APPENDIX E
MESSAGE AUTHENTICATION CODES BASED ON BLOCK CIPHERS

William Stallings

Supplement to
Computer Security, Third Edition
Pearson 2014
http://williamstallings.com/ComputerSecurity

In this section, we look at several MACs based on the use of a block cipher.

E.1 CIPHER-BASED MESSAGE AUTHENTICATION CODE

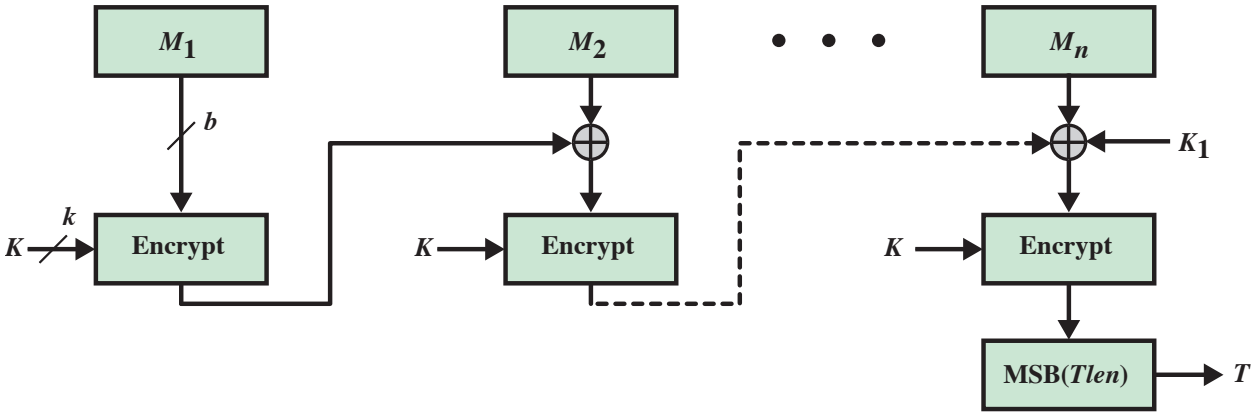
The Cipher-based Message Authentication Code (CMAC) mode of operation is for use with AES and triple DES. It is specified in NIST Special Publication 800-38B.

First, let us consider the operation of CMAC when the message is an integer multiple n of the cipher block length b. For AES, $b = 128$, and for triple DES, $b = 64$. The message is divided into n blocks (M_1, M_2, …, M_n). The algorithm makes use of a k-bit encryption key K and an b-bit constant, K_1. For AES, the key size k is 128, 192, or 256 bits; for triple DES, the key size is 112 or 168 bits. CMAC is calculated as follows (Figure E.1).

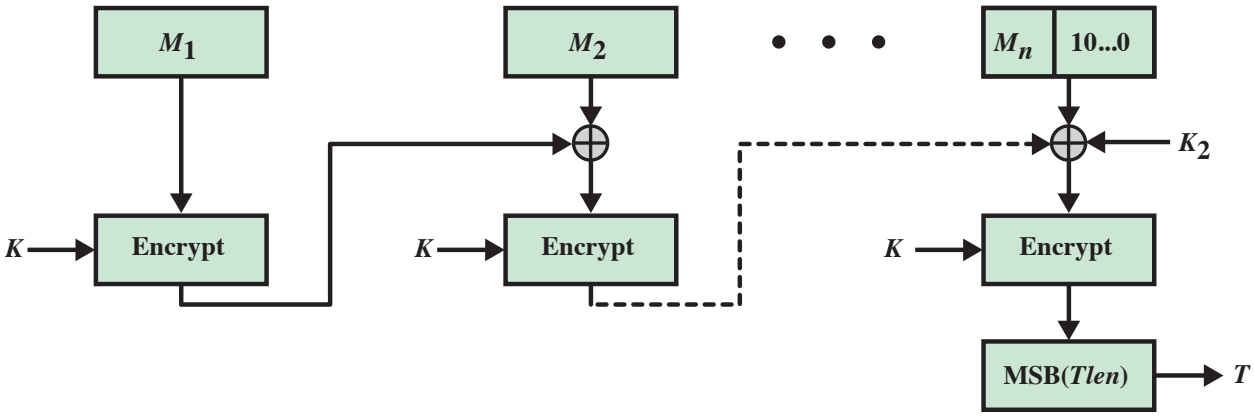
$$C_1 = \mathrm{E}(K, M_1)$$
$$C_2 = \mathrm{E}(K, [M_2 \oplus C_1])$$
$$C_3 = \mathrm{E}(K, [M_3 \oplus C_2])$$
$$\bullet$$
$$\bullet$$
$$\bullet$$
$$C_n = \mathrm{E}(K, [M_n \oplus C_{n-1} \oplus K_1])$$
$$T = \mathrm{MSB}_{Tlen}(C_n)$$

where

T = message authentication code, also referred to as the tag
$Tlen$ = bit length of T
$\mathrm{MSB}_s(X)$ = the s leftmost bits of the bit string X



(a) Message length is integer multiple of block size



(b) Message length is not integer multiple of block size

Figure E.1 Cipher-Based Message Authentication Code (CMAC)

If the message is not an integer multiple of the cipher block length, then the final block is padded to the right (least significant bits) with a 1 and as many 0s as necessary so that the final block is also of length *b*. The CMAC operation then proceeds as before, except that a different *b*-bit key K_2 is used instead of K_1.

To generate the two *b*-bit keys, the block cipher is applied to the block that consists entirely of 0 bits. The first subkey is derived from the resulting ciphertext by a left shift of one bit and, conditionally, by XORing a constant

that depends on the block size. The second subkey is derived in the same manner from the first subkey.

E.2 COUNTER WITH CIPHER BLOCK CHAINING MESSAGE AUTHENTICATION CODE

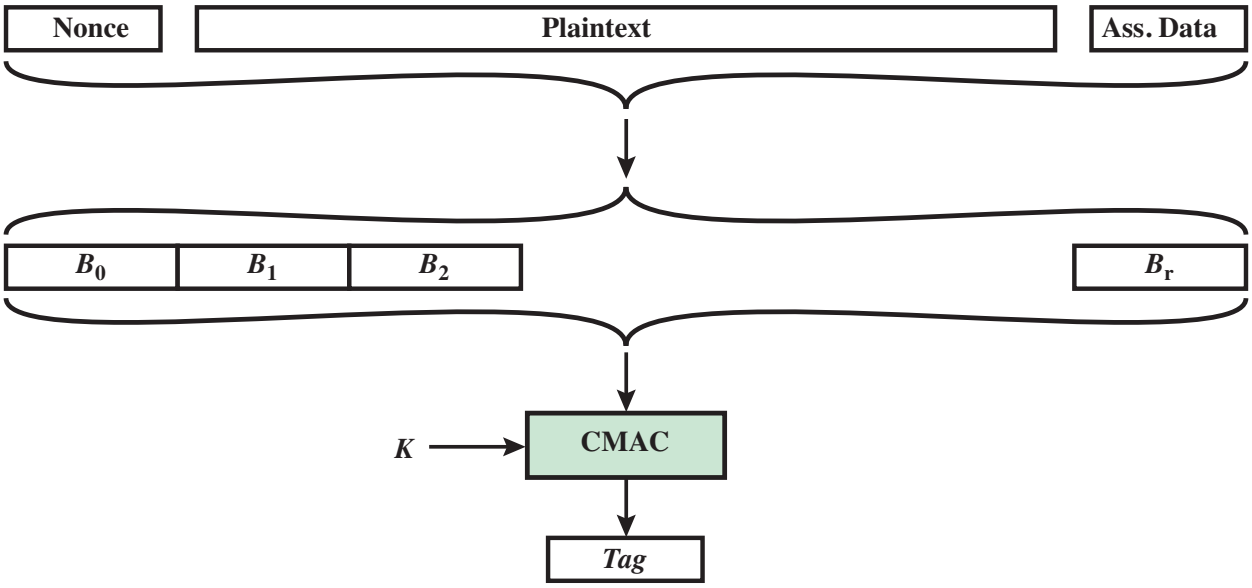
The CCM mode of operation, defined in NIST SP 800-38C, is referred to as an **authenticated encryption** mode. Authenticated encryption is a term used to describe encryption systems that simultaneously protect confidentiality and authenticity (integrity) of communications. Many applications and protocols require both forms of security, but until recently the two services have been designed separately.

The key algorithmic ingredients of CCM are the AES encryption algorithm (Section 2.2), the CTR mode of operation (Section 2.5), and the CMAC authentication algorithm. A single key *K* is used for both encryption and MAC algorithms. The input to the CCM encryption process consists of three elements.

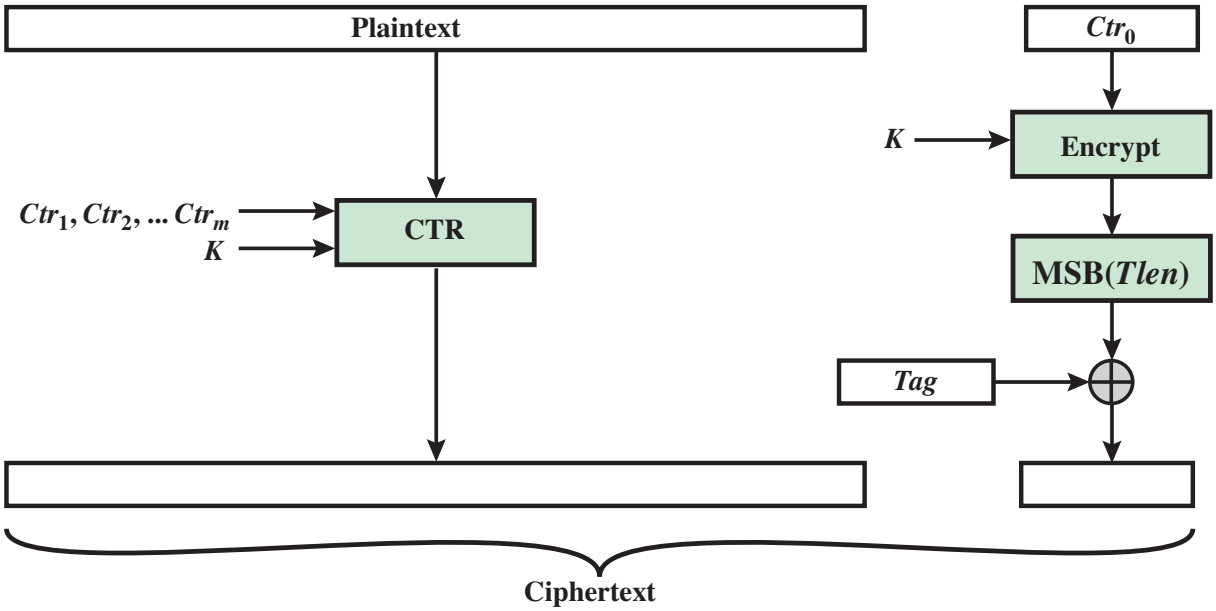
1. Data that will be both authenticated and encrypted. This is the plaintext message *P* of data block.
2. Associated data *A* that will be authenticated but not encrypted. An example is a protocol header that must be transmitted in the clear for proper protocol operation but which needs to be authenticated.
3. A nonce *N* that is assigned to the payload and the associated data. This is a unique value that is different for every instance during the lifetime of a protocol association and is intended to prevent replay attacks and certain other types of attacks.

Figure E.2 illustrates the operation of CCM. For authentication, the input includes the nonce, the associated data, and the plaintext. This input is formatted as a sequence of blocks B_0 through B_r. The first block contains the nonce plus some formatting bits that indicate the lengths of the *N*, *A*, and *P* elements. This is followed by zero or more blocks that contain *A*, followed by zero of more blocks that contain *P*. The resulting sequence of blocks serves as input to the CMAC algorithm, which produces a MAC value with length *Tlen*, which is less than or equal to the block length (Figure E.2a).

For encryption, a sequence of counters is generated that must be independent of the nonce. The authentication tag is encrypted in CTR mode using the single counter Ctr_0. The *Tlen* most significant bits of the output are XORed with the tag to produce an encrypted tag. The remaining counters are used for the CTR mode encryption of the plaintext (Figure 20.8). The encrypted plaintext is concatenated with the encrypted tag to form the ciphertext output (Figure E.2b).



(a) Authentication



(b) Encryption

Figure E.2 Counter with Cipher Block Chaining-Message Authentication Code (CCM)