

#####

Block Cipher Modes of Operation

CMAC Mode for Authentication (CMAC)

#####

CMAC-TDES (Generation)

Key1 is

01234567 89ABCDEF

Key2 is

23456789 ABCDEF01

Key3 is

456789AB CDEF0123

=====

Sample #1

Plaintext is

<empty>

Tag length = 8

Full Blocks

L 4EBA739C 998BCB60

Last Block

K2: 3AE9CE72 662F2D9B

Block #0

inBlock = BAE9CE72 662F2D9B

outBlock = 7DB0D37D F936C550

Tag is

7DB0D37D F936C550

Sample #2

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

Tag length = 8

Full Blocks

L 4EBA739C 998BCB60

Block #1

inBlock = 6BC1BEE2 2E409F96

outBlock = 714772F3 39841D34

Last Block

K1: 9D74E739 331796C0

Block #2

inBlock = 050EEBDB 79009CDE

outBlock = 30239CF1 F52E6609

Tag is

30239CF1 F52E6609

Sample #3

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

AE2D8A57

Tag length = 8

Full Blocks

L 4EBA739C 998BCB60

Block #1

inBlock = 6BC1BEE2 2E409F96
outBlock = 714772F3 39841D34

Block #2

inBlock = 987A0CE2 4A170A1E
outBlock = A6668756 9156F45A

Last Block

K2: 3AE9CE72 662F2D9B

Block #3

inBlock = 32A2C373 7779D9C1
outBlock = 6C9F3EE4 923F6BE2

Tag is

6C9F3EE4 923F6BE2

=====

Sample #4

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51

Tag length = 8

Full Blocks

L 4EBA739C 998BCB60

Block #1

inBlock = 6BC1BEE2 2E409F96
outBlock = 714772F3 39841D34

Block #2
inBlock = 987A0CE2 4A170A1E
outBlock = A6668756 9156F45A

Block #3
inBlock = 084B0D01 8F5558C6
outBlock = 6D6A8D86 6556D349

Last Block

K1: 9D74E739 331796C0

Block #4
inBlock = 6EA90513 13EECBD8
outBlock = 99429BD0 BF7904E5

Tag is
99429BD0 BF7904E5

=====

#####

Block Cipher Modes of Operation

CMAC Mode for Authentication (CMAC)

#####

CMAC-TDES (Generation)

Key1 is
01234567 89ABCDEF
Key2 is
23456789 ABCDEF01
Key3 is
01234567 89ABCDEF

=====

Sample #1

Plaintext is

<empty>

Tag length = 8

Full Blocks

L 86E965BD 1EC44461

Last Block

K2: 1BA596F4 7B1111B2

Block #0

inBlock = 9BA596F4 7B1111B2

outBlock = 79CE52A7 F786A960

Tag is

79CE52A7 F786A960

=====

Sample #2

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

Tag length = 8

Full Blocks

L 86E965BD 1EC44461

Block #1

inBlock = 6BC1BEE2 2E409F96

outBlock = 06EDE3D8 2884090A

Last Block

K1: 0DD2CB7A 3D8888D9

Block #2

inBlock = E20256B3 669F96F9

outBlock = CC18A0B7 9AF2413B

Tag is

CC18A0B7 9AF2413B

=====

Sample #3

Plaintext is

6BC1BEE2 2E409F96 E93D7E11 7393172A

AE2D8A57

Tag length = 8

Full Blocks

L 86E965BD 1EC44461

Block #1

inBlock = 6BC1BEE2 2E409F96

outBlock = 06EDE3D8 2884090A

Block #2

inBlock = EFD09DC9 5B171E20

outBlock = 3B7BBD1F C1AD476F

Last Block

K2: 1BA596F4 7B1111B2

Block #3

inBlock = 8EF3A1BC 3ABC56DD
outBlock = C06D377E CD101969

Tag is
C06D377E CD101969

=====

Sample #4

Plaintext is
6BC1BEE2 2E409F96 E93D7E11 7393172A
AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
Tag length = 8

Full Blocks

L 86E965BD 1EC44461

Block #1

inBlock = 6BC1BEE2 2E409F96
outBlock = 06EDE3D8 2884090A

Block #2

inBlock = EFD09DC9 5B171E20
outBlock = 3B7BBD1F C1AD476F

Block #3

inBlock = 95563748 DFAEEBF3
outBlock = 999E82F2 3BF0C275

Last Block

K1: 0DD2CB7A 3D8888D9

Block #4

inBlock = 0AFB2624 43D7C4FD
outBlock = 9CD33580 F9B64DFB

Tag is
9CD33580 F9B64DFB

=====