

#####

SHA-3 Derived Functions

- cSHAKE
- KMAC
- TupleHash
- ParallelHash

#####

KMAC:

Sample #1

Security Strength: 128-bits

Length of Key is 256-bits

Key is

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

Length of data is 32-bits

Data is

00 01 02 03

Requested output length is 256-bits

S (as a character string) is

"(null)"

Encoded K

02 01 00 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

byte_padded stuff

01 A8 02 01 00 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 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00

Right_encoded L

01 00 02

Encoded N

01 20 4B 4D 41 43

Encoded S

01 00

bytepad data

01 A8 01 20 4B 4D 41 43 01 00 00 00 00 00 00 00

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

6B B3 7D 98 44 EE A0 FF BA 27 9A 80 6E B8 C0 FE
CE 28 1C 62 8B E2 28 35 20 51 43 74 02 7B 79 A8
A8 11 31 62 BA F5 60 20 F3 CF 28 E8 35 D8 84 9E
E2 EE 66 5E 1B 9E 29 1A 43 EE B7 A5 16 90 42 C4
1D 5B 92 DB FC C7 58 7F 4D E6 CE FC 99 DB A7 28
70 15 12 DE 44 A6 17 44 50 94 D4 BC F9 FA 99 EB
D2 29 B1 86 2D 8A 5C B7 47 8C DF 2D D9 2B 0A 7A
C7 D2 B0 1C 34 9A B2 94 54 83 AD D3 7E 8A F4 89
48 43 0F 57 C6 2A BD BA 3B 4E 6D B5 7C 38 16 7A
53 03 0D E0 DC 18 64 B4 32 56 FF 73 7E 07 B5 8D
69 70 74 02 57 9D 26 26 A8 FB 00 2C 7A 01 92 8F
F4 DD EB 78 BD 1E 70 01 81 41 44 4A E6 6C CA F7
4B D5 85 37 F3 84 FE 21

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

6B B3 7D 98 44 EE A0 FF BA 27 9A 80 6E B8 C0 FE
CE 28 1C 62 8B E2 28 35 20 51 43 74 02 7B 79 A8
A8 11 31 62 BA F5 60 20 F3 CF 28 E8 35 D8 84 9E
E2 EE 66 5E 1B 9E 29 1A 43 EE B7 A5 16 90 42 C4
1D 5B 92 DB FC C7 58 7F 4D E6 CE FC 99 DB A7 28
70 15 12 DE 44 A6 17 44 50 94 D4 BC F9 FA 99 EB
D2 29 B1 86 2D 8A 5C B7 47 8C DF 2D D9 2B 0A 7A
C7 D2 B0 1C 34 9A B2 94 54 83 AD D3 7E 8A F4 89
48 43 0F 57 C6 2A BD BA 3B 4E 6D B5 7C 38 16 7A
53 03 0D E0 DC 18 64 B4 32 56 FF 73 7E 07 B5 8D
69 70 74 02 57 9D 26 26 A8 FB 00 2C 7A 01 92 8F
F4 DD EB 78 BD 1E 70 01 81 41 44 4A E6 6C CA F7
4B D5 85 37 F3 84 FE 21

Data to be absorbed

01 A8 02 01 00 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 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)

6A 1B 7F 99 44 AE E1 BD F9 63 DF C6 29 F0 89 B4
85 64 51 2C C4 B2 79 67 73 05 16 22 55 23 20 F2

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

Xor'd state (in bytes)

97 82 35 47 D5 0F 99 45 83 5F 3B 61 D0 5A 92 36
B9 DA C5 A2 7F C3 32 CE C0 27 63 B5 81 19 17 CE
8E DB 85 5D C1 D0 4E FF B8 0A 19 6E D5 75 57 94
FD 68 40 62 73 83 EF 2A 11 0F C4 3A E4 F8 83 F6
DF 18 C4 56 27 95 91 54 F0 DD BC 54 26 FE 2A C0
CD 0C 7E 86 4E D2 FB 8C 98 45 A6 9D 05 A8 57 1B
88 B7 36 DA 9F F6 3E 09 F0 DF 36 DC 59 97 A4 88
DE 80 5B D8 02 73 0B 3A 63 52 9C 31 FD 09 64 53
A0 C0 5F CA E9 9F 3C 77 A0 CA 55 76 8E CE 2E 88
1A 29 FF 4B B4 33 83 9E 02 B0 59 31 3B 5C A0 F2
19 95 06 15 FF B0 FC BA 4A 90 B6 E1 F4 90 DB 66
F1 0B 08 53 1E 4E F5 A2 7D 07 AF AB F6 12 0D 40
88 C9 F7 B7 F2 37 E1 4C

After Permutation

E5 78 0B 0D 3E A6 F7 D3 A4 29 C5 70 6A A4 3A 00
FA DB D7 D4 96 28 83 9E 31 87 24 3F 45 6E E1 4E
F9 8D 16 01 65 48 8F 41 D3 B5 DD C2 06 5D 15 47
7A 0C 69 38 A7 31 E1 6D 16 D4 68 A0 7F 39 C5 14
06 AB B3 D0 CB C2 95 2E E9 2C BD 40 67 14 82 B1
5B 89 9A F6 9B 9E C4 EA 74 FD E2 AC E8 45 97 47
BB 44 FF F2 D1 AE C0 95 66 2F 25 DD 22 1D 71 E2
19 DD 4F 1A 41 0F 95 1C 64 35 3B DA D3 F7 49 E4
AE EA 50 54 DD 0C F7 9F 7B 3B 40 92 75 B6 16 10
81 EB 72 34 7B 29 C6 1D 98 BB FA A1 11 FD 26 0D
52 E3 FB 55 EE 1A FC 02 42 65 F1 BF 2D F3 77 7F
CC 2A C8 46 DB A3 BC 4A C8 05 3B 9D A0 6E F1 1F
FE D1 C9 72 17 A6 CF 43

Outval is

E5 78 0B 0D 3E A6 F7 D3 A4 29 C5 70 6A A4 3A 00
FA DB D7 D4 96 28 83 9E 31 87 24 3F 45 6E E1 4E

=====

KMAC:

Sample #2

Security Strength: 128-bits

Length of Key is 256-bits

Key is

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

Length of data is 32-bits

Data is

00 01 02 03

Requested output length is 256-bits

S (as a character string) is

"My Tagged Application"

Encoded K

02 01 00 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

byte_padded stuff

01 A8 02 01 00 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 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Right_encoded L

01 00 02

Encoded N

01 20 4B 4D 41 43

Encoded S

01 A8 4D 79 20 54 61 67 67 65 64 20 41 70 70 6C
69 63 61 74 69 6F 6E

bytepad data

01 A8 01 20 4B 4D 41 43 01 A8 4D 79 20 54 61 67
67 65 64 20 41 70 70 6C 69 63 61 74 69 6F 6E 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 20 4B 4D 41 43 01 A8 4D 79 20 54 61 67
67 65 64 20 41 70 70 6C 69 63 61 74 69 6F 6E 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 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 20 4B 4D 41 43 01 A8 4D 79 20 54 61 67
67 65 64 20 41 70 70 6C 69 63 61 74 69 6F 6E 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 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

0C D8 4E 9B 5F EE 43 74 9B 6A 92 1C 9D 9F 0C B4
96 7B 2F DC 09 45 18 79 F8 FE 6F 39 B9 E8 C6 41
E7 45 96 49 E7 F8 68 77 E7 EA 44 6B FC 68 57 30
75 D4 16 EE 85 EF BC A9 D2 4D 7F 8B 28 CD 02 B7
A5 63 6C 24 F5 EE A9 DD 63 9F 0F D6 1A ED 3E D8
AE 73 AF 7C 25 D8 22 55 B8 F0 A3 6A 64 F9 C3 77
B3 D5 EF 9D 95 FF 75 7D A8 1C 73 BB 05 B4 C4 80
8D CF FE 71 31 9E E1 2B C7 8B 9D 1F 37 A6 27 F9
B0 94 DE 54 AF 8A DF 65 41 C0 4F 39 0E E0 37 95
2F 41 AC 64 C6 60 54 86 07 F8 26 E3 5A 4C A4 E9
D0 A4 E1 35 65 64 81 D3 2F B2 51 38 DD 27 09 91
2B 87 56 CC 86 2A F3 A6 A7 79 BB E4 2E C6 22 DA

D1 FB 87 E3 99 3A AE BE

About to Absorb data

State (in bytes)

0C D8 4E 9B 5F EE 43 74 9B 6A 92 1C 9D 9F 0C B4
96 7B 2F DC 09 45 18 79 F8 FE 6F 39 B9 E8 C6 41
E7 45 96 49 E7 F8 68 77 E7 EA 44 6B FC 68 57 30
75 D4 16 EE 85 EF BC A9 D2 4D 7F 8B 28 CD 02 B7
A5 63 6C 24 F5 EE A9 DD 63 9F 0F D6 1A ED 3E D8
AE 73 AF 7C 25 D8 22 55 B8 F0 A3 6A 64 F9 C3 77
B3 D5 EF 9D 95 FF 75 7D A8 1C 73 BB 05 B4 C4 80
8D CF FE 71 31 9E E1 2B C7 8B 9D 1F 37 A6 27 F9
B0 94 DE 54 AF 8A DF 65 41 C0 4F 39 0E E0 37 95
2F 41 AC 64 C6 60 54 86 07 F8 26 E3 5A 4C A4 E9
D0 A4 E1 35 65 64 81 D3 2F B2 51 38 DD 27 09 91
2B 87 56 CC 86 2A F3 A6 A7 79 BB E4 2E C6 22 DA
D1 FB 87 E3 99 3A AE BE

Data to be absorbed

01 A8 02 01 00 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 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 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)

0D 70 4C 9A 5F AE 02 36 D8 2E D7 5A DA D7 45 FE
DD 37 62 92 46 15 49 2B AB AA 3A 6F EE B0 9F 1B
BC 19 CB 17 B8 F8 68 77 E7 EA 44 6B FC 68 57 30
75 D4 16 EE 85 EF BC A9 D2 4D 7F 8B 28 CD 02 B7
A5 63 6C 24 F5 EE A9 DD 63 9F 0F D6 1A ED 3E D8
AE 73 AF 7C 25 D8 22 55 B8 F0 A3 6A 64 F9 C3 77
B3 D5 EF 9D 95 FF 75 7D A8 1C 73 BB 05 B4 C4 80
8D CF FE 71 31 9E E1 2B C7 8B 9D 1F 37 A6 27 F9
B0 94 DE 54 AF 8A DF 65 41 C0 4F 39 0E E0 37 95
2F 41 AC 64 C6 60 54 86 07 F8 26 E3 5A 4C A4 E9
D0 A4 E1 35 65 64 81 D3 2F B2 51 38 DD 27 09 91
2B 87 56 CC 86 2A F3 A6 A7 79 BB E4 2E C6 22 DA
D1 FB 87 E3 99 3A AE BE

After Permutation

CA 45 05 D4 05 6D 01 72 F6 A1 7B 5F 9F 75 75 D7
94 1B 8E 38 D8 1B F9 DB 86 56 2B 11 39 25 5F 1E
A8 BC EB 25 56 72 AE EA 92 20 78 21 66 A1 EB 89
B4 5F 4F B1 03 41 45 60 11 97 00 04 F9 D2 0D BA

B3 52 D3 E7 31 88 21 7B F4 A2 70 01 9B 95 5F C5
1E 62 1C 7C 61 7F 71 DC DC 45 AD AD 17 CC 74 4D
A8 8E 63 8A 83 48 CE 2A E9 F0 9A CA EE 9A 86 E3
0F EF 14 17 E4 0A 4C 08 22 D2 06 62 90 D3 7B E9
F7 CE 4E DC 7B 49 09 41 43 F1 9D E4 87 3D 2E 58
86 0D A4 86 D6 40 50 02 58 49 9D 3E 4A 2A 38 D1
72 6C A2 E7 A0 74 1A 46 81 21 D0 90 F9 05 3D 5A
87 53 C1 7C 99 81 DB 89 DB 15 2E 4D 08 B5 E8 FB
09 BE 52 BD 32 88 DD B7

about to call last of the absorb phase

About to Absorb data

State (in bytes)

CA 45 05 D4 05 6D 01 72 F6 A1 7B 5F 9F 75 75 D7
94 1B 8E 38 D8 1B F9 DB 86 56 2B 11 39 25 5F 1E
A8 BC EB 25 56 72 AE EA 92 20 78 21 66 A1 EB 89
B4 5F 4F B1 03 41 45 60 11 97 00 04 F9 D2 0D BA
B3 52 D3 E7 31 88 21 7B F4 A2 70 01 9B 95 5F C5
1E 62 1C 7C 61 7F 71 DC DC 45 AD AD 17 CC 74 4D
A8 8E 63 8A 83 48 CE 2A E9 F0 9A CA EE 9A 86 E3
0F EF 14 17 E4 0A 4C 08 22 D2 06 62 90 D3 7B E9
F7 CE 4E DC 7B 49 09 41 43 F1 9D E4 87 3D 2E 58
86 0D A4 86 D6 40 50 02 58 49 9D 3E 4A 2A 38 D1
72 6C A2 E7 A0 74 1A 46 81 21 D0 90 F9 05 3D 5A
87 53 C1 7C 99 81 DB 89 DB 15 2E 4D 08 B5 E8 FB
09 BE 52 BD 32 88 DD B7

Data to be absorbed

00 01 02 03 01 00 02 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

Xor'd state (in bytes)

CA 44 07 D7 04 6D 03 76 F6 A1 7B 5F 9F 75 75 D7
94 1B 8E 38 D8 1B F9 DB 86 56 2B 11 39 25 5F 1E
A8 BC EB 25 56 72 AE EA 92 20 78 21 66 A1 EB 89
B4 5F 4F B1 03 41 45 60 11 97 00 04 F9 D2 0D BA
B3 52 D3 E7 31 88 21 7B F4 A2 70 01 9B 95 5F C5
1E 62 1C 7C 61 7F 71 DC DC 45 AD AD 17 CC 74 4D
A8 8E 63 8A 83 48 CE 2A E9 F0 9A CA EE 9A 86 E3
0F EF 14 17 E4 0A 4C 08 22 D2 06 62 90 D3 7B E9
F7 CE 4E DC 7B 49 09 41 43 F1 9D E4 87 3D 2E 58
86 0D A4 86 D6 40 50 02 58 49 9D 3E 4A 2A 38 D1

72 6C A2 E7 A0 74 1A C6 81 21 D0 90 F9 05 3D 5A
87 53 C1 7C 99 81 DB 89 DB 15 2E 4D 08 B5 E8 FB
09 BE 52 BD 32 88 DD B7

After Permutation

3B 1F BA 96 3C D8 B0 B5 9E 8C 1A 6D 71 88 8B 71
43 65 1A F8 BA 0A 70 70 C0 97 9E 28 11 32 4A A5
3A 25 BB 24 A5 3A 59 D4 E5 CE 83 A6 B9 FE DC 9B
C3 97 B3 F6 CA AE 66 F5 3D E0 75 C9 CF 54 F2 AA
2A D9 E7 BD 7F F6 6A F0 0A D5 44 77 00 1F B1 CC
AF 46 E0 51 9D AF 30 B8 51 8C BE 65 B8 9A 88 74
4F 5C BF 85 E8 A0 40 E3 78 3B F2 E9 79 64 36 FF
89 7B AE F2 1F C8 0F 17 C8 19 C5 60 21 13 CF F8
9B 6B DB 84 2D 6F B1 E3 12 58 C7 39 B5 6E 89 42
92 26 1F 5E 47 34 C4 B2 F1 4C 60 4E 31 88 74 D3
3B 7C BD CB 7A 41 AD 37 34 D7 8E 57 63 F4 49 9B
D7 86 93 02 F6 7C 4A 3E FE 74 F9 18 EF 67 3D E3
E8 56 ED 6A EA E5 61 6D

Output is

3B 1F BA 96 3C D8 B0 B5 9E 8C 1A 6D 71 88 8B 71
43 65 1A F8 BA 0A 70 70 C0 97 9E 28 11 32 4A A5

=====

KMAC:

Sample #3

Security Strength: 128-bits

Length of Key is 256-bits

Key is

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

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

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 20 4B 4D 41 43 01 A8 4D 79 20 54 61 67
67 65 64 20 41 70 70 6C 69 63 61 74 69 6F 6E 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 20 4B 4D 41 43 01 A8 4D 79 20 54 61 67
67 65 64 20 41 70 70 6C 69 63 61 74 69 6F 6E 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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

0C D8 4E 9B 5F EE 43 74 9B 6A 92 1C 9D 9F 0C B4
96 7B 2F DC 09 45 18 79 F8 FE 6F 39 B9 E8 C6 41
E7 45 96 49 E7 F8 68 77 E7 EA 44 6B FC 68 57 30
75 D4 16 EE 85 EF BC A9 D2 4D 7F 8B 28 CD 02 B7
A5 63 6C 24 F5 EE A9 DD 63 9F 0F D6 1A ED 3E D8
AE 73 AF 7C 25 D8 22 55 B8 F0 A3 6A 64 F9 C3 77
B3 D5 EF 9D 95 FF 75 7D A8 1C 73 BB 05 B4 C4 80
8D CF FE 71 31 9E E1 2B C7 8B 9D 1F 37 A6 27 F9
B0 94 DE 54 AF 8A DF 65 41 C0 4F 39 0E E0 37 95
2F 41 AC 64 C6 60 54 86 07 F8 26 E3 5A 4C A4 E9
D0 A4 E1 35 65 64 81 D3 2F B2 51 38 DD 27 09 91
2B 87 56 CC 86 2A F3 A6 A7 79 BB E4 2E C6 22 DA
D1 FB 87 E3 99 3A AE BE

About to Absorb data

State (in bytes)

0C D8 4E 9B 5F EE 43 74 9B 6A 92 1C 9D 9F 0C B4

86 0D A4 86 D6 40 50 02 58 49 9D 3E 4A 2A 38 D1
72 6C A2 E7 A0 74 1A 46 81 21 D0 90 F9 05 3D 5A
87 53 C1 7C 99 81 DB 89 DB 15 2E 4D 08 B5 E8 FB
09 BE 52 BD 32 88 DD B7

About to Absorb data

State (in bytes)

CA 45 05 D4 05 6D 01 72 F6 A1 7B 5F 9F 75 75 D7
94 1B 8E 38 D8 1B F9 DB 86 56 2B 11 39 25 5F 1E
A8 BC EB 25 56 72 AE EA 92 20 78 21 66 A1 EB 89
B4 5F 4F B1 03 41 45 60 11 97 00 04 F9 D2 0D BA
B3 52 D3 E7 31 88 21 7B F4 A2 70 01 9B 95 5F C5
1E 62 1C 7C 61 7F 71 DC DC 45 AD AD 17 CC 74 4D
A8 8E 63 8A 83 48 CE 2A E9 F0 9A CA EE 9A 86 E3
0F EF 14 17 E4 0A 4C 08 22 D2 06 62 90 D3 7B E9
F7 CE 4E DC 7B 49 09 41 43 F1 9D E4 87 3D 2E 58
86 0D A4 86 D6 40 50 02 58 49 9D 3E 4A 2A 38 D1
72 6C A2 E7 A0 74 1A 46 81 21 D0 90 F9 05 3D 5A
87 53 C1 7C 99 81 DB 89 DB 15 2E 4D 08 B5 E8 FB
09 BE 52 BD 32 88 DD B7

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)

CA 44 07 D7 01 68 07 75 FE A8 71 54 93 78 7B D8
84 0A 9C 2B CC 0E EF CC 9E 4F 31 0A 25 38 41 01
88 9D C9 06 72 57 88 CD BA 09 52 0A 4A 8C C5 A6
84 6E 7D 82 37 74 73 57 29 AE 3A 3F C5 EF 33 85
F3 13 91 A4 75 CD 67 3C BC EB 3A 4A D7 D8 11 8A
4E 33 4E 2F 35 2A 27 8B 84 1C F7 F6 4B 91 2A 12
C8 EF 01 E9 E7 2D A8 4D 81 99 F0 A1 82 F7 E8 8C
7F 9E 66 64 90 7F 3A 7F 5A AB 7C 19 EC AE 05 96
77 4F CC 5F FF CC 8F C6 CB 78 17 6F 0B B0 A0 D7
16 9C 36 15 42 D5 C6 95 C0 D0 07 A5 D6 B7 A6 4E
D2 CD 00 44 04 D1 BC E1 81 21 D0 90 F9 05 3D 5A
87 53 C1 7C 99 81 DB 89 DB 15 2E 4D 08 B5 E8 FB
09 BE 52 BD 32 88 DD B7

After Permutation

9E F9 B3 1A 13 95 D1 8D E8 BB DA 53 E0 BB 99 D3

61 E5 B1 C7 29 2A 39 BC B0 6A B6 0C 90 97 DA 36
39 27 11 51 44 D4 8A 59 BA 39 09 EC E6 22 00 04
1D B9 40 55 F7 1A D8 56 3A 75 AC 69 3B A1 E2 BC
DC 9B 01 17 9C AD 35 41 E0 0D D8 8F 78 4F 1B 7F
37 1E 09 6B AA 65 D9 B4 CC B6 01 A3 25 90 43 F7
FF 42 E2 BA 87 E6 06 C2 A7 EA 2D E9 74 6A 0F 2E
5D 74 74 E1 57 7D 8C 3F 2B 98 BA CC AF 38 25 B0
4E 40 CC 0D 64 65 E3 6F 0D 9C 55 70 46 33 A4 6F
32 FC 7E C0 68 BE 04 77 9F 81 14 2A 0B 73 FA 2D
05 A0 3E 5F DA D6 78 FC 50 A8 0D 3E 5A F2 C1 F8
70 20 45 49 BA 45 B6 C2 68 65 C8 AC 7B F5 0F B3
6B 3B 4B BE 1E 1A E2 21

about to call last of the absorb phase

About to Absorb data

State (in bytes)

9E F9 B3 1A 13 95 D1 8D E8 BB DA 53 E0 BB 99 D3
61 E5 B1 C7 29 2A 39 BC B0 6A B6 0C 90 97 DA 36
39 27 11 51 44 D4 8A 59 BA 39 09 EC E6 22 00 04
1D B9 40 55 F7 1A D8 56 3A 75 AC 69 3B A1 E2 BC
DC 9B 01 17 9C AD 35 41 E0 0D D8 8F 78 4F 1B 7F
37 1E 09 6B AA 65 D9 B4 CC B6 01 A3 25 90 43 F7
FF 42 E2 BA 87 E6 06 C2 A7 EA 2D E9 74 6A 0F 2E
5D 74 74 E1 57 7D 8C 3F 2B 98 BA CC AF 38 25 B0
4E 40 CC 0D 64 65 E3 6F 0D 9C 55 70 46 33 A4 6F
32 FC 7E C0 68 BE 04 77 9F 81 14 2A 0B 73 FA 2D
05 A0 3E 5F DA D6 78 FC 50 A8 0D 3E 5A F2 C1 F8
70 20 45 49 BA 45 B6 C2 68 65 C8 AC 7B F5 0F B3
6B 3B 4B BE 1E 1A E2 21

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
01 00 02 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 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)

36 50 19 B1 BF 38 7F 22 58 0A 68 E0 54 0E 2F 64
D9 5C 0B 7C 95 97 87 03 70 AB 74 CF 54 52 1C F1
38 27 13 55 44 D4 8A 59 BA 39 09 EC E6 22 00 04
1D B9 40 55 F7 1A D8 56 3A 75 AC 69 3B A1 E2 BC
DC 9B 01 17 9C AD 35 41 E0 0D D8 8F 78 4F 1B 7F
37 1E 09 6B AA 65 D9 B4 CC B6 01 A3 25 90 43 F7
FF 42 E2 BA 87 E6 06 C2 A7 EA 2D E9 74 6A 0F 2E

5D 74 74 E1 57 7D 8C 3F 2B 98 BA CC AF 38 25 B0
4E 40 CC 0D 64 65 E3 6F 0D 9C 55 70 46 33 A4 6F
32 FC 7E C0 68 BE 04 77 9F 81 14 2A 0B 73 FA 2D
05 A0 3E 5F DA D6 78 7C 50 A8 0D 3E 5A F2 C1 F8
70 20 45 49 BA 45 B6 C2 68 65 C8 AC 7B F5 0F B3
6B 3B 4B BE 1E 1A E2 21

After Permutation

1F 5B 4E 6C CA 02 20 9E 0D CB 5C A6 35 B8 9A 15
E2 71 EC C7 60 07 1D FD 80 5F AA 38 F9 72 92 30
4D 9E 14 F5 20 67 AB D2 AA 07 47 60 10 3D D3 29
B8 9A 8F 83 35 8D 74 CE D5 B9 37 DB F5 66 F3 91
99 5E 56 ED B8 66 BF F2 1D 95 A7 47 DC 24 0C 0E
15 C2 BD BE FC DA CD 6E 3A 8E 5F 29 0A 82 A6 76
29 C1 26 21 A6 8A AE E7 9D E1 3B 85 B7 66 93 64
67 5E 75 E0 88 6C CF 6E EC A0 9D D8 70 23 D5 4B
67 B0 8F F8 70 C9 B0 BF 5C 4C 15 6F 3B 49 83 56
86 E9 94 81 3E 04 31 8D A5 0B 61 58 1D 8D 1B 92
1C 35 15 C8 BC FD 0F E8 BF 36 70 5D 15 37 45 E7
84 76 D4 12 99 89 BB 51 F7 93 54 6C 51 73 67 9B
C3 7E D5 B4 8D 5D 06 AE

Output is

1F 5B 4E 6C CA 02 20 9E 0D CB 5C A6 35 B8 9A 15
E2 71 EC C7 60 07 1D FD 80 5F AA 38 F9 72 92 30

=====

KMAC:

Sample #4

Security Strength: 256-bits

Length of Key is 256-bits

Key is

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

Length of data is 32-bits

Data is

00 01 02 03

Requested output length is 512-bits

S (as a character string) is

"My Tagged Application"

Encoded K

02 01 00 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

byte_padded stuff

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 20 4B 4D 41 43 01 A8 4D 79 20 54 61 67
67 65 64 20 41 70 70 6C 69 63 61 74 69 6F 6E 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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

26 5A F0 F0 3D E7 7A 43 C7 06 AA 09 A5 0D CF 53
CC 9D 88 58 82 69 47 EC 92 4F CA DD 48 A6 72 43
81 05 9A B2 95 AD 43 43 34 C2 56 51 3C ED 8F D5
B6 54 F6 D6 F2 5E 89 8E 2B 77 A0 18 BF DB 42 2C
3F A9 D4 16 88 24 60 AD 8F C6 B3 9F 0D 67 17 F0
A5 68 95 D4 B2 D5 A8 84 3F D7 BD AD 17 EE 38 11
FD DD 16 01 7B 6E A3 E0 CD 81 DD 0B 96 1B 5F B8
9E C2 72 DE 0D 4B 57 91 0B 12 49 7E 2A 78 64 89
01 A3 A0 BA 98 AF AA 7F 6C 3D 50 2C AB 2E 17 CE
87 75 A6 69 98 84 96 2F 18 F1 6A 6F 1E 9A B8 F1
09 E1 1E 4F 8B C0 BA F8 D6 AC C5 9F 97 4F 14 DB
88 22 04 F7 BF 7A 42 A4 66 ED C5 81 AA FD 08 62
91 EB 95 EB AE 86 7A BE

About to Absorb data

State (in bytes)

26 5A F0 F0 3D E7 7A 43 C7 06 AA 09 A5 0D CF 53
CC 9D 88 58 82 69 47 EC 92 4F CA DD 48 A6 72 43
81 05 9A B2 95 AD 43 43 34 C2 56 51 3C ED 8F D5
B6 54 F6 D6 F2 5E 89 8E 2B 77 A0 18 BF DB 42 2C
3F A9 D4 16 88 24 60 AD 8F C6 B3 9F 0D 67 17 F0
A5 68 95 D4 B2 D5 A8 84 3F D7 BD AD 17 EE 38 11
FD DD 16 01 7B 6E A3 E0 CD 81 DD 0B 96 1B 5F B8
9E C2 72 DE 0D 4B 57 91 0B 12 49 7E 2A 78 64 89
01 A3 A0 BA 98 AF AA 7F 6C 3D 50 2C AB 2E 17 CE
87 75 A6 69 98 84 96 2F 18 F1 6A 6F 1E 9A B8 F1
09 E1 1E 4F 8B C0 BA F8 D6 AC C5 9F 97 4F 14 DB
88 22 04 F7 BF 7A 42 A4 66 ED C5 81 AA FD 08 62
91 EB 95 EB AE 86 7A BE

Data to be absorbed

01 88 02 01 00 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 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 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)

27 D2 F2 F1 3D A7 3B 01 84 42 EF 4F E2 45 86 19
87 D1 C5 16 CD 39 16 BE C1 1B 9F 8B 1F FE 2B 19
DA 59 C7 EC CA AD 43 43 34 C2 56 51 3C ED 8F D5
B6 54 F6 D6 F2 5E 89 8E 2B 77 A0 18 BF DB 42 2C
3F A9 D4 16 88 24 60 AD 8F C6 B3 9F 0D 67 17 F0
A5 68 95 D4 B2 D5 A8 84 3F D7 BD AD 17 EE 38 11
FD DD 16 01 7B 6E A3 E0 CD 81 DD 0B 96 1B 5F B8
9E C2 72 DE 0D 4B 57 91 0B 12 49 7E 2A 78 64 89
01 A3 A0 BA 98 AF AA 7F 6C 3D 50 2C AB 2E 17 CE
87 75 A6 69 98 84 96 2F 18 F1 6A 6F 1E 9A B8 F1
09 E1 1E 4F 8B C0 BA F8 D6 AC C5 9F 97 4F 14 DB
88 22 04 F7 BF 7A 42 A4 66 ED C5 81 AA FD 08 62
91 EB 95 EB AE 86 7A BE

After Permutation

41 28 71 21 36 7D F6 F0 6E 72 B3 7B 8B 67 35 D7
D2 A7 67 BC CB 25 76 47 AE 2C CE 70 EE F6 10 6E
CC 48 5E 74 54 C7 83 D8 CD 24 50 BD 01 09 8E 1F
A2 45 FA DF 06 C2 B6 67 2D 85 8C 8A 9D 15 5E 7E
50 9C 75 F9 16 B3 8F 4D 77 D6 D7 E6 A6 8B 41 B6
5D D5 78 DA A6 FB 1C 91 2B 6F D9 94 54 04 B5 B0
32 B5 D1 0F 2B B1 97 95 BC 50 4D 35 E8 74 3D 5B
CC 74 66 DA 1C 41 DB 8F 59 81 FC 7F A8 DD 18 D4
F3 1E 97 59 54 45 0D 0E 62 85 D6 BF 02 DD 0C E0
D1 5D 94 7A F0 5F DD 2A 25 56 04 D2 F6 46 44 FF
9F FB B1 A0 BB 81 AC CD C2 23 6B C4 27 82 7D 47
AF 7A 45 1B A8 83 6A 4F 6D FB D7 25 DF 6A 47 0C
30 F7 6D 3D DD CD 86 D2

about to call last of the absorb phase

About to Absorb data

State (in bytes)

41 28 71 21 36 7D F6 F0 6E 72 B3 7B 8B 67 35 D7
D2 A7 67 BC CB 25 76 47 AE 2C CE 70 EE F6 10 6E
CC 48 5E 74 54 C7 83 D8 CD 24 50 BD 01 09 8E 1F
A2 45 FA DF 06 C2 B6 67 2D 85 8C 8A 9D 15 5E 7E
50 9C 75 F9 16 B3 8F 4D 77 D6 D7 E6 A6 8B 41 B6

5D D5 78 DA A6 FB 1C 91 2B 6F D9 94 54 04 B5 B0
32 B5 D1 0F 2B B1 97 95 BC 50 4D 35 E8 74 3D 5B
CC 74 66 DA 1C 41 DB 8F 59 81 FC 7F A8 DD 18 D4
F3 1E 97 59 54 45 0D 0E 62 85 D6 BF 02 DD 0C E0
D1 5D 94 7A F0 5F DD 2A 25 56 04 D2 F6 46 44 FF
9F FB B1 A0 BB 81 AC CD C2 23 6B C4 27 82 7D 47
AF 7A 45 1B A8 83 6A 4F 6D FB D7 25 DF 6A 47 0C
30 F7 6D 3D DD CD 86 D2

Data to be absorbed

00 01 02 03 02 00 02 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 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 00 00 00 00

Xor'd state (in bytes)

41 29 73 22 34 7D F4 F4 6E 72 B3 7B 8B 67 35 D7
D2 A7 67 BC CB 25 76 47 AE 2C CE 70 EE F6 10 6E
CC 48 5E 74 54 C7 83 D8 CD 24 50 BD 01 09 8E 1F
A2 45 FA DF 06 C2 B6 67 2D 85 8C 8A 9D 15 5E 7E
50 9C 75 F9 16 B3 8F 4D 77 D6 D7 E6 A6 8B 41 B6
5D D5 78 DA A6 FB 1C 91 2B 6F D9 94 54 04 B5 B0
32 B5 D1 0F 2B B1 97 95 BC 50 4D 35 E8 74 3D 5B
CC 74 66 DA 1C 41 DB 8F 59 81 FC 7F A8 DD 18 D4
F3 1E 97 59 54 45 0D 8E 62 85 D6 BF 02 DD 0C E0
D1 5D 94 7A F0 5F DD 2A 25 56 04 D2 F6 46 44 FF
9F FB B1 A0 BB 81 AC CD C2 23 6B C4 27 82 7D 47
AF 7A 45 1B A8 83 6A 4F 6D FB D7 25 DF 6A 47 0C
30 F7 6D 3D DD CD 86 D2

After Permutation

20 C5 70 C3 13 46 F7 03 C9 AC 36 C6 1C 03 CB 64
C3 97 0D 0C FC 78 7E 9B 79 59 9D 27 3A 68 D2 F7
F6 9D 4C C3 DE 9D 10 4A 35 16 89 F2 7C F6 F5 95
1F 01 03 F3 3F 4F 24 87 10 24 D9 C2 77 73 A8 DD
92 8C 9A 0A BF 3F 40 9A 6C C9 DD D0 A3 A3 E0 B1
AD 9B B6 BF A8 2E 6B 99 82 13 1B B9 7D D8 A7 7F
99 D1 C9 78 A8 62 65 7E 90 10 50 85 2B 3C DF D5
0A 71 C7 C7 49 62 57 B8 67 C2 99 46 37 3B 51 6E
10 03 3D E7 D2 82 DA FF F9 AE 73 0D 70 4C 99 10
5B 28 69 94 B2 03 5B 96 45 12 5F 9D DC 64 43 C7
DB B1 A4 DD 6E C5 EC 01 F4 09 4C BC 5E 89 2B CC
D2 A1 F5 75 78 1C C6 75 3F 02 B3 27 72 24 4B 93
F6 D0 A7 4E 14 2F 14 F2

Output is

20 C5 70 C3 13 46 F7 03 C9 AC 36 C6 1C 03 CB 64
C3 97 0D 0C FC 78 7E 9B 79 59 9D 27 3A 68 D2 F7
F6 9D 4C C3 DE 9D 10 4A 35 16 89 F2 7C F6 F5 95
1F 01 03 F3 3F 4F 24 87 10 24 D9 C2 77 73 A8 DD

=====

KMAC:

Sample #5

Security Strength: 256-bits

Length of Key is 256-bits

Key is

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

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

S (as a character string) is

"(null)"

Encoded K

02 01 00 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

byte_padded stuff

01 88 02 01 00 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 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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

Right_encoded L

02 00 02

Encoded N

01 20 4B 4D 41 43

Encoded S

01 00

bytepad data

01 88 01 20 4B 4D 41 43 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Data to be absorbed

01 88 01 20 4B 4D 41 43 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 20 4B 4D 41 43 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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

6C 1C 95 F8 7B 03 63 5D 35 EC DA C6 7F 3D 5E 13
45 90 57 76 63 80 73 29 35 23 5E 7A C8 74 BC 4E
13 C9 2A 02 67 E6 A0 A4 90 1C 71 9B 41 46 81 36
D4 54 A2 12 B1 67 E9 8D 23 48 B7 8E 95 7D BB 2D
78 82 46 B7 20 3C D0 BE 03 A0 F3 C0 A8 C0 94 06
0E A8 7F E8 65 FC 40 64 FD 58 EB 0C DA 5A F3 E5
F7 0C 2D 8E 84 E0 87 3B 1C 77 A0 C5 1F 18 2A 7B
7D D5 9A B1 C0 23 17 76 04 71 F6 4E 5A DC BA AC
29 2F 30 AF 18 51 21 7A 0A 14 DD 16 EE D1 94 EB
BD 4F 49 1E BF 33 1F B4 3E 4B 0B 83 0C 77 67 F4
54 B5 00 FA C7 E5 0D 91 5B 42 46 52 17 5C EC 6B
64 18 D6 CF F1 DE CF 38 C6 D8 CB 11 30 A9 E4 29
C6 86 CD 5F 82 0C 80 07

About to Absorb data
State (in bytes)

6C 1C 95 F8 7B 03 63 5D 35 EC DA C6 7F 3D 5E 13
45 90 57 76 63 80 73 29 35 23 5E 7A C8 74 BC 4E
13 C9 2A 02 67 E6 A0 A4 90 1C 71 9B 41 46 81 36
D4 54 A2 12 B1 67 E9 8D 23 48 B7 8E 95 7D BB 2D
78 82 46 B7 20 3C D0 BE 03 A0 F3 C0 A8 C0 94 06
0E A8 7F E8 65 FC 40 64 FD 58 EB 0C DA 5A F3 E5
F7 0C 2D 8E 84 E0 87 3B 1C 77 A0 C5 1F 18 2A 7B
7D D5 9A B1 C0 23 17 76 04 71 F6 4E 5A DC BA AC
29 2F 30 AF 18 51 21 7A 0A 14 DD 16 EE D1 94 EB
BD 4F 49 1E BF 33 1F B4 3E 4B 0B 83 0C 77 67 F4
54 B5 00 FA C7 E5 0D 91 5B 42 46 52 17 5C EC 6B
64 18 D6 CF F1 DE CF 38 C6 D8 CB 11 30 A9 E4 29
C6 86 CD 5F 82 0C 80 07

Data to be absorbed

01 88 02 01 00 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 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)

6D 94 97 F9 7B 43 22 1F 76 A8 9F 80 38 75 17 59
0E DC 1A 38 2C D0 22 7B 66 77 0B 2C 9F 2C E5 14
48 95 77 5C 38 E6 A0 A4 90 1C 71 9B 41 46 81 36
D4 54 A2 12 B1 67 E9 8D 23 48 B7 8E 95 7D BB 2D
78 82 46 B7 20 3C D0 BE 03 A0 F3 C0 A8 C0 94 06
0E A8 7F E8 65 FC 40 64 FD 58 EB 0C DA 5A F3 E5
F7 0C 2D 8E 84 E0 87 3B 1C 77 A0 C5 1F 18 2A 7B
7D D5 9A B1 C0 23 17 76 04 71 F6 4E 5A DC BA AC
29 2F 30 AF 18 51 21 7A 0A 14 DD 16 EE D1 94 EB
BD 4F 49 1E BF 33 1F B4 3E 4B 0B 83 0C 77 67 F4
54 B5 00 FA C7 E5 0D 91 5B 42 46 52 17 5C EC 6B
64 18 D6 CF F1 DE CF 38 C6 D8 CB 11 30 A9 E4 29
C6 86 CD 5F 82 0C 80 07

After Permutation

EF 7D A7 22 E7 C0 6A 5E 08 BF AE CA 44 CF 88 09
20 5C E7 40 CC 1F B0 B2 40 02 BA 05 ED BD 4D 6D
74 E1 EB DA FD DB A4 AA 71 DA 7D B5 4E 11 3B FA
2B 65 7B 9C B8 B5 BA A8 50 E3 66 54 F3 D3 20 03
0D AF E7 25 06 EF 5B 1F 46 93 57 D7 41 4F B3 98
E0 93 93 1F 49 8D 66 AE F7 FF 8B 87 14 6F CF F1
CB A0 ED 89 CD B3 5B 99 2A C3 32 17 6D 85 0F 8F
49 36 AA E6 56 64 F2 23 7F D4 A4 91 FB 83 88 A3
88 2F 92 5B D7 6C E6 0B AF 2C 5E 32 CE F0 64 0F
B2 85 C9 DA 1B 17 5A 9F C9 BB C5 07 DC EC 7C 20
CB 5D 2E FB 97 A9 F5 F6 56 14 E8 CD 55 42 E0 6C
06 07 39 44 D2 2D 71 F5 EE 75 F0 BF 3B D1 A9 9C
D3 B6 48 C1 57 DE 1A 49

About to Absorb data

State (in bytes)

EF 7D A7 22 E7 C0 6A 5E 08 BF AE CA 44 CF 88 09
20 5C E7 40 CC 1F B0 B2 40 02 BA 05 ED BD 4D 6D
74 E1 EB DA FD DB A4 AA 71 DA 7D B5 4E 11 3B FA
2B 65 7B 9C B8 B5 BA A8 50 E3 66 54 F3 D3 20 03
0D AF E7 25 06 EF 5B 1F 46 93 57 D7 41 4F B3 98
E0 93 93 1F 49 8D 66 AE F7 FF 8B 87 14 6F CF F1
CB A0 ED 89 CD B3 5B 99 2A C3 32 17 6D 85 0F 8F
49 36 AA E6 56 64 F2 23 7F D4 A4 91 FB 83 88 A3
88 2F 92 5B D7 6C E6 0B AF 2C 5E 32 CE F0 64 0F
B2 85 C9 DA 1B 17 5A 9F C9 BB C5 07 DC EC 7C 20
CB 5D 2E FB 97 A9 F5 F6 56 14 E8 CD 55 42 E0 6C
06 07 39 44 D2 2D 71 F5 EE 75 F0 BF 3B D1 A9 9C
D3 B6 48 C1 57 DE 1A 49

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 7C A5 21 E3 C5 6C 59 00 B6 A4 C1 48 C2 86 06
30 4D F5 53 D8 0A A6 A5 58 1B A0 1E F1 A0 53 72
54 C0 C9 F9 D9 FE 82 8D 59 F3 57 9E 62 3C 15 D5
1B 54 49 AF 8C 80 8C 9F 68 DA 5C 6F CF EE 1E 3C
4D EE A5 66 42 AA 1D 58 0E DA 1D 9C 0D 02 FD D7
B0 C2 C1 4C 1D D8 30 F9 AF A6 D1 DC 48 32 91 AE
AB C1 8F EA A9 D6 3D FE 42 AA 58 7C 01 E8 61 E0
39 47 D8 95 22 11 84 54 07 AD DE EA 87 FE F6 DC
08 AE 10 D8 53 E9 60 8C AF 2C 5E 32 CE F0 64 0F
B2 85 C9 DA 1B 17 5A 9F C9 BB C5 07 DC EC 7C 20
CB 5D 2E FB 97 A9 F5 F6 56 14 E8 CD 55 42 E0 6C
06 07 39 44 D2 2D 71 F5 EE 75 F0 BF 3B D1 A9 9C
D3 B6 48 C1 57 DE 1A 49

After Permutation

E0 AB D9 46 3A AA 82 2B A5 3A 0F CC D4 43 58 F9
EC 13 45 A5 73 26 D7 A8 E6 8C F2 E7 78 EB 09 ED
E3 82 5A D2 77 25 E1 A0 85 C4 83 D6 48 B4 4D F0
13 EF D4 0D 99 C4 0D 8E 0E A7 8A 02 BF 32 C7 11
26 B0 E6 5A 5A 8F BF 95 B0 A2 82 C8 E4 BB 5D 7A
39 36 E7 0A 78 D0 E7 54 8A 58 25 DA FE 97 4B 19
DF 53 1E 08 C6 CF 0C 98 F4 3B BA 96 3B 39 CB 1C
00 1F DA A4 7B 43 C7 46 FD 12 FA 2A 82 AA 27 9C
25 B8 E0 4E 6D B8 A5 76 DD 00 0D 75 B3 47 1B A0
92 46 8D 34 5E A0 18 97 C1 19 A7 E3 28 FE 7E D6
93 8F 3A C8 86 1A 67 5F 46 7A 50 B7 8F 56 79 37
80 FF 3F B7 26 6A C2 75 B8 FA 26 BB 81 5B 4D 59
00 6B 82 DA 70 BE 4E F9

about to call last of the absorb phase

About to Absorb data

State (in bytes)

E0 AB D9 46 3A AA 82 2B A5 3A 0F CC D4 43 58 F9
EC 13 45 A5 73 26 D7 A8 E6 8C F2 E7 78 EB 09 ED
E3 82 5A D2 77 25 E1 A0 85 C4 83 D6 48 B4 4D F0
13 EF D4 0D 99 C4 0D 8E 0E A7 8A 02 BF 32 C7 11
26 B0 E6 5A 5A 8F BF 95 B0 A2 82 C8 E4 BB 5D 7A

39 36 E7 0A 78 D0 E7 54 8A 58 25 DA FE 97 4B 19
DF 53 1E 08 C6 CF 0C 98 F4 3B BA 96 3B 39 CB 1C
00 1F DA A4 7B 43 C7 46 FD 12 FA 2A 82 AA 27 9C
25 B8 E0 4E 6D B8 A5 76 DD 00 0D 75 B3 47 1B A0
92 46 8D 34 5E A0 18 97 C1 19 A7 E3 28 FE 7E D6
93 8F 3A C8 86 1A 67 5F 46 7A 50 B7 8F 56 79 37
80 FF 3F B7 26 6A C2 75 B8 FA 26 BB 81 5B 4D 59
00 6B 82 DA 70 BE 4E F9

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
02 00 02 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 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 00 00 00 00

Xor'd state (in bytes)

68 22 53 CD B6 27 0C A4 35 AB 9D 5F 40 D6 CE 6E
74 8A DF 3E EF BB 49 37 46 2D 50 44 DC 4E AF 4A
4B 2B F0 79 DB 88 4F 0F 35 75 31 65 FC 01 FB 47
AB 56 6E B6 25 79 B3 31 CE 66 48 C1 7B F7 01 D6
24 B0 E4 5E 5A 8F BF 95 B0 A2 82 C8 E4 BB 5D 7A
39 36 E7 0A 78 D0 E7 54 8A 58 25 DA FE 97 4B 19
DF 53 1E 08 C6 CF 0C 98 F4 3B BA 96 3B 39 CB 1C
00 1F DA A4 7B 43 C7 46 FD 12 FA 2A 82 AA 27 9C
25 B8 E0 4E 6D B8 A5 F6 DD 00 0D 75 B3 47 1B A0
92 46 8D 34 5E A0 18 97 C1 19 A7 E3 28 FE 7E D6
93 8F 3A C8 86 1A 67 5F 46 7A 50 B7 8F 56 79 37
80 FF 3F B7 26 6A C2 75 B8 FA 26 BB 81 5B 4D 59
00 6B 82 DA 70 BE 4E F9

After Permutation

75 35 8C F3 9E 41 49 4E 94 97 07 92 7C EE 0A F2
0A 3F F5 53 90 4C 86 B0 8F 21 CC 41 4B CF D6 91
58 9D 27 CF 5E 15 36 9C BB FF 8B 9A 4C 2E B1 78
00 85 5D 02 35 FF 63 5D A8 25 33 EC 6B 75 9B 69
DE 8D 34 BE 57 F8 A6 53 7F B1 98 8F 10 FA F6 89
C4 64 8A EE 37 D9 AC F7 80 D5 15 3E 24 BD 73 E6
1A 8F 6A CC AA 19 07 F4 17 CC 76 90 92 D7 AD 60
CF 12 EC 3B 49 E8 6D FD F0 89 86 8C 73 E9 7C 47
A9 29 79 95 96 CE DD E7 7C 0E 45 25 93 DB 3A 81
D5 16 9A 04 20 26 6F 40 49 07 DE AB 33 EE F7 9E
88 58 A8 EF AF 5E 58 14 26 79 75 7D 52 8D 46 36
CA 87 F9 48 E5 BA BF 48 2E E7 FE 8F BE FC 51 B8
10 9C 43 EF 63 77 0B 1A

Output is

75 35 8C F3 9E 41 49 4E 94 97 07 92 7C EE 0A F2
0A 3F F5 53 90 4C 86 B0 8F 21 CC 41 4B CF D6 91
58 9D 27 CF 5E 15 36 9C BB FF 8B 9A 4C 2E B1 78
00 85 5D 02 35 FF 63 5D A8 25 33 EC 6B 75 9B 69

=====

KMAC:

Sample #6

Security Strength: 256-bits

Length of Key is 256-bits

Key is

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

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

S (as a character string) is

"My Tagged Application"

Encoded K

02 01 00 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

byte_padded stuff

01 88 02 01 00 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 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

67 65 64 20 41 70 70 6C 69 63 61 74 69 6F 6E 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 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

26 5A F0 F0 3D E7 7A 43 C7 06 AA 09 A5 0D CF 53
CC 9D 88 58 82 69 47 EC 92 4F CA DD 48 A6 72 43
81 05 9A B2 95 AD 43 43 34 C2 56 51 3C ED 8F D5
B6 54 F6 D6 F2 5E 89 8E 2B 77 A0 18 BF DB 42 2C
3F A9 D4 16 88 24 60 AD 8F C6 B3 9F 0D 67 17 F0
A5 68 95 D4 B2 D5 A8 84 3F D7 BD AD 17 EE 38 11
FD DD 16 01 7B 6E A3 E0 CD 81 DD 0B 96 1B 5F B8
9E C2 72 DE 0D 4B 57 91 0B 12 49 7E 2A 78 64 89
01 A3 A0 BA 98 AF AA 7F 6C 3D 50 2C AB 2E 17 CE
87 75 A6 69 98 84 96 2F 18 F1 6A 6F 1E 9A B8 F1
09 E1 1E 4F 8B C0 BA F8 D6 AC C5 9F 97 4F 14 DB
88 22 04 F7 BF 7A 42 A4 66 ED C5 81 AA FD 08 62
91 EB 95 EB AE 86 7A BE

About to Absorb data

State (in bytes)

26 5A F0 F0 3D E7 7A 43 C7 06 AA 09 A5 0D CF 53
CC 9D 88 58 82 69 47 EC 92 4F CA DD 48 A6 72 43
81 05 9A B2 95 AD 43 43 34 C2 56 51 3C ED 8F D5
B6 54 F6 D6 F2 5E 89 8E 2B 77 A0 18 BF DB 42 2C
3F A9 D4 16 88 24 60 AD 8F C6 B3 9F 0D 67 17 F0
A5 68 95 D4 B2 D5 A8 84 3F D7 BD AD 17 EE 38 11
FD DD 16 01 7B 6E A3 E0 CD 81 DD 0B 96 1B 5F B8
9E C2 72 DE 0D 4B 57 91 0B 12 49 7E 2A 78 64 89
01 A3 A0 BA 98 AF AA 7F 6C 3D 50 2C AB 2E 17 CE
87 75 A6 69 98 84 96 2F 18 F1 6A 6F 1E 9A B8 F1
09 E1 1E 4F 8B C0 BA F8 D6 AC C5 9F 97 4F 14 DB
88 22 04 F7 BF 7A 42 A4 66 ED C5 81 AA FD 08 62
91 EB 95 EB AE 86 7A BE

Data to be absorbed

01 88 02 01 00 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 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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)

27 D2 F2 F1 3D A7 3B 01 84 42 EF 4F E2 45 86 19
87 D1 C5 16 CD 39 16 BE C1 1B 9F 8B 1F FE 2B 19
DA 59 C7 EC CA AD 43 43 34 C2 56 51 3C ED 8F D5
B6 54 F6 D6 F2 5E 89 8E 2B 77 A0 18 BF DB 42 2C
3F A9 D4 16 88 24 60 AD 8F C6 B3 9F 0D 67 17 F0
A5 68 95 D4 B2 D5 A8 84 3F D7 BD AD 17 EE 38 11
FD DD 16 01 7B 6E A3 E0 CD 81 DD 0B 96 1B 5F B8
9E C2 72 DE 0D 4B 57 91 0B 12 49 7E 2A 78 64 89
01 A3 A0 BA 98 AF AA 7F 6C 3D 50 2C AB 2E 17 CE
87 75 A6 69 98 84 96 2F 18 F1 6A 6F 1E 9A B8 F1
09 E1 1E 4F 8B C0 BA F8 D6 AC C5 9F 97 4F 14 DB
88 22 04 F7 BF 7A 42 A4 66 ED C5 81 AA FD 08 62
91 EB 95 EB AE 86 7A BE

After Permutation

41 28 71 21 36 7D F6 F0 6E 72 B3 7B 8B 67 35 D7
D2 A7 67 BC CB 25 76 47 AE 2C CE 70 EE F6 10 6E
CC 48 5E 74 54 C7 83 D8 CD 24 50 BD 01 09 8E 1F
A2 45 FA DF 06 C2 B6 67 2D 85 8C 8A 9D 15 5E 7E
50 9C 75 F9 16 B3 8F 4D 77 D6 D7 E6 A6 8B 41 B6
5D D5 78 DA A6 FB 1C 91 2B 6F D9 94 54 04 B5 B0
32 B5 D1 0F 2B B1 97 95 BC 50 4D 35 E8 74 3D 5B
CC 74 66 DA 1C 41 DB 8F 59 81 FC 7F A8 DD 18 D4
F3 1E 97 59 54 45 0D 0E 62 85 D6 BF 02 DD 0C E0
D1 5D 94 7A F0 5F DD 2A 25 56 04 D2 F6 46 44 FF
9F FB B1 A0 BB 81 AC CD C2 23 6B C4 27 82 7D 47
AF 7A 45 1B A8 83 6A 4F 6D FB D7 25 DF 6A 47 0C
30 F7 6D 3D DD CD 86 D2

About to Absorb data

State (in bytes)

41 28 71 21 36 7D F6 F0 6E 72 B3 7B 8B 67 35 D7
D2 A7 67 BC CB 25 76 47 AE 2C CE 70 EE F6 10 6E
CC 48 5E 74 54 C7 83 D8 CD 24 50 BD 01 09 8E 1F
A2 45 FA DF 06 C2 B6 67 2D 85 8C 8A 9D 15 5E 7E
50 9C 75 F9 16 B3 8F 4D 77 D6 D7 E6 A6 8B 41 B6
5D D5 78 DA A6 FB 1C 91 2B 6F D9 94 54 04 B5 B0
32 B5 D1 0F 2B B1 97 95 BC 50 4D 35 E8 74 3D 5B
CC 74 66 DA 1C 41 DB 8F 59 81 FC 7F A8 DD 18 D4
F3 1E 97 59 54 45 0D 0E 62 85 D6 BF 02 DD 0C E0
D1 5D 94 7A F0 5F DD 2A 25 56 04 D2 F6 46 44 FF
9F FB B1 A0 BB 81 AC CD C2 23 6B C4 27 82 7D 47
AF 7A 45 1B A8 83 6A 4F 6D FB D7 25 DF 6A 47 0C
30 F7 6D 3D DD CD 86 D2

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)

41 29 73 22 32 78 F0 F7 66 7B B9 70 87 6A 3B D8
C2 B6 75 AF DF 30 60 50 B6 35 D4 6B F2 EB 0E 71
EC 69 7C 57 70 E2 A5 FF E5 0D 7A 96 2D 24 A0 30
92 74 C8 EC 32 F7 80 50 15 BC B6 B1 A1 28 60 41
10 DD 37 BA 52 F6 C9 0A 3F 9F 9D AD EA C6 0F F9
0D 84 2A 89 F2 AE 4A C6 73 36 83 CF 08 59 EB EF
52 D4 B3 6C 4F D4 F1 F2 D4 39 27 5E 84 19 53 34
BC 05 14 A9 68 34 AD F8 21 F8 86 04 D4 A0 66 AB
73 9F 15 DA D0 C0 8B 89 62 85 D6 BF 02 DD 0C E0
D1 5D 94 7A F0 5F DD 2A 25 56 04 D2 F6 46 44 FF
9F FB B1 A0 BB 81 AC CD C2 23 6B C4 27 82 7D 47
AF 7A 45 1B A8 83 6A 4F 6D FB D7 25 DF 6A 47 0C
30 F7 6D 3D DD CD 86 D2

After Permutation

B6 99 D6 5D 2B 77 4A C0 C0 57 A5 23 6B 33 8D ED
16 39 32 94 FF 85 3A FA 8C 68 74 45 84 59 7F C9
E5 9A 26 E4 46 13 97 64 45 D2 E2 5A FC 21 E8 DA
CF 2D 91 BC A0 BA 73 A6 05 5A 28 99 A7 99 63 73
98 DB 17 B2 E9 3D C4 F6 F3 4C 36 2B C9 1A 95 6C
84 CB 84 5F F7 0D 97 44 39 0B 87 9F FB ED CE B9
10 AB B2 B2 B4 26 85 1C 31 CF 12 19 B1 82 EC 28
FF 58 CA 34 73 E5 A1 D3 F0 5E EE 98 FF 26 7A 3B
1B 99 6F C6 0B 85 F3 1C E4 F4 F5 4A 34 D7 A9 6F
2E FB 06 34 D3 68 C4 44 C0 C1 B7 A6 48 96 78 B6
B9 3C 24 28 1A 79 96 5B 98 A0 7D 1B 2C DE 26 C5
AD 39 E4 4D 43 C6 38 40 67 84 BE 3F 98 9D 68 A3
09 8F 26 8C 5F D6 30 7B

about to call last of the absorb phase

About to Absorb data

State (in bytes)

B6 99 D6 5D 2B 77 4A C0 C0 57 A5 23 6B 33 8D ED
16 39 32 94 FF 85 3A FA 8C 68 74 45 84 59 7F C9
E5 9A 26 E4 46 13 97 64 45 D2 E2 5A FC 21 E8 DA
CF 2D 91 BC A0 BA 73 A6 05 5A 28 99 A7 99 63 73

98 DB 17 B2 E9 3D C4 F6 F3 4C 36 2B C9 1A 95 6C
84 CB 84 5F F7 0D 97 44 39 0B 87 9F FB ED CE B9
10 AB B2 B2 B4 26 85 1C 31 CF 12 19 B1 82 EC 28
FF 58 CA 34 73 E5 A1 D3 F0 5E EE 98 FF 26 7A 3B
1B 99 6F C6 0B 85 F3 1C E4 F4 F5 4A 34 D7 A9 6F
2E FB 06 34 D3 68 C4 44 C0 C1 B7 A6 48 96 78 B6
B9 3C 24 28 1A 79 96 5B 98 A0 7D 1B 2C DE 26 C5
AD 39 E4 4D 43 C6 38 40 67 84 BE 3F 98 9D 68 A3
09 8F 26 8C 5F D6 30 7B

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
02 00 02 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 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

Xor'd state (in bytes)

3E 10 5C D6 A7 FA C4 4F 50 C6 37 B0 FF A6 1B 7A
8E A0 A8 0F 63 18 A4 65 2C C9 D6 E6 20 FC D9 6E
4D 33 8C 4F EA BE 39 CB F5 63 50 E9 48 94 5E 6D
77 94 2B 07 1C 07 CD 19 C5 9B EA 5A 63 5C A5 B4
9A DB 15 B6 E9 3D C4 F6 F3 4C 36 2B C9 1A 95 6C
84 CB 84 5F F7 0D 97 44 39 0B 87 9F FB ED CE B9
10 AB B2 B2 B4 26 85 1C 31 CF 12 19 B1 82 EC 28
FF 58 CA 34 73 E5 A1 D3 F0 5E EE 98 FF 26 7A 3B
1B 99 6F C6 0B 85 F3 9C E4 F4 F5 4A 34 D7 A9 6F
2E FB 06 34 D3 68 C4 44 C0 C1 B7 A6 48 96 78 B6
B9 3C 24 28 1A 79 96 5B 98 A0 7D 1B 2C DE 26 C5
AD 39 E4 4D 43 C6 38 40 67 84 BE 3F 98 9D 68 A3
09 8F 26 8C 5F D6 30 7B

After Permutation

B5 86 18 F7 1F 92 E1 D5 6C 1B 8C 55 DD D7 CD 18
8B 97 B4 CA 4D 99 83 1E B2 69 9A 83 7D A2 E4 D9
70 FB AC FD E5 00 33 AE A5 85 F1 A2 70 85 10 C3
2D 07 88 08 01 BD 18 28 98 FE 47 68 76 FC 89 65
FE 70 F6 F5 14 88 18 89 22 A6 3E F6 5D F5 9D 0B
43 8B 8E 52 35 27 F5 1B 0D 04 DA BC 95 A4 5E 36
6B 78 9B 54 31 05 5E 3A 51 4D FD 3F D9 4C 26 FE
9D 74 FE 7F 6B AE 8F C7 E7 CA 4D 12 FD AE 2D 4C
73 B8 FF 1F 7D C2 02 12 34 78 44 FE 73 B5 2C FA
B8 72 3B FC 63 E6 30 B2 EE 57 DE 29 B9 2D B6 D1
52 B9 CC E5 B5 25 49 B1 3A 55 54 B2 B5 E0 D6 70
64 77 71 24 81 72 F0 D5 0F AD 70 89 1B C6 99 0B

6D B2 51 75 AD D2 E2 8E

Output is

B5 86 18 F7 1F 92 E1 D5 6C 1B 8C 55 DD D7 CD 18
8B 97 B4 CA 4D 99 83 1E B2 69 9A 83 7D A2 E4 D9
70 FB AC FD E5 00 33 AE A5 85 F1 A2 70 85 10 C3
2D 07 88 08 01 BD 18 28 98 FE 47 68 76 FC 89 65

