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

  Block Cipher Modes of Operation

      CMAC Mode for Authentication

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

CMAC-AES128
--------------------------------------------------------------

Example #1

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Mlen=0

PT is
    <empty>

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

Full Blocks

  L
    7DF76B0C 1AB899B3 3E42F047 B91B546F

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

Last Block

  K2:
    F7DDAC30 6AE266CC F90BC11E E46D513B

  Block #0
     inBlock =  77DDAC30 6AE266CC F90BC11E E46D513B
    outBlock =  BB1D6929 E9593728 7FA37D12 9B756746

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


Tag is
    BB1D6929 E9593728 7FA37D12 9B756746

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

```
Example #2

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Mlen=16

PT is
    6BC1BEE2 2E409F96 E93D7E11 7393172A

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

Full Blocks

  L
    7DF76B0C 1AB899B3 3E42F047 B91B546F

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

Last Block

  K1:
    FBEED618 35713366 7C85E08F 7236A8DE

  Block #1
     inBlock =  902F68FA 1B31ACF0 95B89E9E 01A5BFF4
    outBlock =  070A16B4 6B4D4144 F79BDD9D D04A287C

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


Tag is
    070A16B4 6B4D4144 F79BDD9D D04A287C

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

Example #3

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Mlen=20

PT is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
```

```
    AE2D8A57

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

Full Blocks

  L
    7DF76B0C 1AB899B3 3E42F047 B91B546F

  Block #1
     inBlock =  6BC1BEE2 2E409F96 E93D7E11 7393172A
    outBlock =  3AD77BB4 0D7A3660 A89ECAF3 2466EF97

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

Last Block

  K2:
    F7DDAC30 6AE266CC F90BC11E E46D513B

  Block #2
     inBlock =  63275DD3 E79850AC 51950BED C00BBEAC
    outBlock =  7D85449E A6EA19C8 23A7BF78 837DFADE

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


Tag is
    7D85449E A6EA19C8 23A7BF78 837DFADE

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

Example #4

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Mlen=64

PT is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

```
Full Blocks

  L
    7DF76B0C 1AB899B3 3E42F047 B91B546F

  Block #1
     inBlock =  6BC1BEE2 2E409F96 E93D7E11 7393172A
    outBlock =  3AD77BB4 0D7A3660 A89ECAF3 2466EF97

  Block #2
     inBlock =  94FAF1E3 13799AFC 3629A55F 61C961C6
    outBlock =  B148C17F 309EE692 287AE57C F12ADD49

  Block #3
     inBlock =  8180DD39 93C20283 CD812465 EB208FA6
    outBlock =  C93D11BF AF08C5DC 4D90B37B 4DEE002B

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

Last Block

  K1:
    FBEED618 35713366 7C85E08F 7236A8DE

  Block #4
     inBlock =  C44CE3E2 45366DAD 9C3E128F D9B49FE5
    outBlock =  51F0BEBF 7E3B9D92 FC497417 79363CFE

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


Tag is
    51F0BEBF 7E3B9D92 FC497417 79363CFE

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

**************************************************************

CMAC-AES192
--------------------------------------------------------------

Example #1

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
```

```
    62F8EAD2 522C6B7B

Mlen=0

PT is
    <empty>

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

Full Blocks

  L
    22452D8E 49A8A593 9F7321CE EA6D514B

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

Last Block

  K2:
    8914B639 26A2964E 7DCC873B A9B5452C

  Block #0
     inBlock =  0914B639 26A2964E 7DCC873B A9B5452C
    outBlock =  D17DDF46 ADAACDE5 31CAC483 DE7A9367

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


Tag is
    D17DDF46 ADAACDE5 31CAC483 DE7A9367

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

Example #2

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Mlen=16

PT is
    6BC1BEE2 2E409F96 E93D7E11 7393172A

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

```
Full Blocks

  L
    22452D8E 49A8A593 9F7321CE EA6D514B

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

Last Block

  K1:
    448A5B1C 93514B27 3EE6439D D4DAA296

  Block #1
     inBlock =  2F4BE5FE BD11D4B1 D7DB3D8C A749B5BC
    outBlock =  9E99A7BF 31E71090 0662F65E 617C5184

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


Tag is
    9E99A7BF 31E71090 0662F65E 617C5184

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

Example #3

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Mlen=20

PT is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57

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

Full Blocks

  L
    22452D8E 49A8A593 9F7321CE EA6D514B

  Block #1
     inBlock =  6BC1BEE2 2E409F96 E93D7E11 7393172A
    outBlock =  BD334F1D 6E45F25F F712A214 571FA5CC
```

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

Last Block

  K2:
    8914B639 26A2964E 7DCC873B A9B5452C

  Block #2
     inBlock =  9A0A7373 C8E76411 8ADE252F FEAAE0E0
    outBlock =  3D75C194 ED960704 44A9FA7E C740ECF8

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


Tag is
    3D75C194 ED960704 44A9FA7E C740ECF8

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

Example #4

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Mlen=64

PT is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

Full Blocks

  L
    22452D8E 49A8A593 9F7321CE EA6D514B

  Block #1
     inBlock =  6BC1BEE2 2E409F96 E93D7E11 7393172A
    outBlock =  BD334F1D 6E45F25F F712A214 571FA5CC

  Block #2
```

```
     inBlock =  131EC54A 70465EC3 69A5CDB8 12B02B9D
    outBlock =  0F771E2A 4F0FBE32 3CB4146A 0D1B86D9

  Block #3
     inBlock =  3FBF026C EC535A23 D94FD573 1711D436
    outBlock =  7A163DE1 BB451E2F 1B15CC1F 0B8C2B6D

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

Last Block

  K1:
    448A5B1C 93514B27 3EE6439D D4DAA296

  Block #4
     inBlock =  C80342B8 F75BCE1F 88D8CEF9 393ABEEB
    outBlock =  A1D5DF0E ED790F79 4D775896 59F39A11

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


Tag is
    A1D5DF0E ED790F79 4D775896 59F39A11

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

**************************************************************

CMAC-AES256
--------------------------------------------------------------

Example #1

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Mlen=0

PT is
    <empty>

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

Full Blocks
```

```
  L
    E568F681 94CF76D6 174D4CC0 4310A854

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

Last Block

  K2:
    95A3DA06 533DDB58 5D353301 0C42A0D9

  Block #0
     inBlock =  15A3DA06 533DDB58 5D353301 0C42A0D9
    outBlock =  028962F6 1B7BF89E FC6B551F 4667D983

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


Tag is
    028962F6 1B7BF89E FC6B551F 4667D983

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

Example #2

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Mlen=16

PT is
    6BC1BEE2 2E409F96 E93D7E11 7393172A

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

Full Blocks

  L
    E568F681 94CF76D6 174D4CC0 4310A854

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

Last Block

  K1:
    CAD1ED03 299EEDAC 2E9A9980 8621502F
```

```
  Block #1
     inBlock =  A11053E1 07DE723A C7A7E791 F5B24705
    outBlock =  28A7023F 452E8F82 BD4BF28D 8C37C35C

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

Tag is
    28A7023F 452E8F82 BD4BF28D 8C37C35C

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

Example #3

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Mlen=20

PT is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57

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

Full Blocks

  L
    E568F681 94CF76D6 174D4CC0 4310A854

  Block #1
     inBlock =  6BC1BEE2 2E409F96 E93D7E11 7393172A
    outBlock =  F3EED1BD B5D2A03C 064B5A7E 3DB181F8

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

Last Block

  K2:
    95A3DA06 533DDB58 5D353301 0C42A0D9

  Block #2
     inBlock =  C86081EC 66EF7B64 5B7E697F 31F32121
    outBlock =  156727DC 0878944A 023C1FE0 3BAD6D93
```

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


Tag is
    156727DC 0878944A 023C1FE0 3BAD6D93

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

Example #4

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Mlen=64

PT is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

Full Blocks

  L
    E568F681 94CF76D6 174D4CC0 4310A854

  Block #1
     inBlock =  6BC1BEE2 2E409F96 E93D7E11 7393172A
    outBlock =  F3EED1BD B5D2A03C 064B5A7E 3DB181F8

  Block #2
     inBlock =  5DC35BEA ABD10CA0 98FC35D2 781E0FA9
    outBlock =  E3C48B48 365CFB14 DC9AAA37 B1ABC15C

  Block #3
     inBlock =  D30C970E 95001F05 39616B2E ABA193B3
    outBlock =  8F6D7E85 D8A2CE79 C29FE1A4 D17E2F9F

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

Last Block
```

```
  K1:
    CAD1ED03 299EEDAC 2E9A9980 8621502F

  Block #4
     inBlock =  B323B7C3 2E73B8C2 412E395F B13348A0
    outBlock =  E1992190 549F6ED5 696A2C05 6C315410

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


Tag is
    E1992190 549F6ED5 696A2C05 6C315410

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

**************************************************************
```