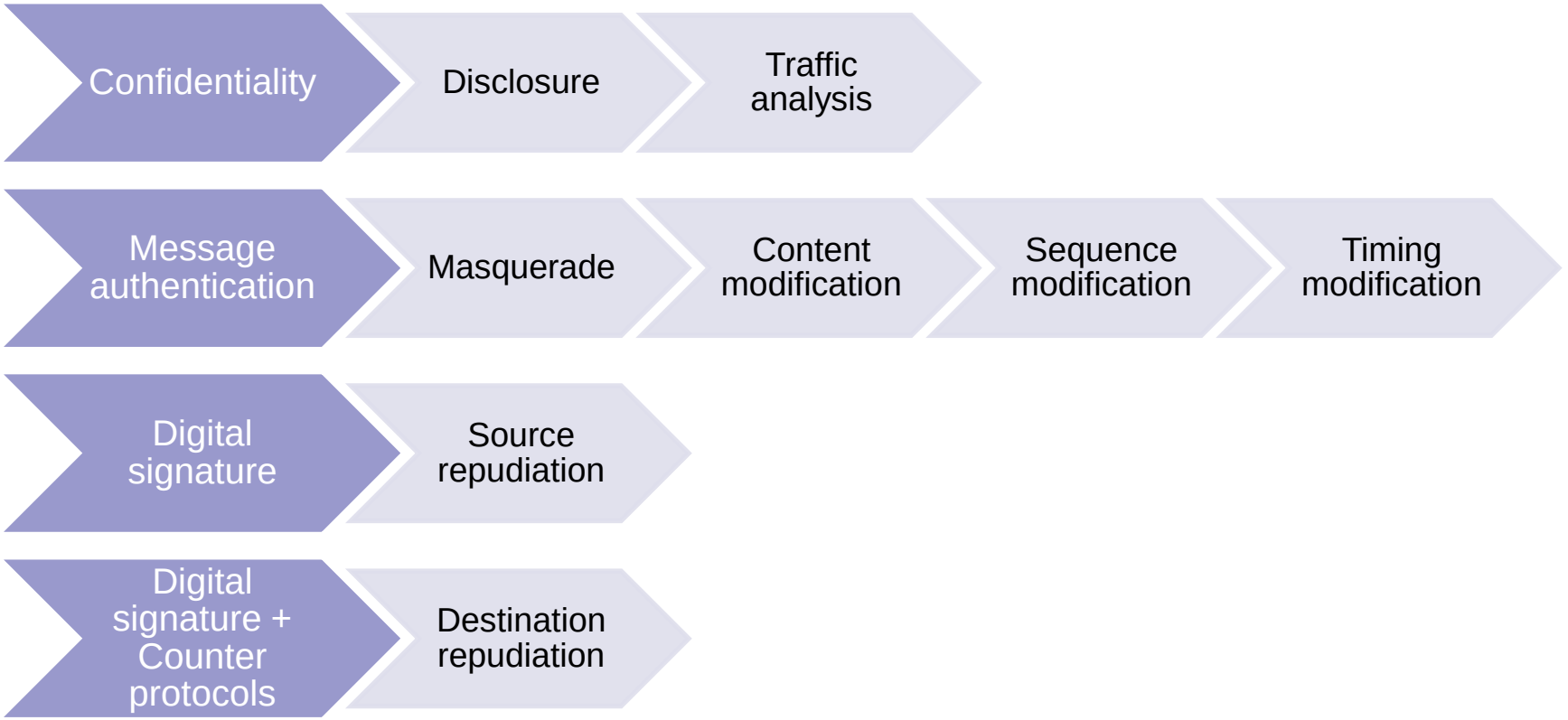
CYB 241 Digital Cryptography Techniques

Message Authentication Codes

Possible Attacks

- Disclosure
  - Release of message contents to any person or process not possessing the appropriate cryptographic key
- Traffic analysis
  - Discovery of the pattern of traffic between parties
- Masquerade
  - Insertion of messages into the network from a fraudulent source
- Content modification
  - Changes to the contents of a message, including insertion, deletion, transposition, and modification
- Sequence modification
  - Any modification to a sequence of messages between parties, including insertion, deletion, and reordering
- 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

Possible Attacks



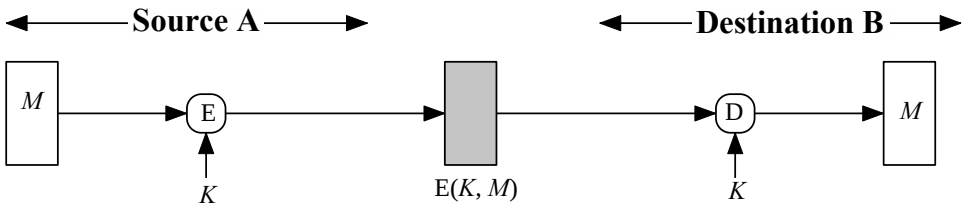
Authentication Requirements

- Verify messages come from the alleged source
- Have not been altered
- Verify sequencing and timeliness
- Counter repudiation by the source (signature)

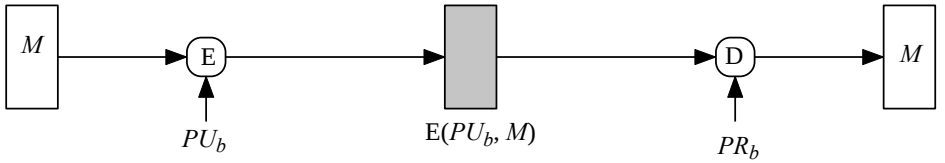
Message Authentication Functions

- Message Authentication functions are used to produce an authenticator
- Functions can be grouped into three classes
  - Hash functions (already studied)
    - A function that maps a message of any length into a fixed-length hash value which serves as the authenticator
  - Message encryption (must be structured)
    - The ciphertext of the entire message serves as its authenticator
  - Message authentication codes (MAC)
    - A function of the message and a secret key that produces a fixed-length value that serves as the authenticator

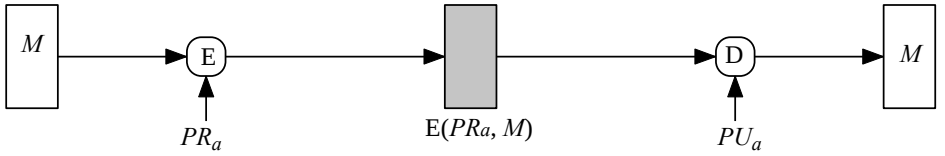
Message Encryption



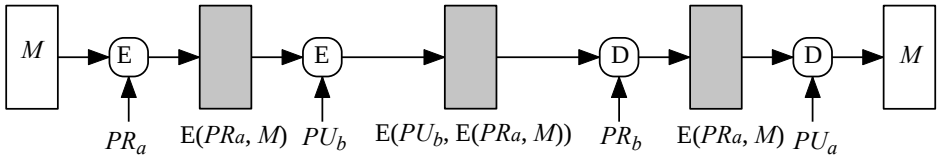
(a) Symmetric encryption: confidentiality and authentication



(b) Public-key encryption: confidentiality



(c) Public-key encryption: authentication and signature



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

Figure 12.1 Basic Uses of Message Encryption

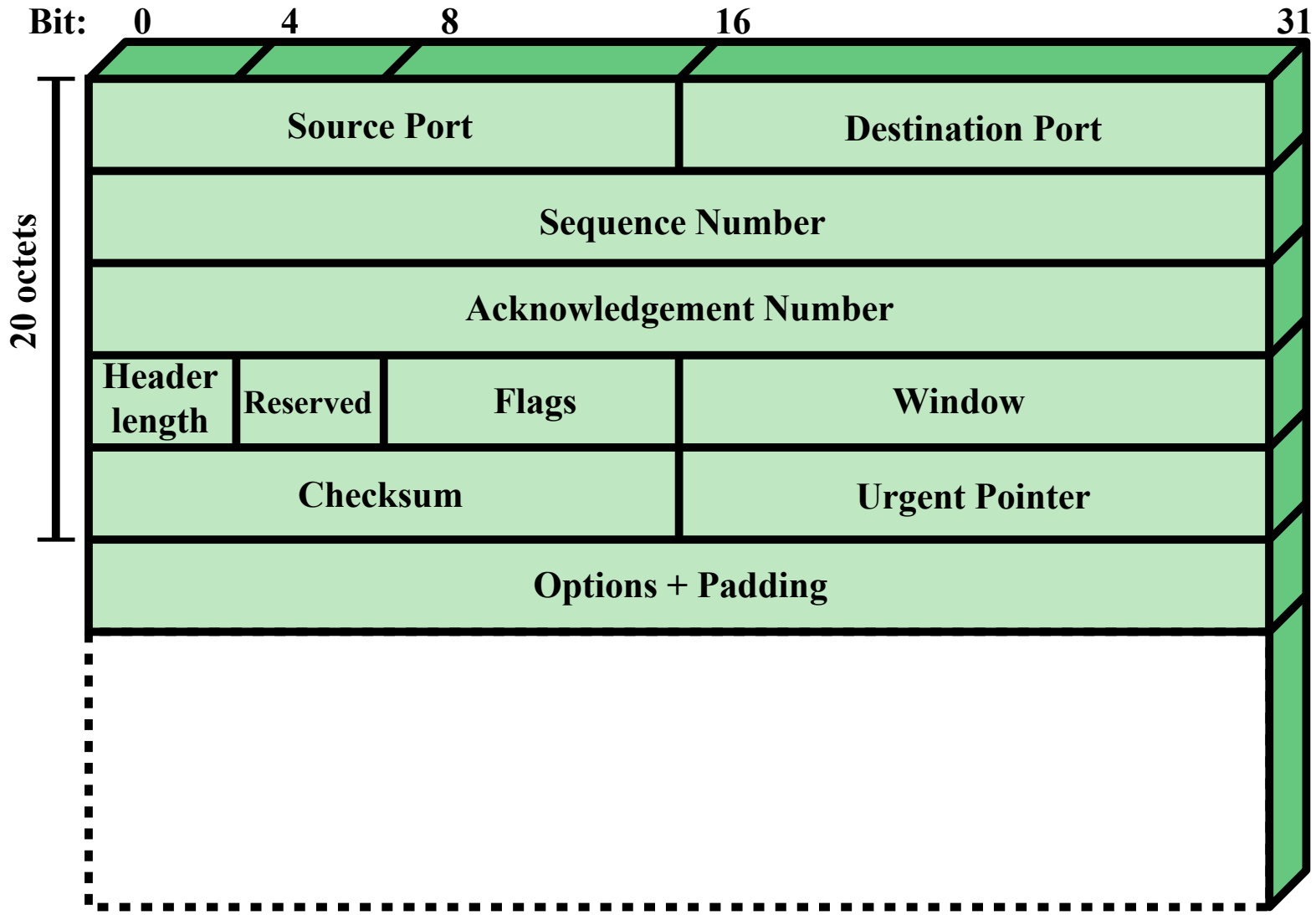


Figure 12.3 TCP Segment

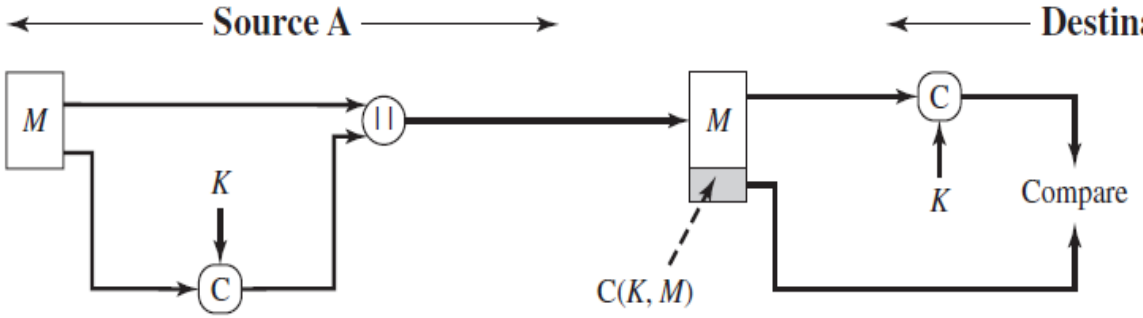
Message Authentication Codes (MAC)

- MAC is Known as Cryptographic checksum or Authentication tag
- Similar to hash function, but uses a secret key
- Also MAC is similar to encryption but can be nonreversible (decryption is not needed).

MAC = C*(K,M)*

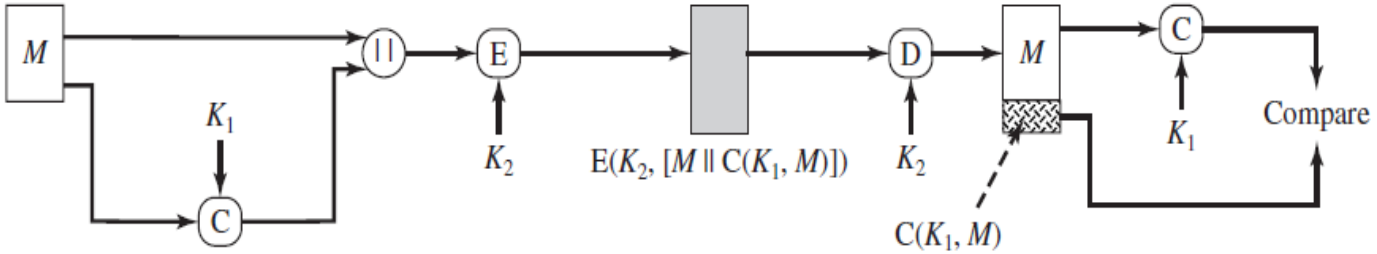
- M = input message
- K = secret key
- C = MAC function
- MAC = message authentication code

A → B: $M \| C(K, M)$
- Provides authentication
  - —Only A and B share K



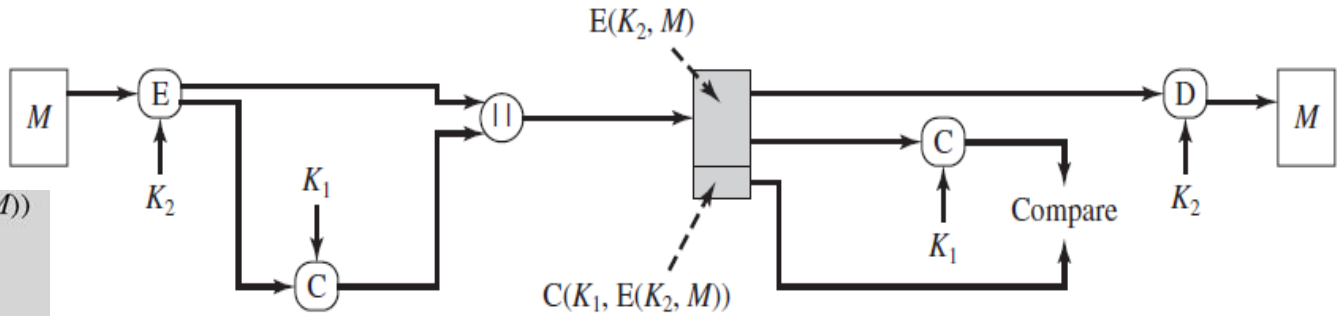
(a) Message authentication

A → B: $E(K_2, [M \| C(K, M)])$
- Provides authentication
  - —Only A and B share K_1
- Provides confidentiality
  - —Only A and B share K_2



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

A → B: $E(K_2, M) \| C(K_1, E(K_2, M))$
- Provides authentication
  - —Using K_1
- Provides confidentiality
  - —Using K_2



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

MAC

- Why not simply use encryption instead of a separate message authentication code?

MAC Approaches

- MACs Based on Hash Functions
  - HMAC
- MACs Based on Block Ciphers
  - DAA: Data Authentication Algorithm
  - CMAC: Cipher-Based MAC

HMAC

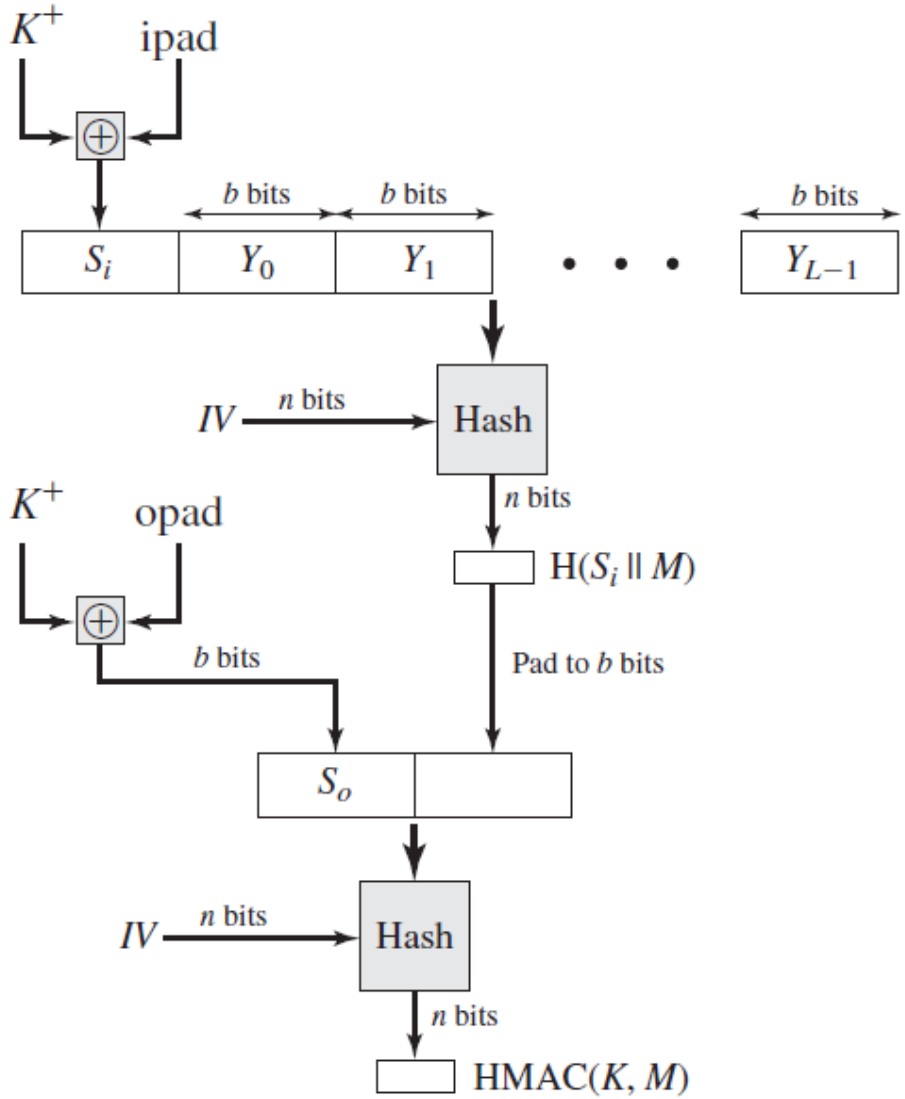
- There has been increased interest in developing a MAC derived from a cryptographic hash function
- Motivations:
  - Cryptographic hash functions such as MD5 and SHA generally execute faster in software than symmetric block ciphers such as DES
  - Library code for cryptographic hash functions is widely available
- HMAC has been chosen as the mandatory-to-implement MAC for IP security
- Has also been issued as a NIST standard (FIPS 198)

HMAC

Y_i = *i* th block of M,

K_+ = *Padded secret key*

ipad = 00110110
(36 in hexadecimal)
repeated *b*/8 times
opad = 01011100
(5C in hexadecimal)
repeated *b*/8 times

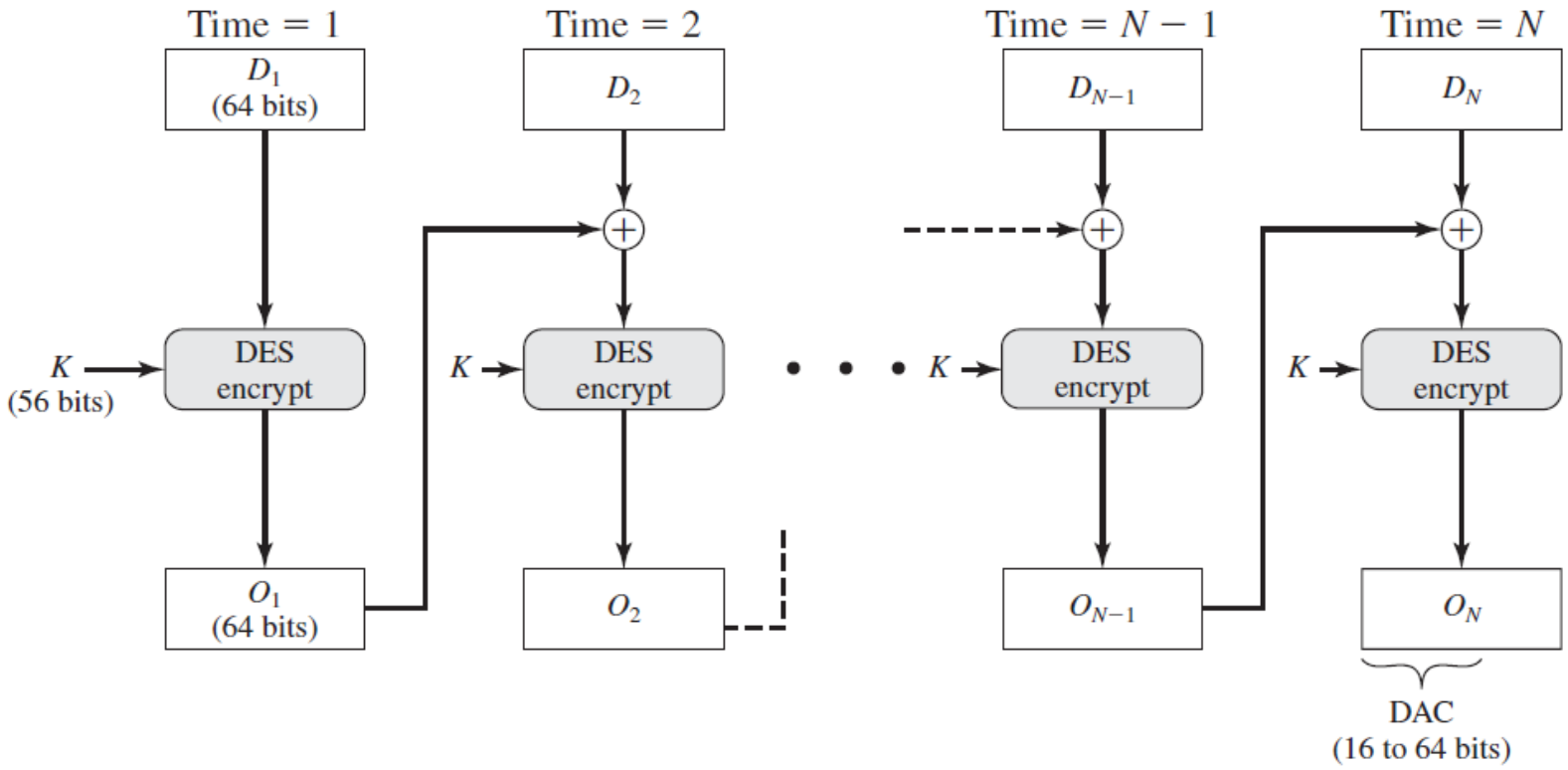


$$\text{HMAC}(K, M) = \text{H}[(K^+ \oplus \text{opad}) \| \text{H}[(K^+ \oplus \text{ipad}) \| M]]$$

Data Authentication Algorithm (DAA)

- Based on DES
- Encrypts message using cipher block chaining (CBC) mode with IV equals zero
- Equivalent to CBC-MAC using DES cipher

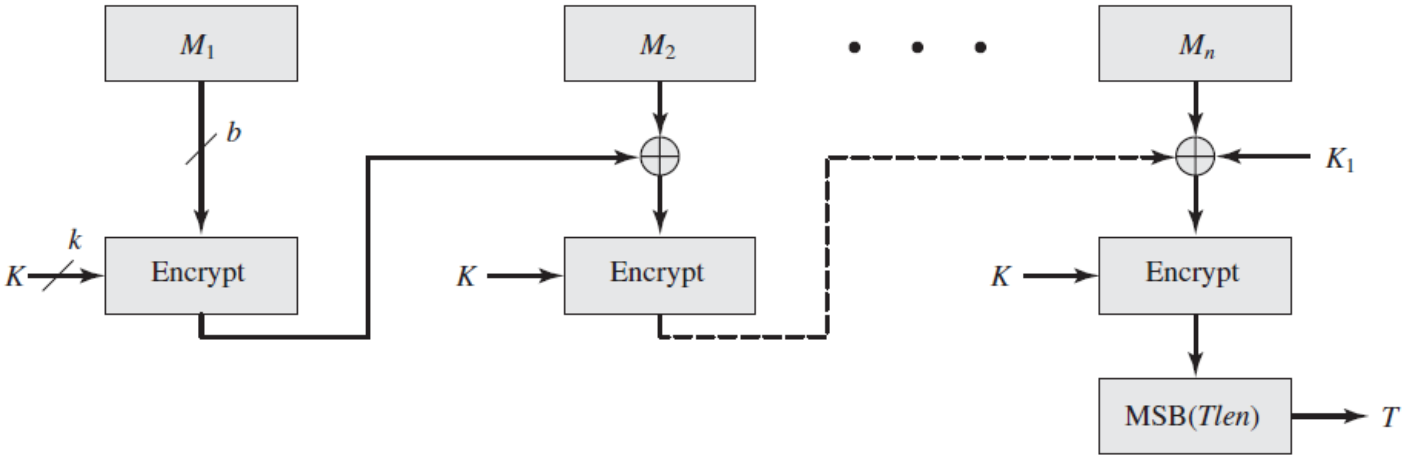
Data Authentication Algorithm



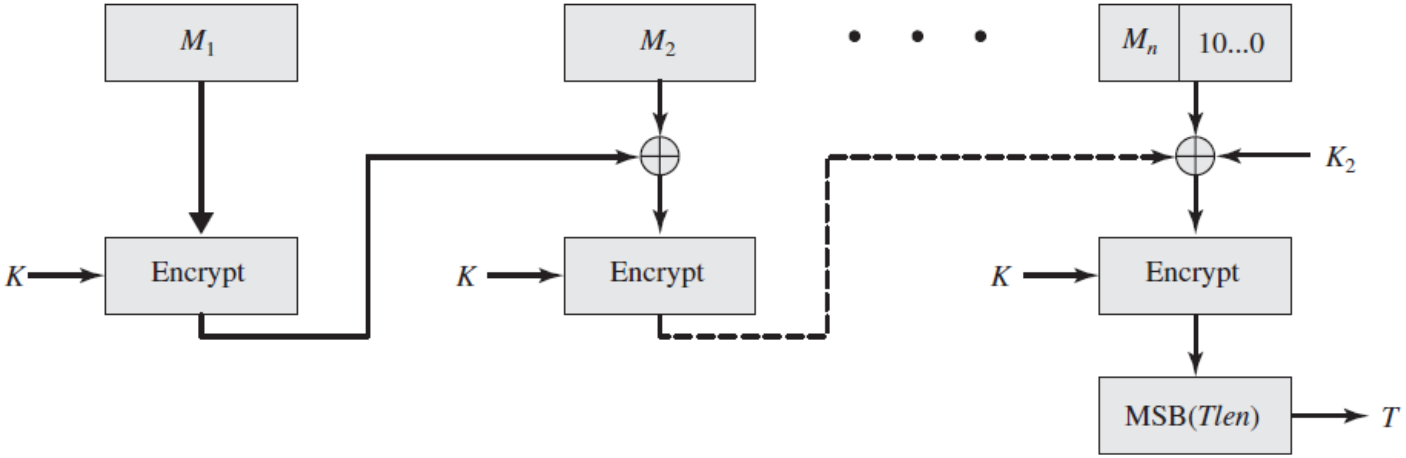
CMAC

- Modify CBC-MAC/DAA
- Work on variable length message
- Use any block cipher

CMAC



(a) Message length is integer multiple of block size



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

Reading Assignment

- Textbook
  - Chapter 12
    - 12.1, 12.2, 12.5, 12.6,12.7