Cryptography and Network Security

Chapter 4 – Part B

Message Authetication Codes

Lectured by

Nguyễn Đức Thái

Outline

- Message Authentication Requirements
- Message Authentication Functions
- Basic Use of MACs
- MACs based on Hash Functions: HMAC

Message Authentication

- Message authentication is a ***mechanism*** or ***service*** used to verify the integrity of a message.
- Message authentication assures that data received are ***exactly*** as sent by (i.e., contain no modification, insertion, deletion, or replay) and that the purported identity of the sender is valid.
- Symmetric encryption provides authentication among those who share the secret key.

Message Authentication

- A ***message authentication code*** (MAC) is an ***algorithm*** that requires the use of a ***secret key***.
- A MAC takes a *variable-length message* and a *secret key* as ***input*** and ***produces an authentication code***.
- A recipient in possession of the secret key can generate an authentication code to verify the integrity of the message
- One way: a MAC is ***to combine*** a ***cryptographic hash function*** in some fashion ***with a secret key***
- Another way: to use a symmetric block cipher in such a way that it produces a fixed-length output for a variablelength input

Message Authentication Requirements

- **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

Message Authentication

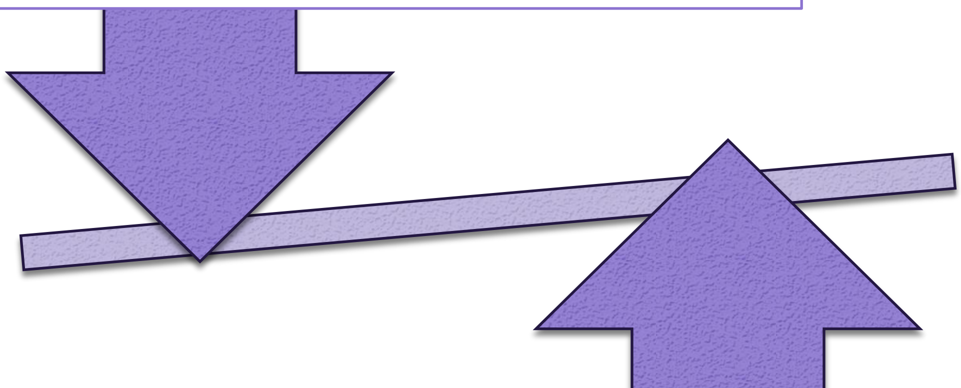
- ***Message authentication*** is a ***procedure*** to verify that received messages come from the alleged source and ***have not been altered***.
- Message authentication may also verify sequencing and timeliness
- A ***digital signature*** is an ***authentication technique*** that also includes measures to counter ***repudiation by the source***.

Message Authentication Functions

Two levels of

Lower level

- There must be some sort of function that produces an authenticator



Higher-level

- Uses the lower-level function as a primitive in an authentication protocol that enables a receiver to verify the authenticity of a message

- Hash function
  - A function that maps a message of any length into a fixed-length hash value which serves as the authenticator
- Message encryption
  - The ciphertext of the entire message serves as its authenticator
- Message authentication code (MAC)
  - A function of the message and a secret key that produces a fixed-length value that serves as the authenticator

Message Encryption

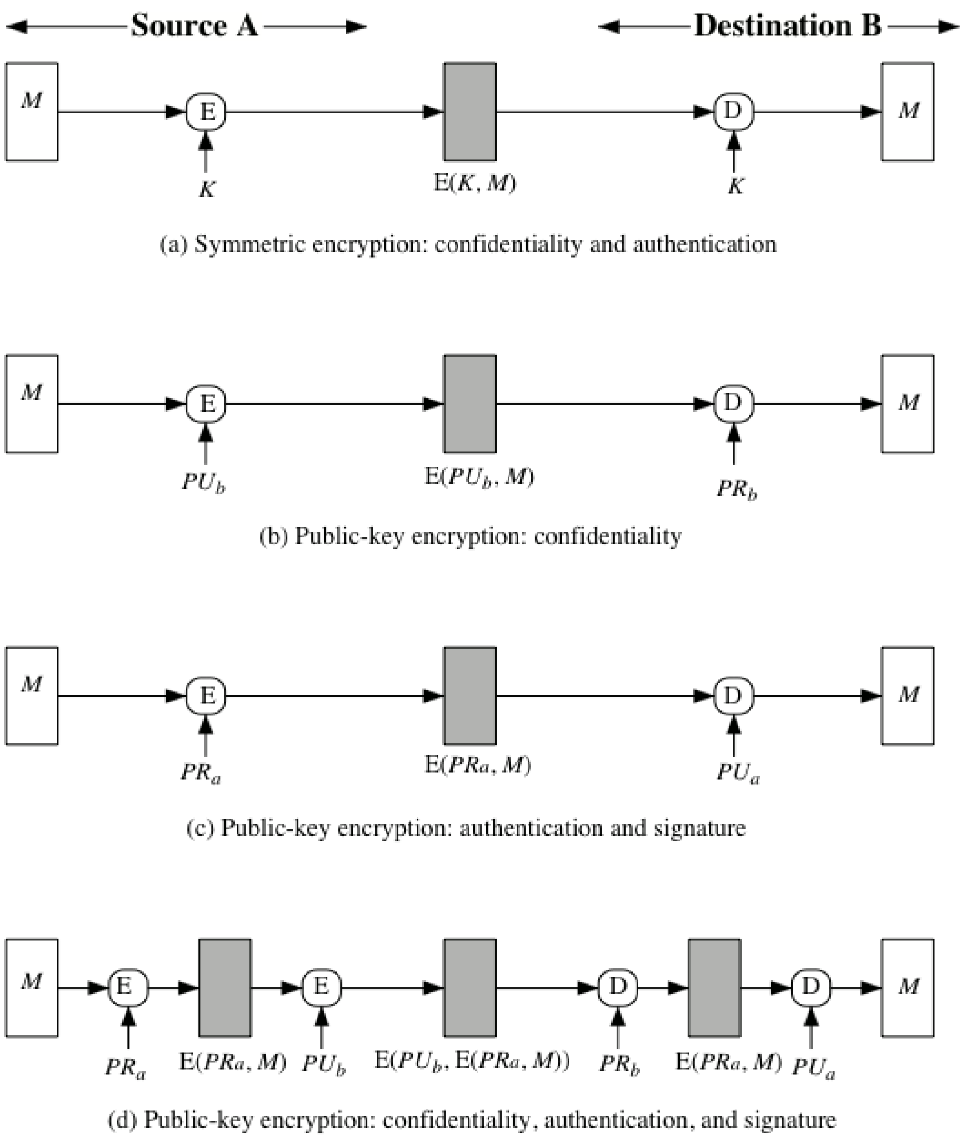


Figure 12.1 Basic Uses of Message Encryption

Internal and External Error Control

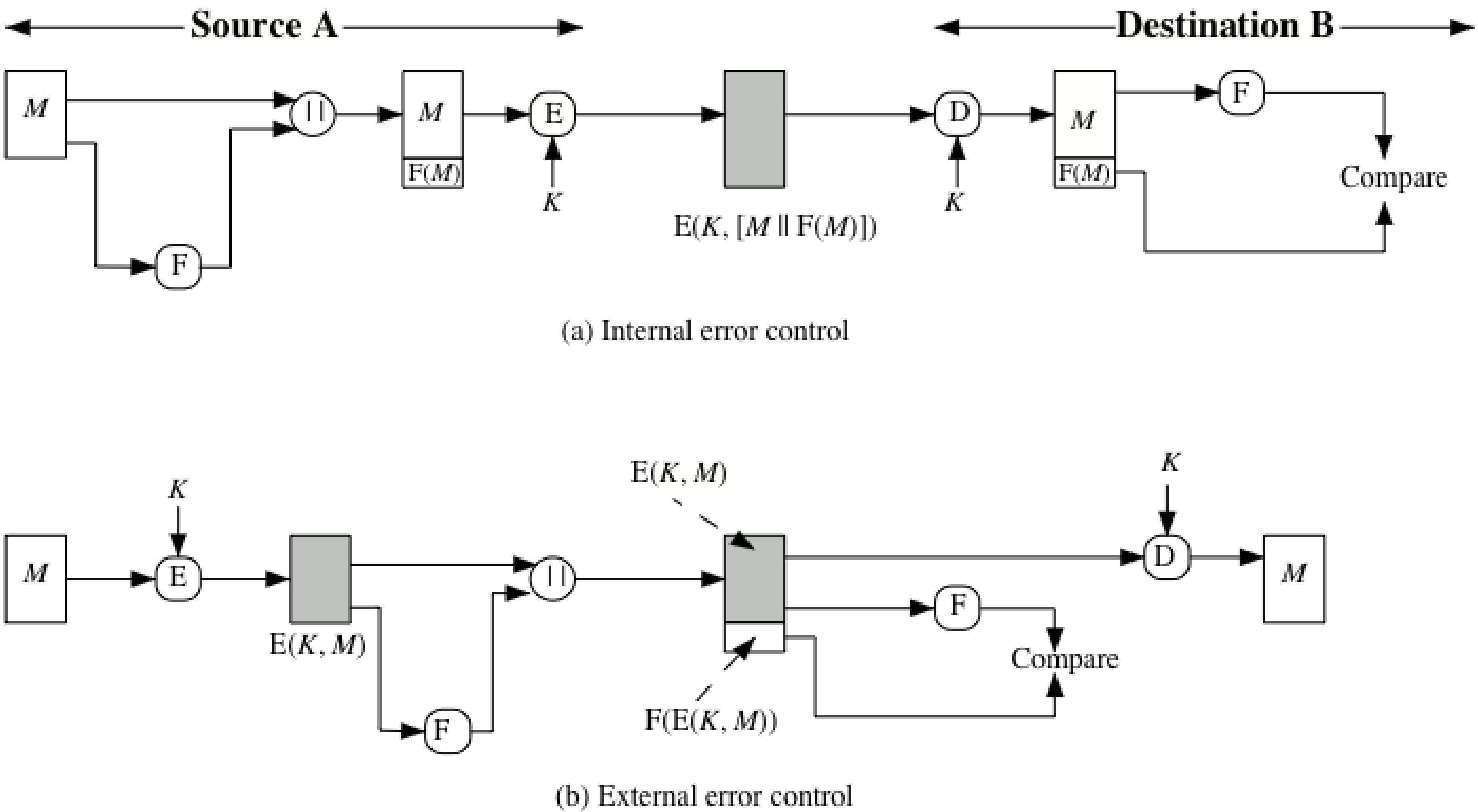


Figure 12.2 Internal and External Error Control

TCP Segment

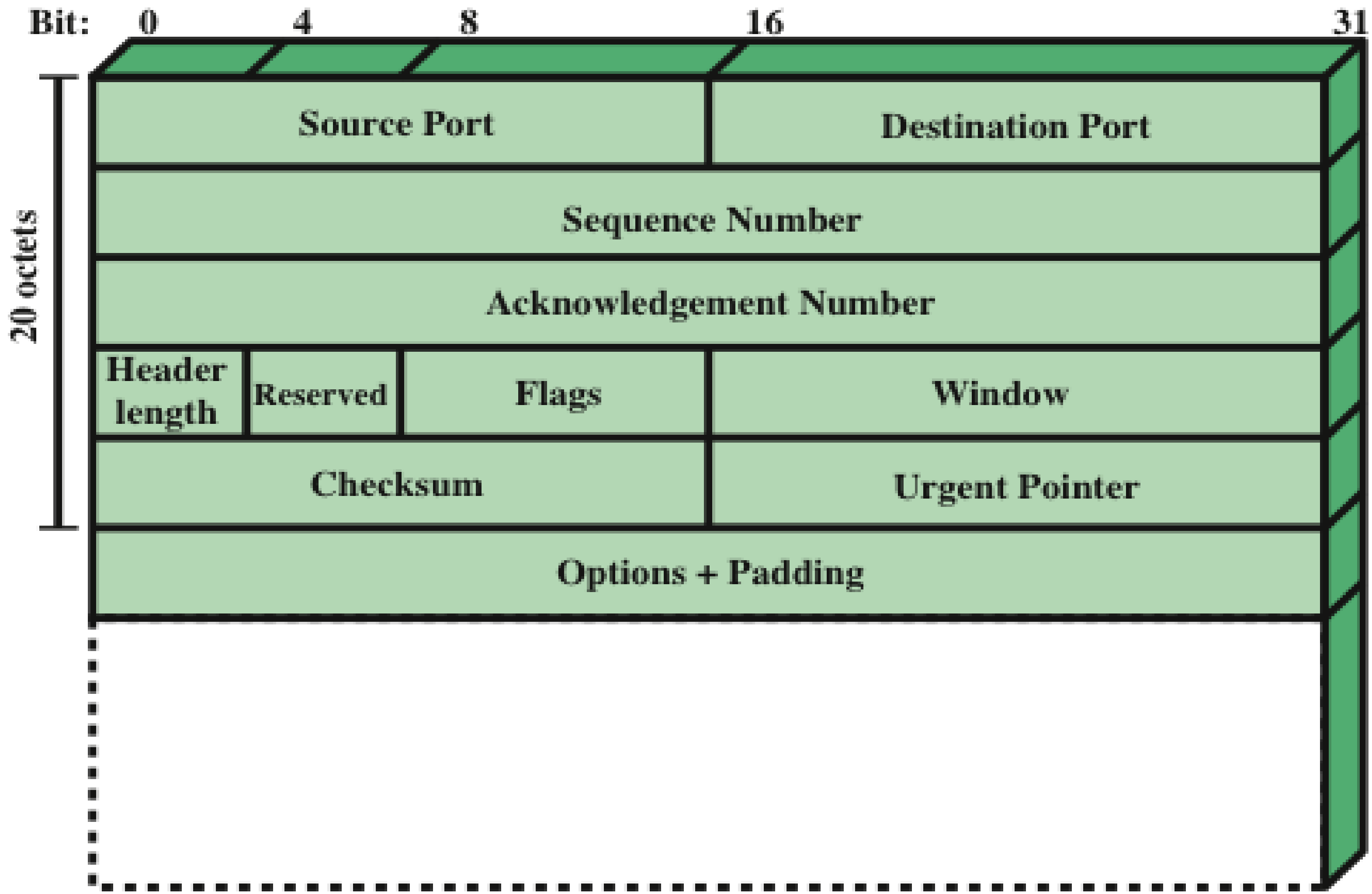


Figure 12.3 TCP Segment

Public Key Encryption

- The straightforward use of public-key encryption provides ***confidentiality*** ***but not authentication***
- To provide *both* ***confidentiality*** and ***authentication***, A can **encrypt M first using its private key** which provides the digital signature, and **then using B's public key**, which provides confidentiality
- ***Disadvantage*** is that the public-key algorithm must be exercised ***four times*** rather than two in each communication

Basic Uses of MAC

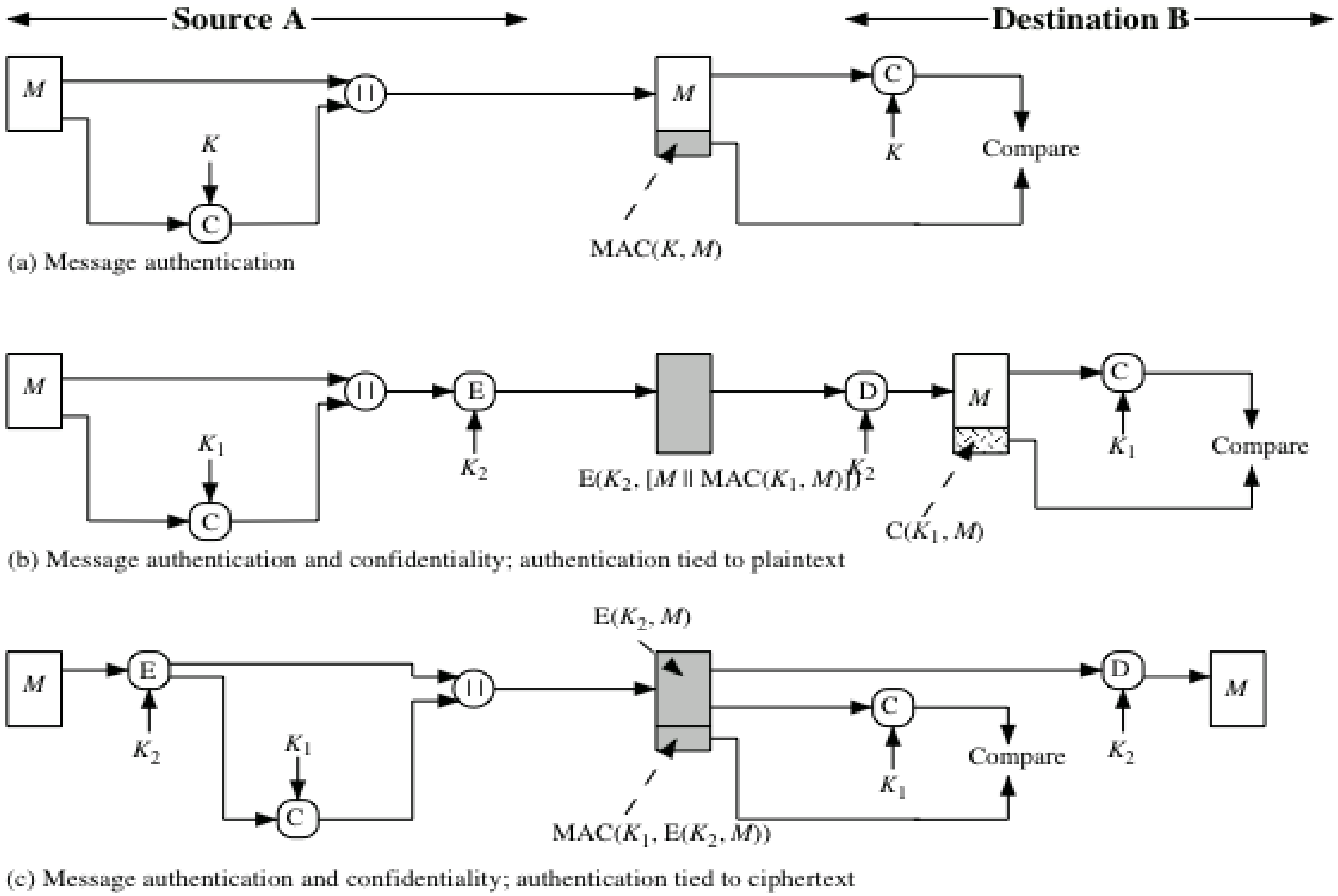


Figure 12.4 Basic Uses of Message Authentication Code (MAC)

Requirements for MAC

Taking into account the types of attacks, the MAC needs to satisfy the following:

The first requirement deals with message replacement attacks, in which an opponent is able to construct a new message to match a given MAC, even though the opponent does not know and does not learn the key

The second requirement deals with the need to thwart a brute-force attack based on chosen plaintext

The final requirement dictates that the authentication algorithm should not be weaker with respect to certain parts or bits of the message than others

Brute-Force Attacks

- Requires known message-tag pairs
  - A brute-force method of finding a collision is to pick a random bit string *y* and check if H(*y*) = H(*x*)

Two lines of attack:

- Attack the key space
  - If an attacker can determine the MAC key then it is possible to generate a valid MAC value for any input *x*
- Attack the MAC value
  - Objective is to generate a valid tag for a given message or to find a message that matches a given tag

Cryptanalysis

- Cryptanalytic attacks seek to exploit some property of the algorithm to perform some attack other than an exhaustive search

- An ideal MAC algorithm will require a cryptanalytic effort greater than or equal to the brute-force effort

- There is much more variety in the structure of MACs than in hash functions, so it is difficult to generalize about the cryptanalysis of MACs

MACs based on Hash Functions: 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)

Summary

- Message Authentication Requirements
- Message Authentication Functions
- Basic Use of MACs
- MACs based on Hash Functions: HMAC

References

1. Cryptography and Network Security, Principles and Practice, William Stallings, Prentice Hall, Sixth Edition, 2013