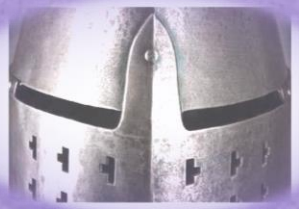


Chapter 12

Message Authentication Codes

Security problems

- Masquerade
  - Insertion of messages into the network from a fraudulent source
- Content modification
  - Changes to the contents of a message
- Sequence modification
  - Any modification to a sequence of messages
- Timing modification
  - Delay or replay of messages
- Source repudiation
  - Denial of transmission of message by source
- Destination repudiation
  - Denial of receipt of message by destination

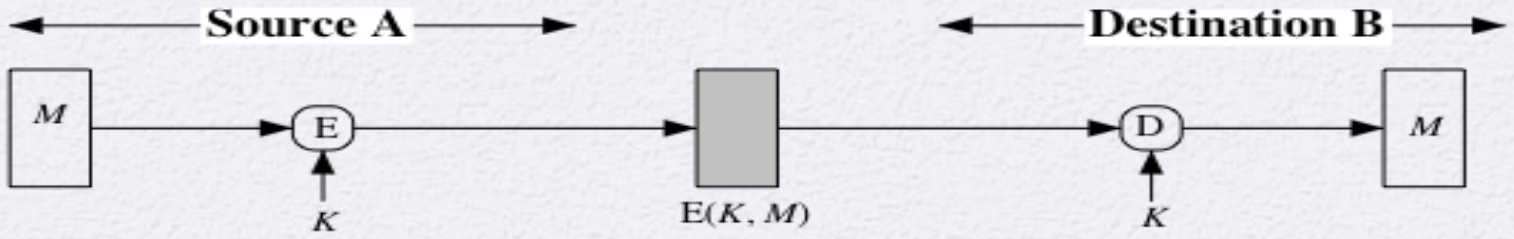
Message Authentication

- A service objective for making sure that the message is authenticated.
  - Content authentication: the content has not been modified.
  - Source authentication: the message is indeed from what is claimed

Message Authentication Functions

- Hash function
  - Hash serves as the authenticator
- Message encryption
  - The ciphertext serves as the authenticator
- Message authentication code (MAC)
  - Keyed hash value serves as the authenticator

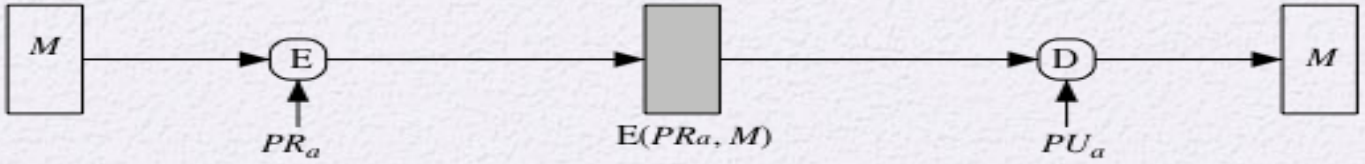
SK Encryption for Authentication



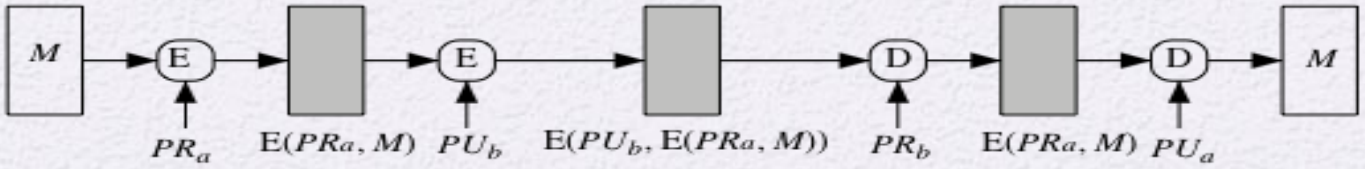
(a) Symmetric encryption: confidentiality and authentication

PK Encryption for Authentication

(b) Public-key encryption: confidentiality

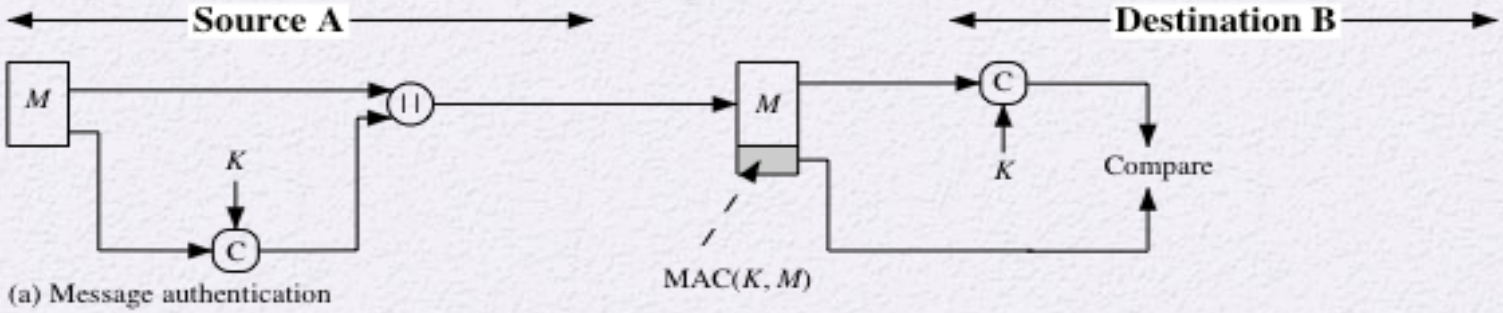


(c) Public-key encryption: authentication and signature

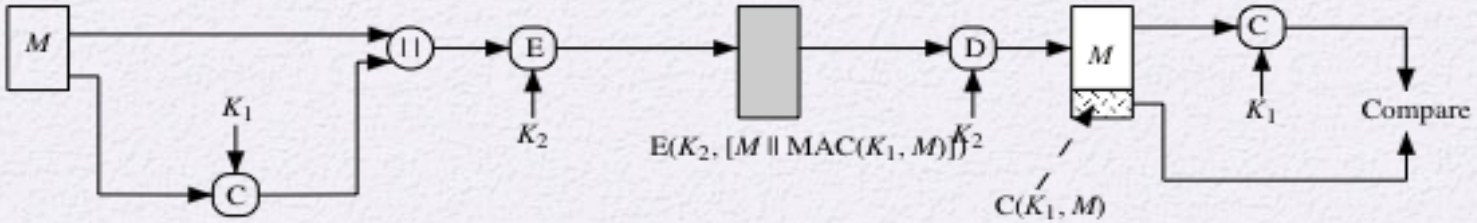


(d) Public-key encryption: confidentiality, authentication, and signature

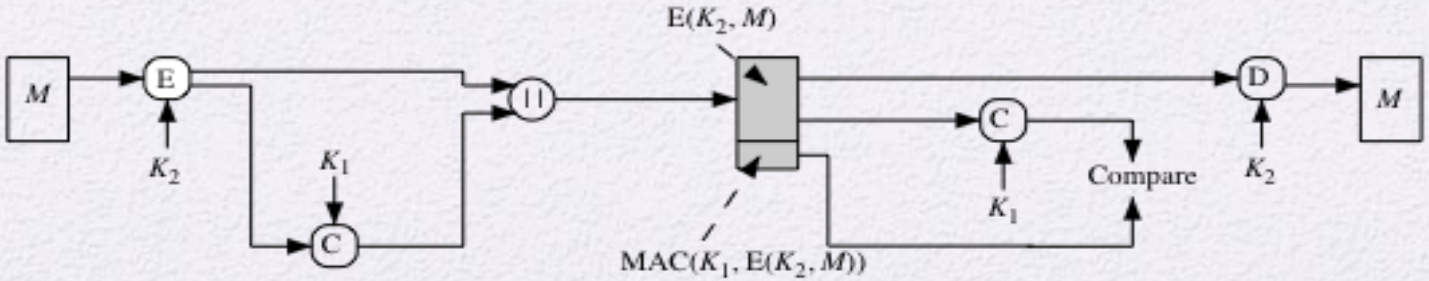
MAC for Authentication



(a) Message authentication



(b) Message authentication and confidentiality; authentication tied to plaintext

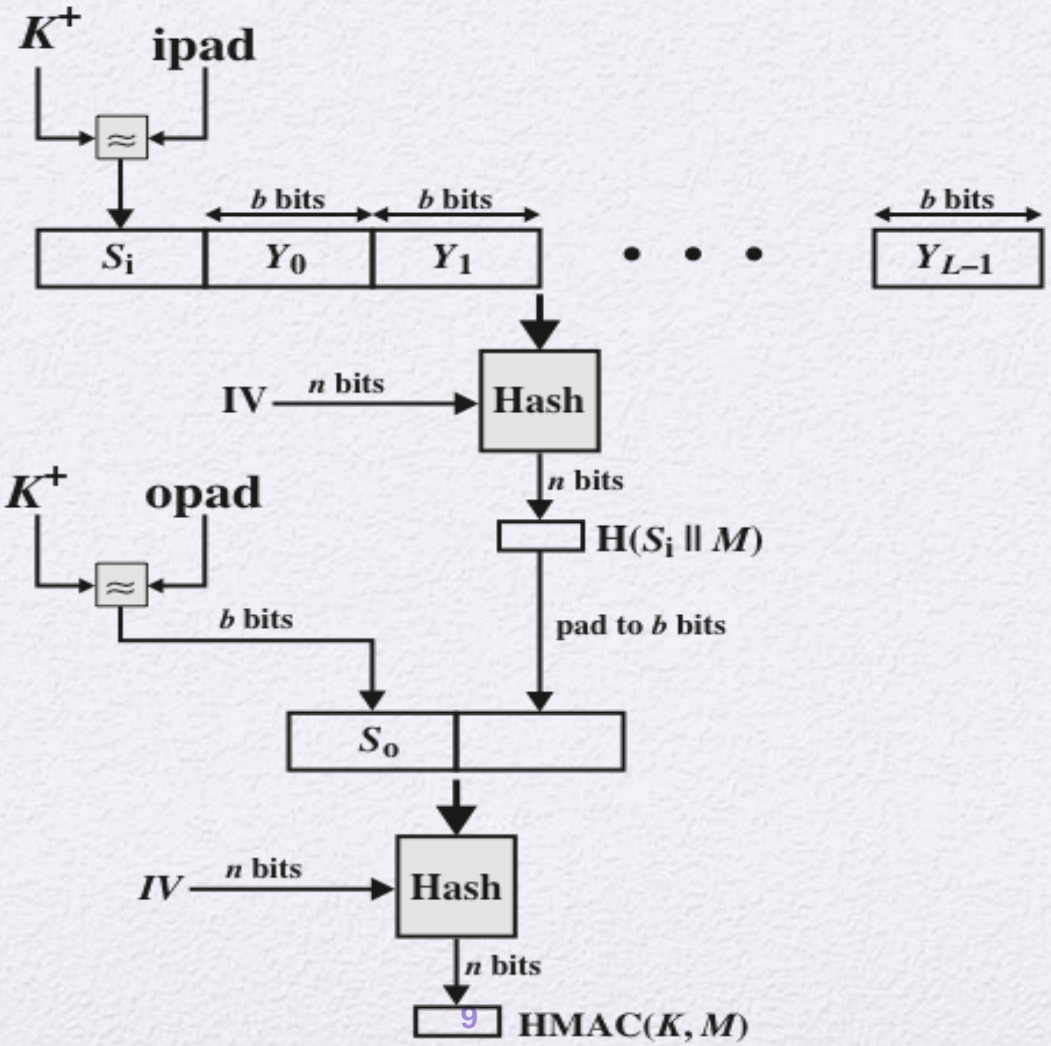


(c) Message authentication and confidentiality; authentication tied to ciphertext

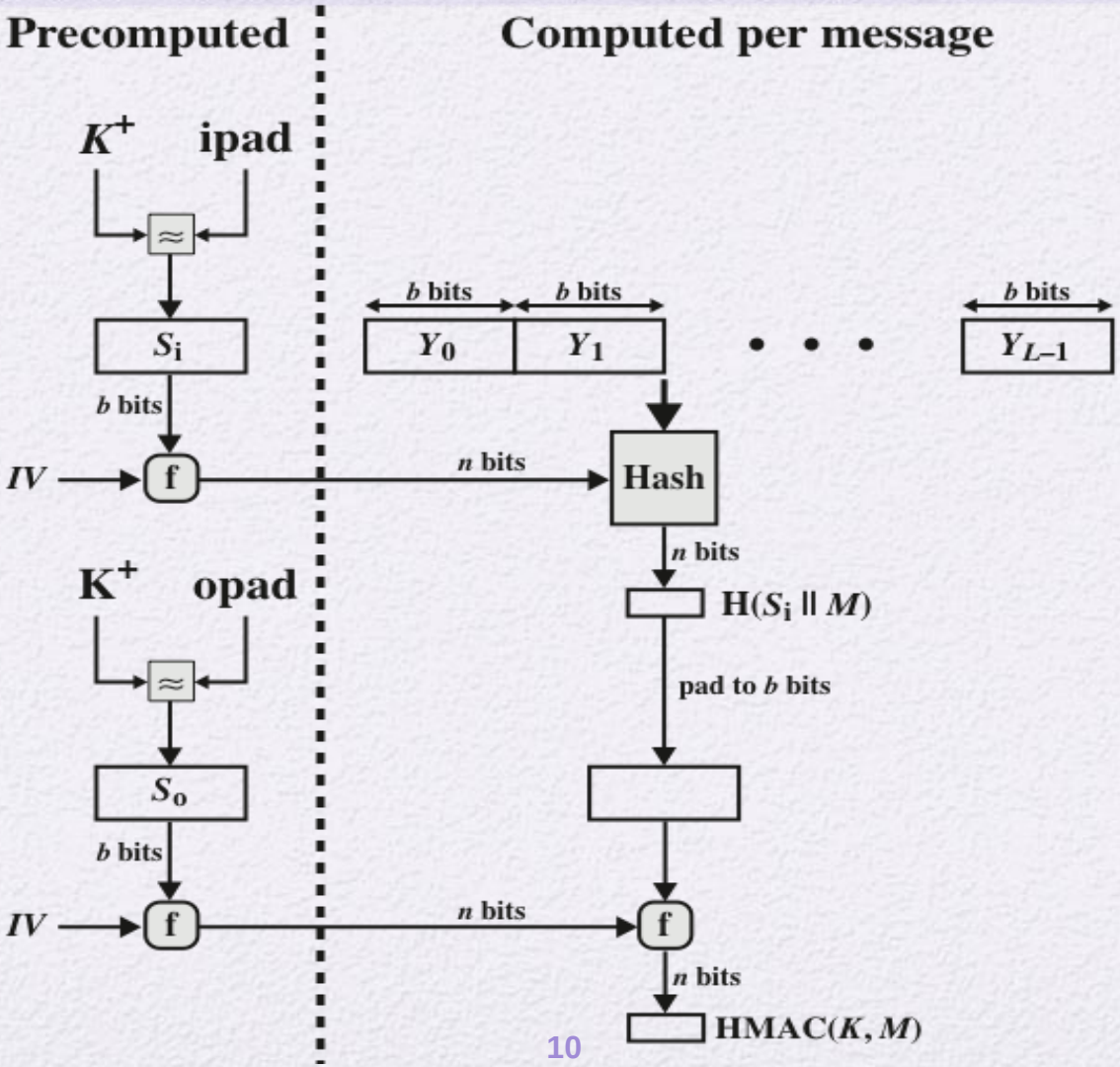
HMAC: Hash Function-based MAC

- Motivations
  - Cryptographic hash functions such as MD5 and SHA are faster in software than symmetric block ciphers
  - Library code for cryptographic hash functions is widely available
- HMAC: mandatory-to-implement for IP security
- FIPS 198: NIST standard

HMAC Structure



Efficient implementation

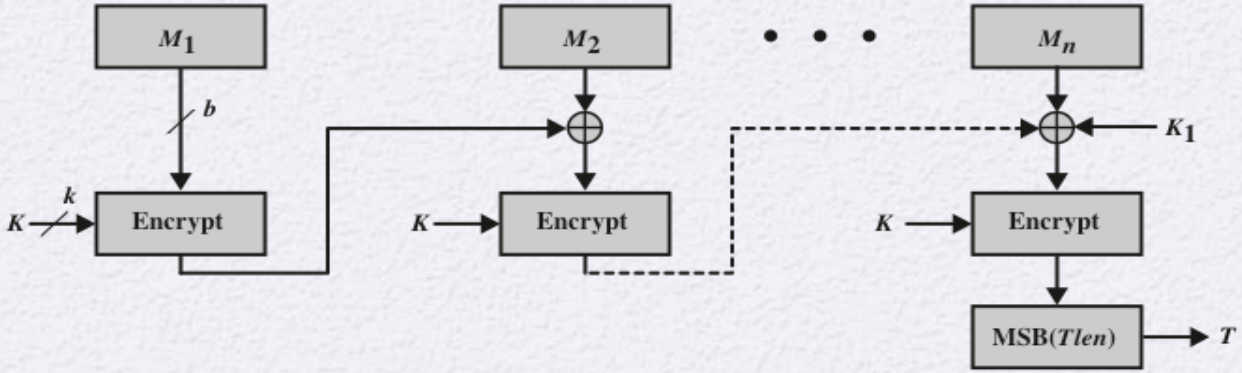


Security of HMAC

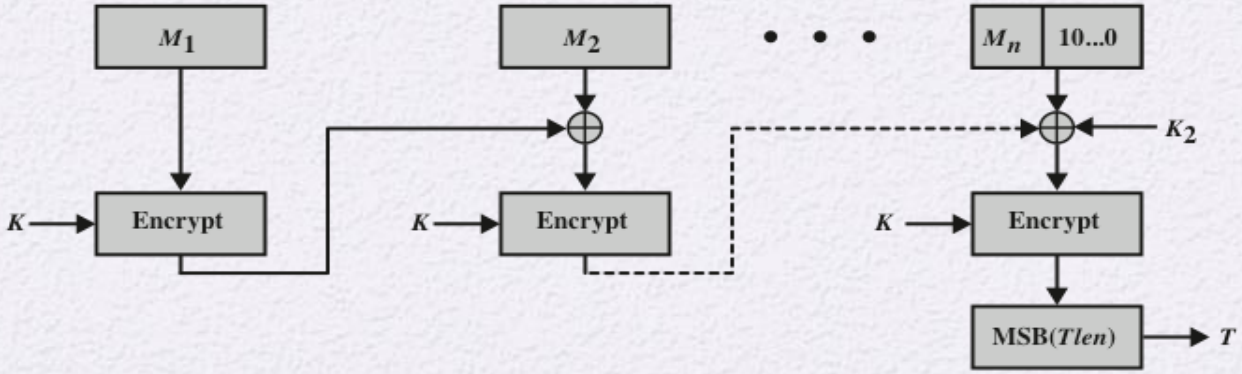
- Depend on the strength of the underlying hash function
- Proved security:

  security of HMAC = strength of the embedded hash function

CMAC: Cipher-based MAC



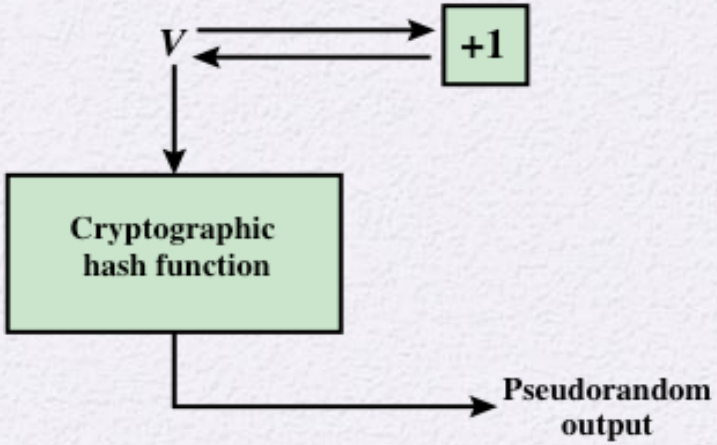
(a) Message length is integer multiple of block size



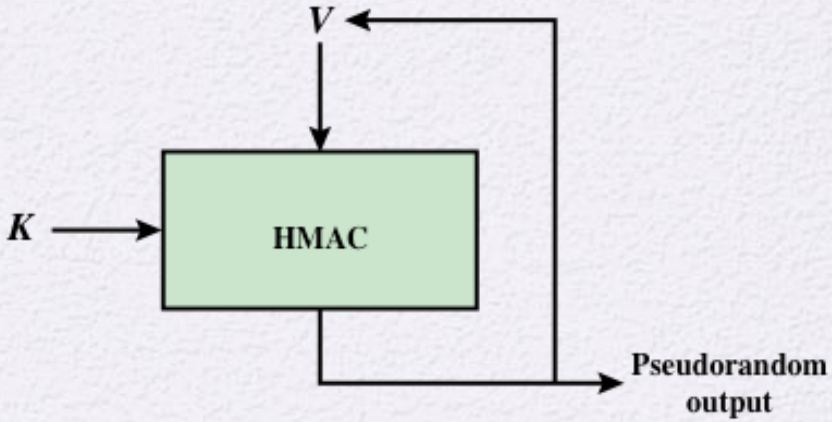
(b) Message length is not integer multiple of block size

Figure 12.8 Cipher-Based Message Authentication Code (CMAC)

Hash Functions and MAC for PRNG



(a) PRNG using cryptographic hash function



(b) PRNG using HMAC

Three PRNG based on HMAC

$m = \lceil n/\text{outlen} \rceil$ $w_0 = V$ W = the null string For $i = 1$ to m $w_i = \text{MAC}(K, w_{i-1})$ $W = W \| w_i$ Return leftmost n bits of W	$m = \lceil n/\text{outlen} \rceil$ W = the null string For $i = 1$ to m $w_i = \text{MAC}(K, (V \| i))$ $W = W \| w_i$ Return leftmost n bits of W	$m = \lceil n/\text{outlen} \rceil$ $\text{A}(0) = V$ W = the null string For $i = 1$ to m $\text{A}(i) = \text{MAC}(K, \text{A}(i-1))$ $w_i = \text{MAC}(K, (\text{A}(i) \| V)$ $W = W \| w_i$ Return leftmost n bits of W
NIST SP 800-90	**IEEE 802.11i**	**TLS/WTLS**

Summary

- Security problems
- Message authentication
  - Authentication service
  - Message encryption
  - Message authentication code
- Message authentication functions
  - Hash functions
  - Message encryption
  - Message authentication codes
- MACs based on hash functions: (HMAC)
  - HMAC design objectives
  - HMAC algorithm
  - Security of HMAC
- MAC based on block ciphers: CMAC
- Pseudorandom number generation using hash functions and MACs