C5 3C 2F 1D CA BF C3 94 76 DB FD 5B 8E 2E
7E A1 04 D2 8B 86 27 70 2A 98 60 B4 56 84 1C BA
D0 71 04 1F 8B 1A 88 38 F6 3E 07 EE CD C8 99 A6
C0 69 78 E4 0A 14 96 28 3C 3E D5 69 2A 86 02 F0
8A A7 90 2D 11 6C EC 3C

Outval is

07 DC 27 B1 1E 51 FB AC 75 BC 7B 3C 1D 98 3E 8B
4B 85 FB 1D EF AF 21 89 12 AC 86 43 02 73 09 17
27 F4 2B 17 ED 1D F6 3E 8E C1 18 F0 4B 23 63 3C
1D FB 15 74 C8 FB 55 CB 45 DA 8E 25 AF B0 92 BB

==========