Chương III

3

TOÀN VẸN DỮ LIỆU

PHẦN II: MÃ XÁC THỰC THÔNG ĐIỆP

(MESSAGE AUTHENTICATION CODES)

Nội dung chính

1. Khái niệm toàn vẹn và xác thực thông điệp

2. MAC (Message Authentication Code)

3. Thảo luận vài cơ chế MAC
   - Nested MAC
   - HMAC
   - CMAC

(*Cryptography & Network Security*. McGraw-Hill, Inc., 2007., Chapter 11)

Mục tiêu

- Khái niệm về toàn vẹn và xác thực thông điệp
  - Toàn vẹn là gì
  - Phương pháp nhận diện dữ liệu không toàn vẹn
  - Mục tiêu của MAC; Các phương pháp để xác thực thông điệp
- Tìm hiểu về MAC
  - Mô hình tổng quát MAC
  - Bảo mật MAC
  - Đặc tính của MAC
  - Yêu cầu đối với MAC
  - An toàn của MAC

Mục tiêu

- Thảo luận về và cơ chế MAC
  - Nested MAC
  - Keyed Hash Function
  - HMAC
  - CMAC

1. Khái niệm xác thực thông điệp

1.1 Toàn vẹn thông điệp
(Message Integrity)

1.2 Xác thực thông điệp
(Message Authentication)

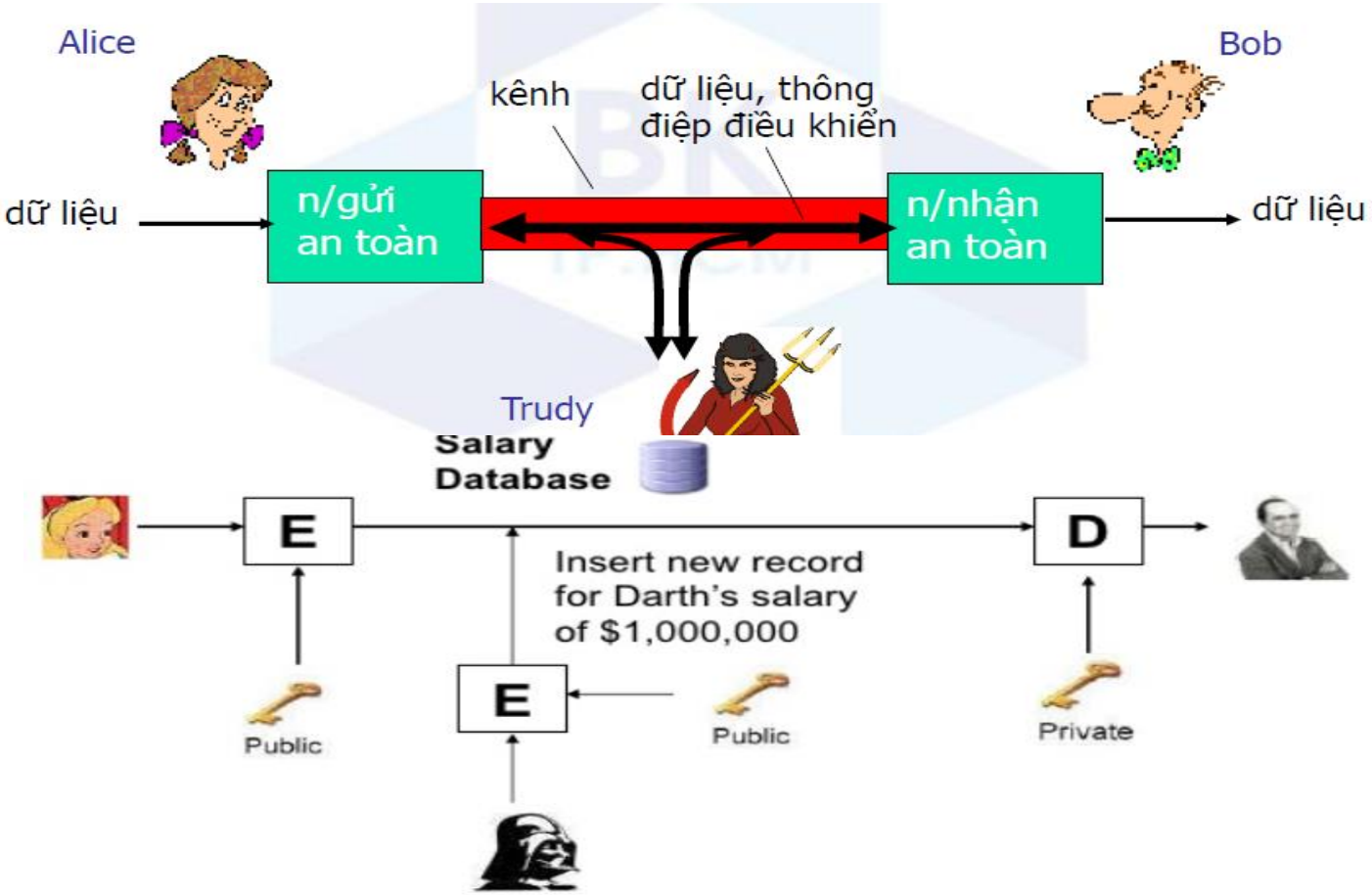
Integrity Message

Tính toàn vẹn thông điệp:

- Cho phép các bên liên lạc xác minh rằng các tin nhắn nhận được được xác thực.
  - Nội dung thông điệp chưa bị thay đổi
  - Nguồn của thông điệp tin cậy
  - Thông điệp chưa bị phát lại
  - Thông điệp được xác minh đúng thời điểm
  - Sự liên tục của thông điệp được duy trì

1.1 Integrity Message

- Đối phương insert/modify/delete nội dung thông điệp



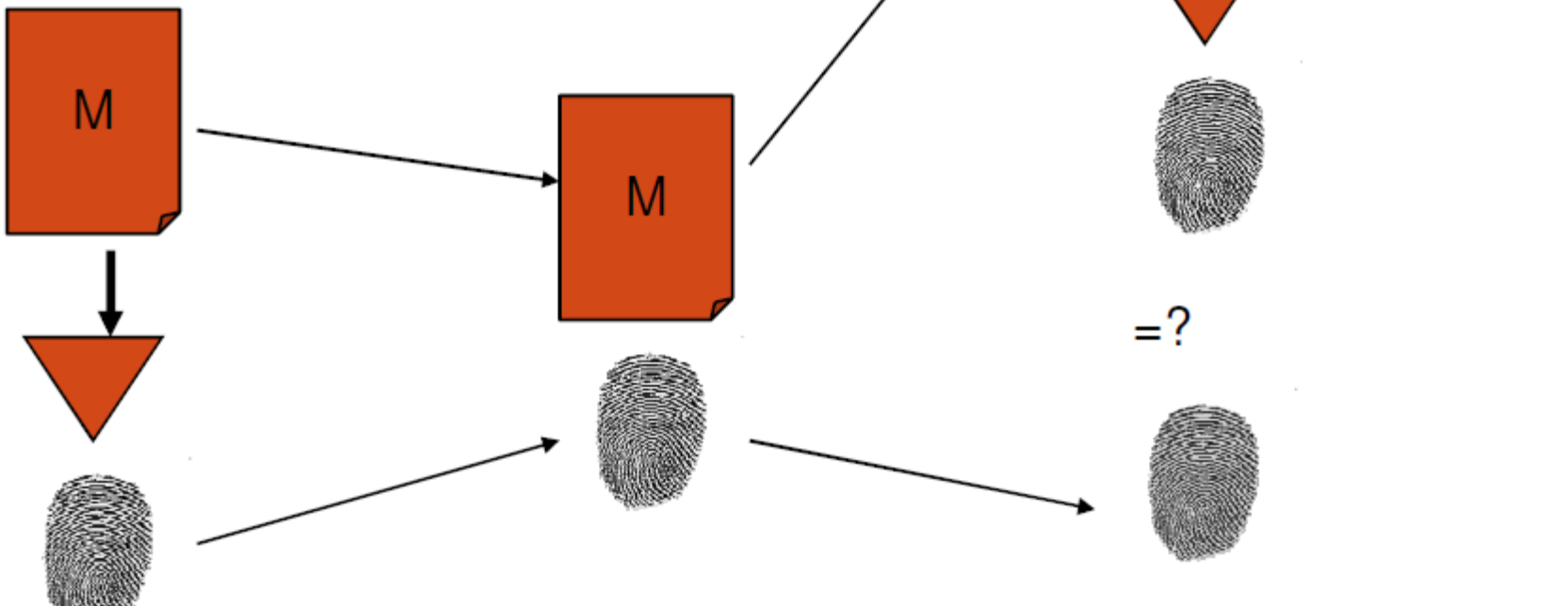
1.1 Integrity Message

Chuyển $100 cho TK 123-456-789

Chuyển $5000 cho TK 123-456-789

1.1 Integrity Message

- Gởi
  - Gởi đính kèm theo thông điệp một bảm băm của nó
- Nhận
  - Băm thông điệp và so sánh với bảm băm đi kèm



1.1 Integrity Message

Chuyển $100 cho TK 123-456-789

Chuyển $5000 cho TK 123-456-789