The document contains a corrected version of Appendix D of Special Publication 800-38B, which specifies examples for the CMAC authentication mode. In particular, the values of the MAC, *T*, for Examples 14, 15, 18, and 19 have been corrected.

Appendix D: Examples

In this appendix, twenty examples are provided for the MAC generation process. The underlying block cipher is either the AES algorithm or TDEA. A block cipher key is fixed for each of the currently allowed key sizes, i.e., AES-128, AES-192, AES-256, two key TDEA, and three key TDEA. For each key, the generation of the associated subkeys is given, followed by four examples of MAC generation with the key. The messages in each set of examples are derived by truncating a common fixed string of 64 bytes.

All strings are represented in hexadecimal notation, with a space (or a new line) inserted every 8 symbols, for readability. As in the body of the Recommendation, *K1* and *K2* denote the subkeys, *M* denotes the message, and *T* denotes the MAC. For the AES algorithm examples, *Tlen* is 128, i.e., 32 hexadecimal symbols, and *K* denotes the key. For the TDEA examples, *Tlen* is 64, i.e., 16 hexadecimal symbols, and the key, *K*, is the ordered triple of strings, (*Key1*, *Key2*, *Key3*). For two key TDEA, *Key1* = *Key3*.

D.1 AES-128

For Examples 1–4 below, the block cipher is the AES algorithm with the following 128 bit key:

K	`2b7e1516 28aed2a6 abf71588 09cf4f3c`.

Subkey Generation

$\mathrm{CIPH}_K(0^{128})$	`7df76b0c 1ab899b3 3e42f047 b91b546f`
K1	`fbeed618 35713366 7c85e08f 7236a8de`
K2	`f7ddac30 6ae266cc f90bc11e e46d513b`

Example 1: *Mlen* 0

M	<empty string>
T	`bb1d6929 e9593728 7fa37d12 9b756746`

Example 2: *Mlen* = 128

M	`6bc1bee2 2e409f96 e93d7e11 7393172a`
T	`070a16b4 6b4d4144 f79bdd9d d04a287c`

Example 3: *Mlen* = 320

M	`6bc1bee2 2e409f96 e93d7e11 7393172a`
	`ae2d8a57 1e03ac9c 9eb76fac 45af8e51`
	`30c81c46 a35ce411`

T	`dfa66747 de9ae630 30ca3261 1497c827`

Example 4: *Mlen* = 512

M	`6bc1bee2 2e409f96 e93d7e11 7393172a`
	`ae2d8a57 1e03ac9c 9eb76fac 45af8e51`
	`30c81c46 a35ce411 e5fbc119 1a0a52ef`
	`f69f2445 df4f9b17 ad2b417b e66c3710`

T	`51f0bebf 7e3b9d92 fc497417 79363cfe`

D.2 AES-192

For Examples 5–8 below, the block cipher is the AES algorithm with the following 192 bit key:

K	`8e73b0f7 da0e6452 c810f32b 809079e5` `62f8ead2 522c6b7b`.

Subkey Generation

$\mathrm{CIPH}_K(0^{128})$	`22452d8e 49a8a593 9f7321ce ea6d514b`
K1	`448a5b1c 93514b27 3ee6439d d4daa296`
K2	`8914b639 26a2964e 7dcc873b a9b5452c`

Example 5: *Mlen* = 0

M	<empty string>
T	`d17ddf46 adaacde5 31cac483 de7a9367`

Example 6: *Mlen* = 128

M	`6bc1bee2 2e409f96 e93d7e11 7393172a`
T	`9e99a7bf 31e71090 0662f65e 617c5184`

Example 7: *Mlen* = 320

M	`6bc1bee2 2e409f96 e93d7e11 7393172a`
	`ae2d8a57 1e03ac9c 9eb76fac 45af8e51`
	`30c81c46 a35ce411`

T	`8a1de5be 2eb31aad 089a82e6 ee908b0e`

Example 8: *Mlen* = 512

M	`6bc1bee2 2e409f96 e93d7e11 7393172a`
	`ae2d8a57 1e03ac9c 9eb76fac 45af8e51`
	`30c81c46 a35ce411 e5fbc119 1a0a52ef`
	`f69f2445 df4f9b17 ad2b417b e66c3710`

T	`a1d5df0e ed790f79 4d775896 59f39a11`

D.3 AES-256

For Examples 9–12 below, the block cipher is the AES algorithm with the following 256 bit key:

K	603deb10 15ca71be 2b73aef0 857d7781 1f352c07 3b6108d7 2d9810a3 0914dff4.

Subkey Generation

$\mathrm{CIPH}_K(0^{128})$	e568f681 94cf76d6 174d4cc0 4310a854
K1	cad1ed03 299eedac 2e9a9980 8621502f
K2	95a3da06 533ddb58 5d353301 0c42a0d9

Example 9: *Mlen* = 0

M	<empty string>
T	028962f6 1b7bf89e fc6b551f 4667d983

Example 10: *Mlen* = 128

M	6bc1bee2 2e409f96 e93d7e11 7393172a
T	28a7023f 452e8f82 bd4bf28d 8c37c35c

Example 11: *Mlen* = 320

M	6bc1bee2 2e409f96 e93d7e11 7393172a ae2d8a57 1e03ac9c 9eb76fac 45af8e51 30c81c46 a35ce411
T	aaf3d8f1 de5640c2 32f5b169 b9c911e6

Example 12: *Mlen* = 512

M	6bc1bee2 2e409f96 e93d7e11 7393172a ae2d8a57 1e03ac9c 9eb76fac 45af8e51 30c81c46 a35ce411 e5fbc119 1a0a52ef f69f2445 df4f9b17 ad2b417b e66c3710
T	e1992190 549f6ed5 696a2c05 6c315410

D.4 Three Key TDEA

For Examples 13-16 below, the block cipher is three key TDEA with the following key:

Key1	8aa83bf8 cbda1062
Key2	0bc1bf19 fbb6cd58
Key3	bc313d4a 371ca8b5

Subkey Generation

$\mathrm{CIPH}_K(0^{64})$	c8cc74e9 8a7329a2
K1	9198e9d3 14e6535f
K2	2331d3a6 29cca6a5

Example 13: *Mlen* = 0

M	<empty string>
T	b7a688e1 22ffaf95

Example 14: *Mlen* = 64

M	6bc1bee2 2e409f96
T	8e8f2931 36283797

Example 15: *Mlen* = 160

M	6bc1bee2 2e409f96 e93d7e11 7393172a ae2d8a57
T	743ddbe0 ce2dc2ed

Example 16: *Mlen* = 256

M	6bc1bee2 2e409f96 e93d7e11 7393172a ae2d8a57 1e03ac9c 9eb76fac 45af8e51
T	33e6b109 2400eae5

D.5 Two Key TDEA

For Examples 17-20 below, the block cipher is two key TDEA with the following key:

Key1	4cf15134 a2850dd5
Key2	8a3d10ba 80570d38
Key3	4cf15134 a2850dd5

Subkey Generation

CIPH$_K$(0^{64})	c7679b9f 6b8d7d7a
K1	8ecf373e d71afaef
K2	1d9e6e7d ae35f5c5

Example 17: *Mlen* = 0

M	<empty string>
T	bd2ebf9a 3ba00361

Example 18: *Mlen* = 64

M	6bc1bee2 2e409f96
T	4ff2ab81 3c53ce83

Example 19: *Mlen* = 160

M	6bc1bee2 2e409f96 e93d7e11 7393172a ae2d8a57
T	62dd1b47 1902bd4e

Example 20: *Mlen* = 256

M	6bc1bee2 2e409f96 e93d7e11 7393172a ae2d8a57 1e03ac9c 9eb76fac 45af8e51
T	31b1e431 dabc4eb8