Trường Đại Học Công Nghệ Thông Tin
Khoa Mạng Máy Tính và Truyền Thông

AN TOÀN MẠNG MÁY TÍNH

ThS. Tô Nguyễn Nhật Quang

NỘI DUNG MÔN HỌC

1. Tổng quan về an ninh mạng
2. Các phần mềm gây hại
3. Các giải thuật mã hoá dữ liệu
4. Mã hoá khoá công khai và quản lý khoá
5. Chứng thực dữ liệu
6. Một số giao thức bảo mật mạng
7. Bảo mật mạng không dây
8. Bảo mật mạng vành đai
9. Tìm kiếm phát hiện xâm nhập

BÀI 5

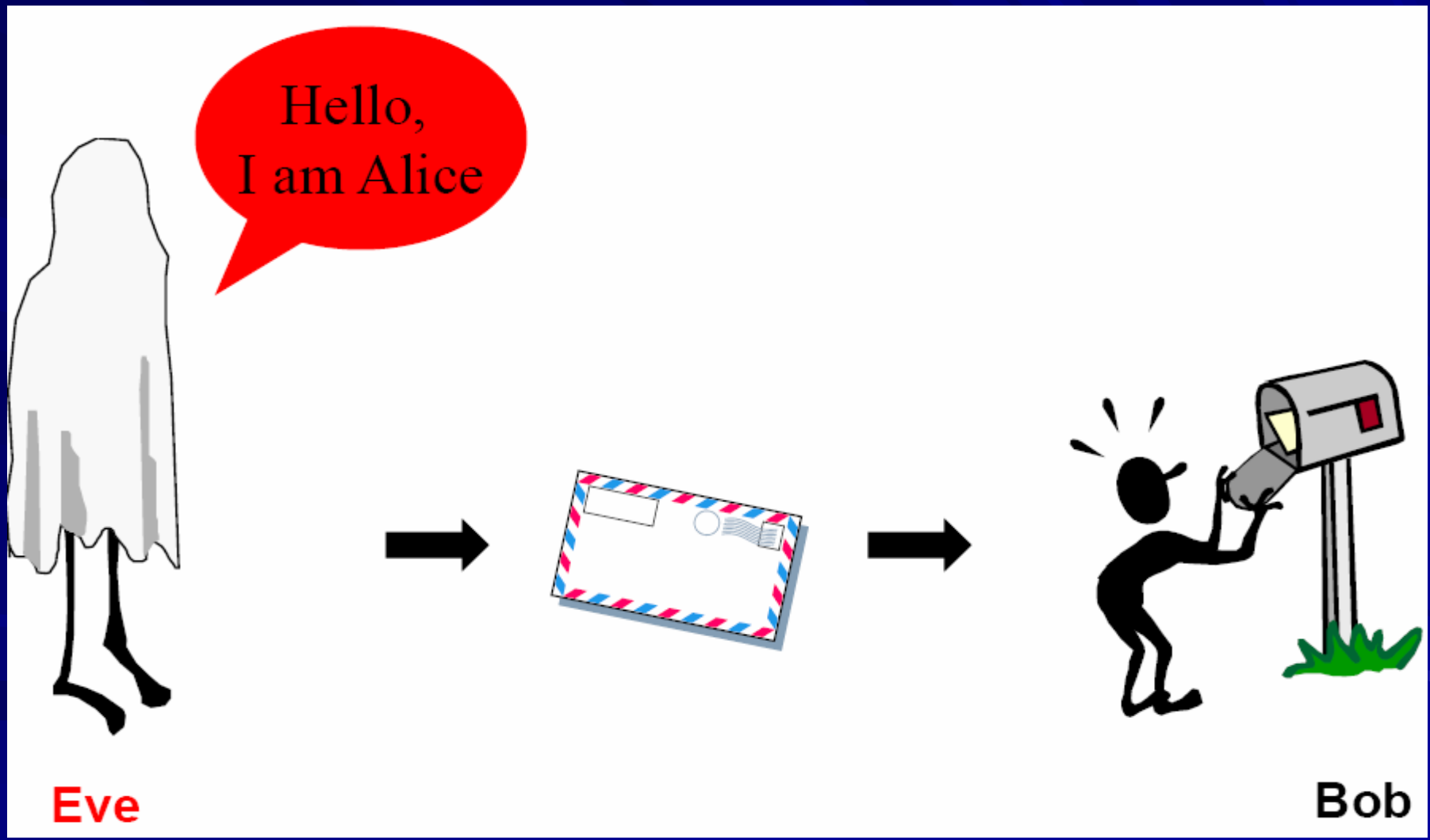
CHỨNG THỰC DỮ LIỆU

NỘI DUNG BÀI HỌC

1. Mở đầu
2. Mã chứng thực thông điệp
3. Hàm băm
4. Chữ ký số
5. Bài tập

1. Mở đầu

Vai trò của chứng thực



1. Mở đầu

Vai trò của chứng thực

- Chứng thực (xác thực, xác nhận - authentication) nhằm:
  - Xác nhận nguồn gốc của dữ liệu.
  - Thuyết phục người sử dùng là dữ liệu này chưa bị sửa đổi hoặc giả mạo.
- Chứng thực dữ liệu là cơ chế quan trọng để duy trì tính toàn vẹn và không thể từ chối của dữ liệu.

1. Mở đầu

Các phương pháp chứng thực

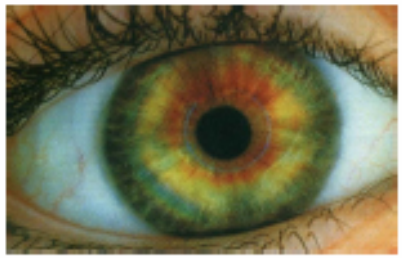
- Việc chứng thực được thực hiện với các phương pháp:
  - Mã hoá thông điệp: sử dụng mật mã hoá khoá bí mật hoặc mật mã hoá khoá công khai để mã hoá thông điệp rõ thành mật mã.
  - Mã chứng thực thông điệp (MAC – Message Authentication Code): một hàm và một khoá bí mật tạo ra một giá trị có chiều dài cố định sử dụng để chứng thực.
  - Hàm băm (Hash Function): một hàm ánh xạ một thông điệp có chiều dài bất kỳ vào một giá trị băm có chiều dài cố định sử dụng để chứng thực.

1. Mở đầu

Chứng thực thông qua nhận dạng

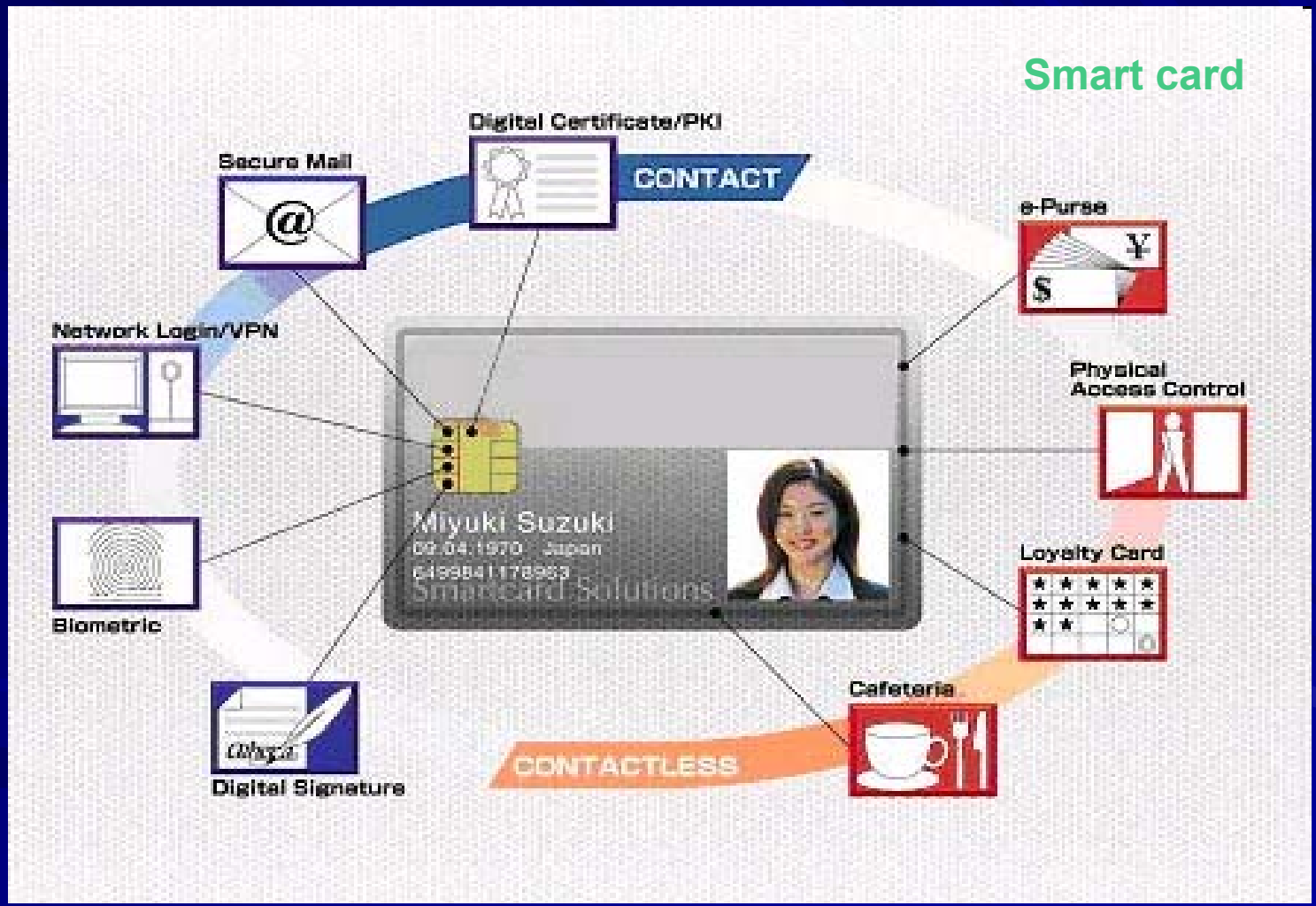
- Việc nhận dạng dựa trên một hoặc nhiều yếu tố:
  - Password, PIN
  - Smart card
  - Biometric: vân tay, võng mạc…
  - Chữ ký
  - …

ert5^r$#89Oy



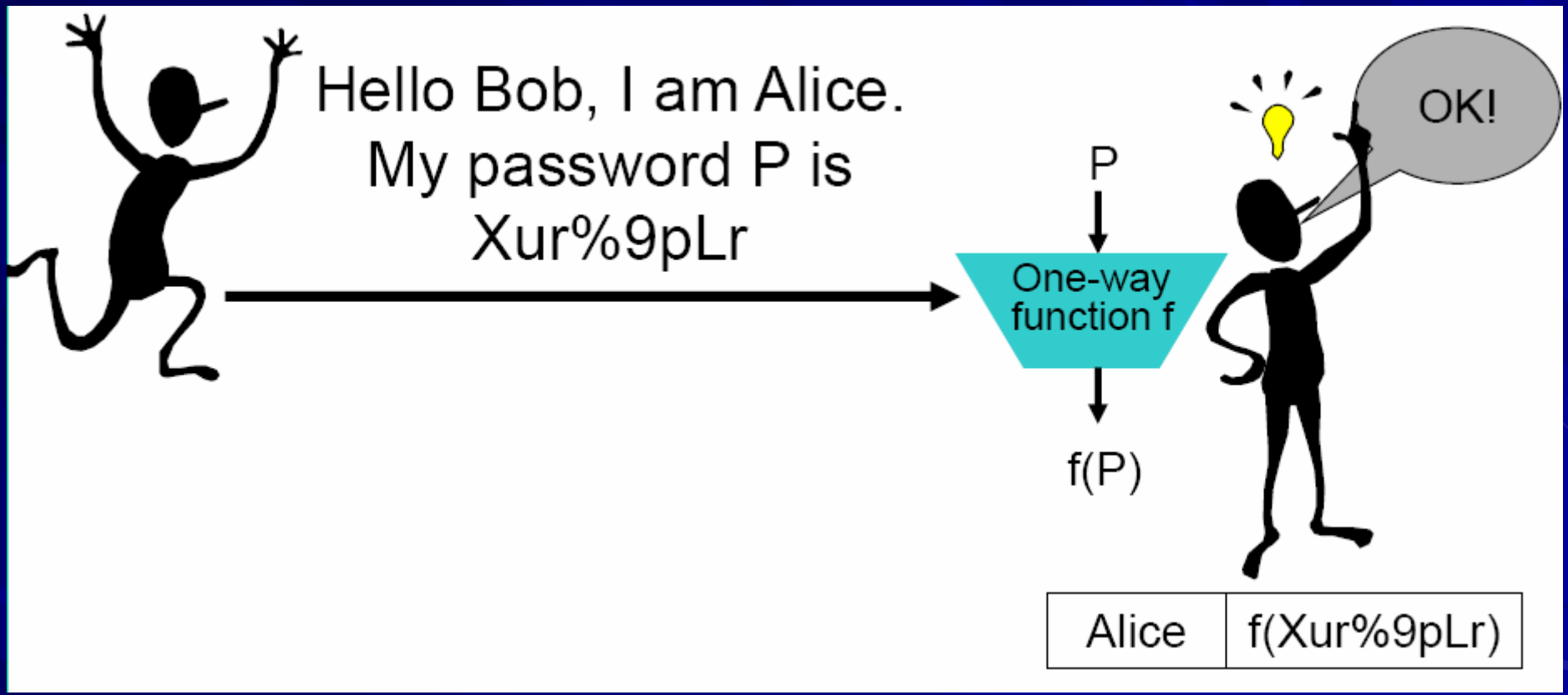
1. Mở đầu

Chứng thực thông qua nhận dạng



1. Mở đầu

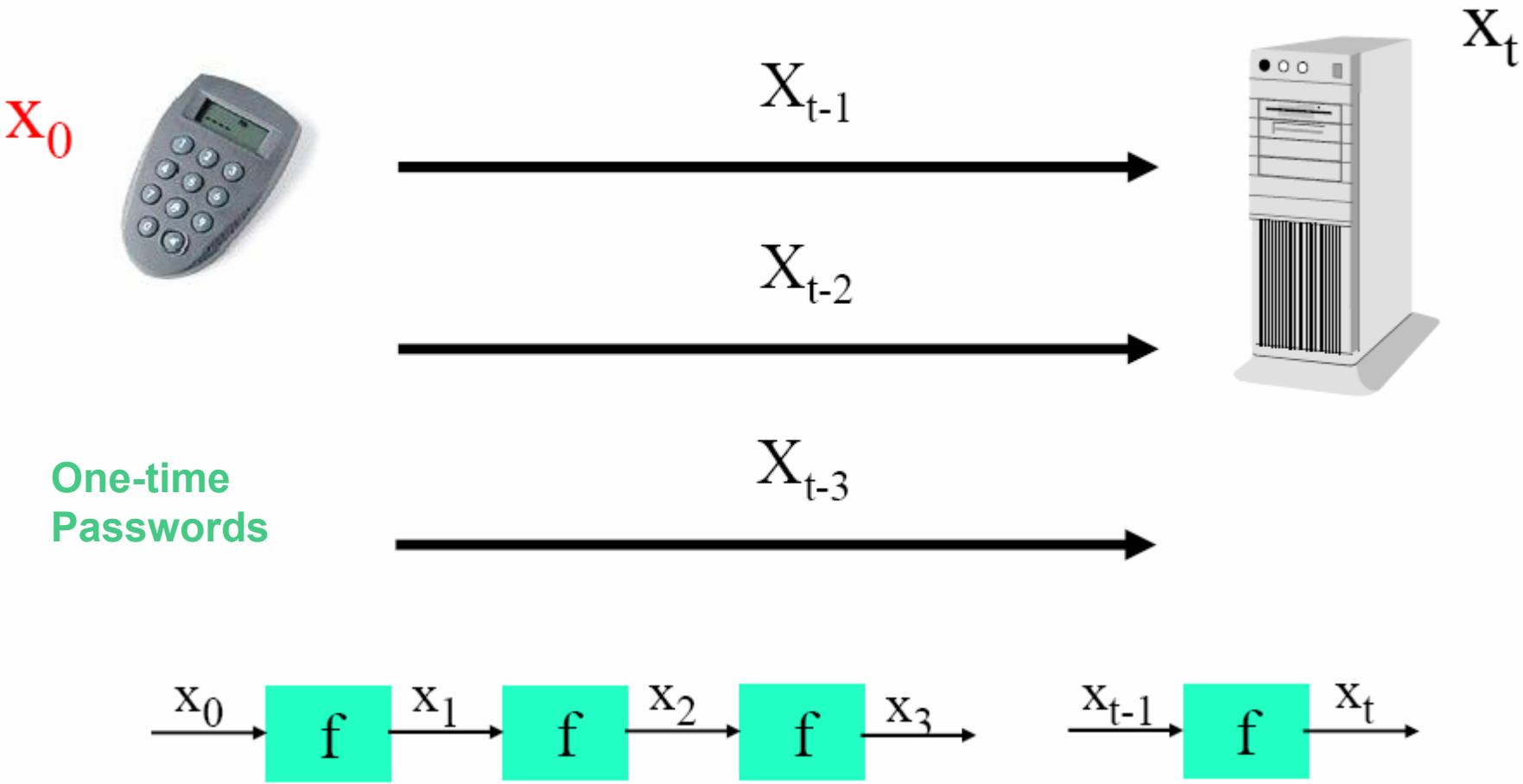
Chứng thực thông qua nhận dạng



1. Mở đầu

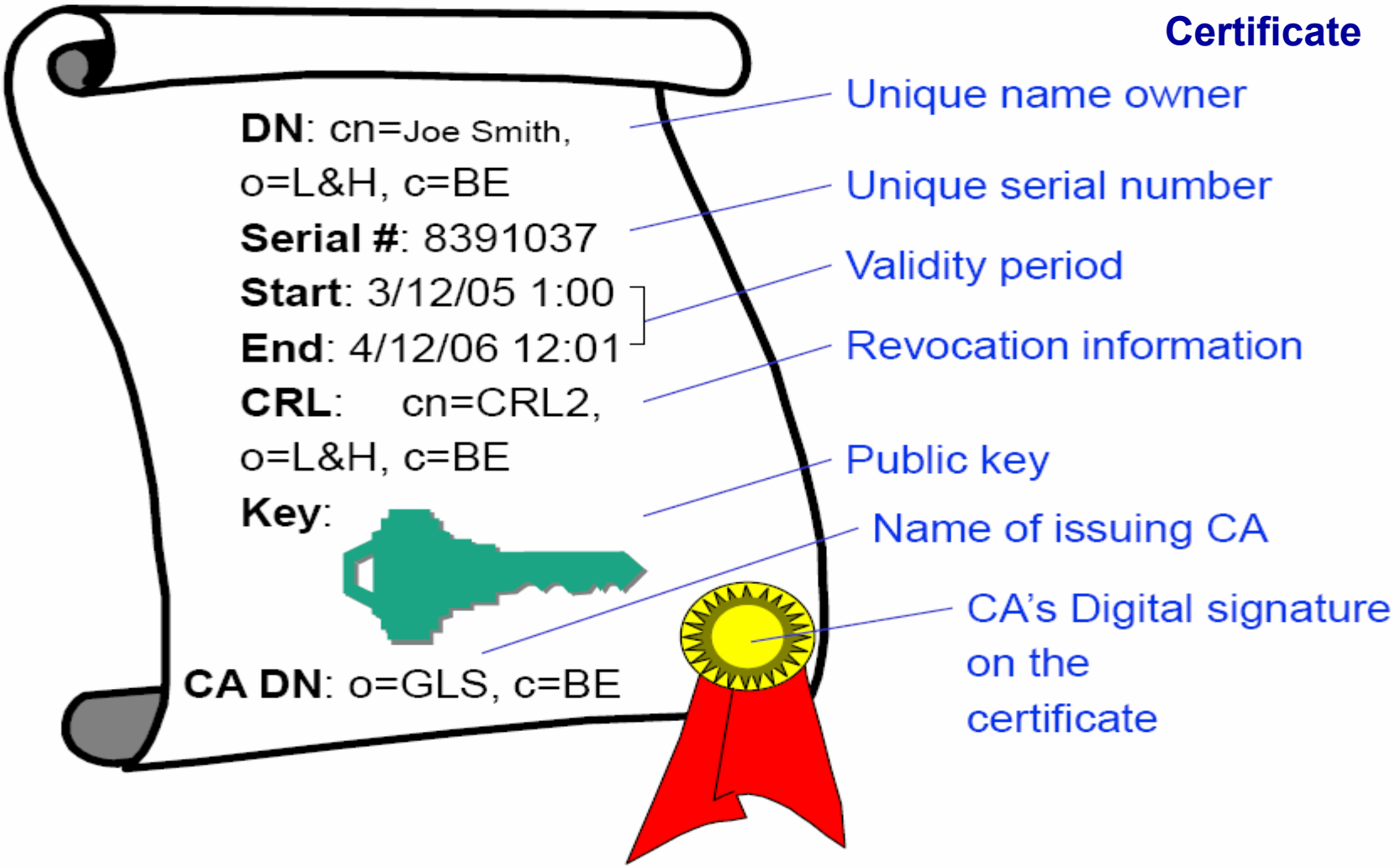
Chứng thực thông qua nhận dạng

iterated one-way function



1. Mở đầu

Chứng thực thông qua nhận dạng



1. Mở đầu
Ví dụ

- Giả sử Alice và Bob chia sẻ một khoá bí mật chung K. Alice muốn gởi một chuỗi dữ liệu M cho Bob và thuyết phục Bob rằng M thực sự đến từ Alice và không bị sửa trong quá trình truyền. Điều này có thể thực hiện như sau:
  - Alice gởi M cùng với C cho Bob, với $C=E_K(M)$ và E là một giải thuật mã hoá thông thường đã quy ước trước giữa Alice và Bob.
  - Do chỉ có Alice và Bob biết K, Bob có thể sử dụng K để giải mã C thu được M'.
  - Bob sẽ được thuyết phục rằng M thực sự đến từ Alice và M không bị thay đổi trong quá trình truyền nếu và chỉ nếu M'=M.

1. Mở đầu

Ví dụ

– Tuy nhiên, phương pháp này cho phép Alice có thể từ chối Charlie rằng M xuất phát từ Alice vì M có khả năng xuất phát từ Bob do cùng chia sẻ khoá bí mật K.

→ Nhược điểm này được giải quyết bằng mật mã hoá khoá công khai.

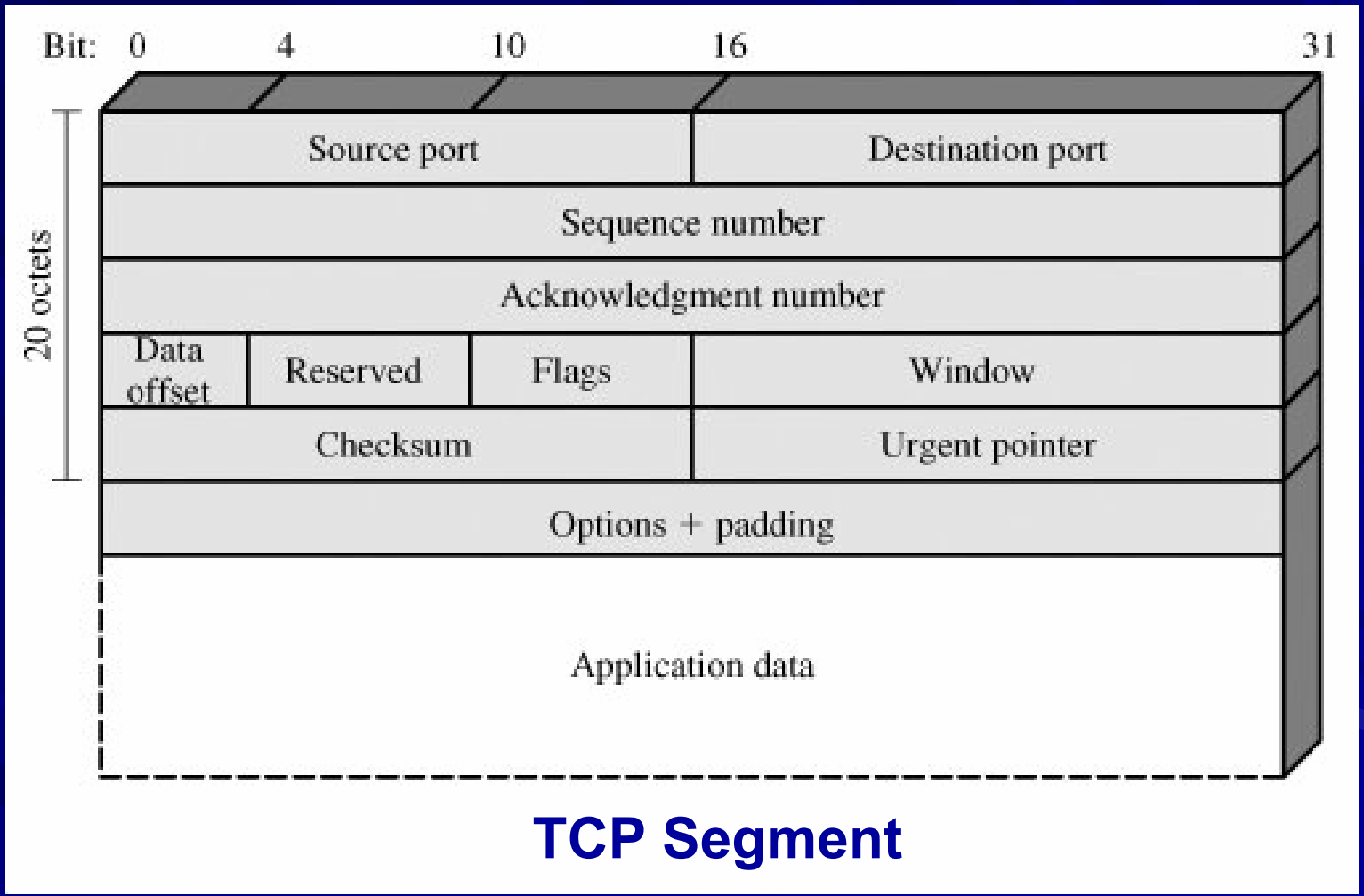
– Nếu chuỗi M ngắn, có thể mã hóa M trực tiếp để xác nhận nó.

– Nếu chuỗi M dài, chỉ cần tính toán một h ngắn đại diện cho M và mã hóa h.

1. Mở đầu
Ví dụ

- h được tạo ra mà không sử dụng khoá bí mật được gọi là digital digest hoặc digital fingerprint (dấu vân tay kỹ thuật số), có thể thu được từ một hàm băm (Hash Function).
- h được tạo ra bằng cách sử dụng một khoá bí mật được gọi là một mã xác thực thông điệp (MAC – Message Authentication Code).
- h cũng có thể thu được bằng cách sử dụng giải thuật checksum. Kết hợp một hàm băm và giải thuật checksum để tạo ra một mã xác thực tin nhắn keyed-hash (HMAC, Keyed-Hash Message Authentication Code).

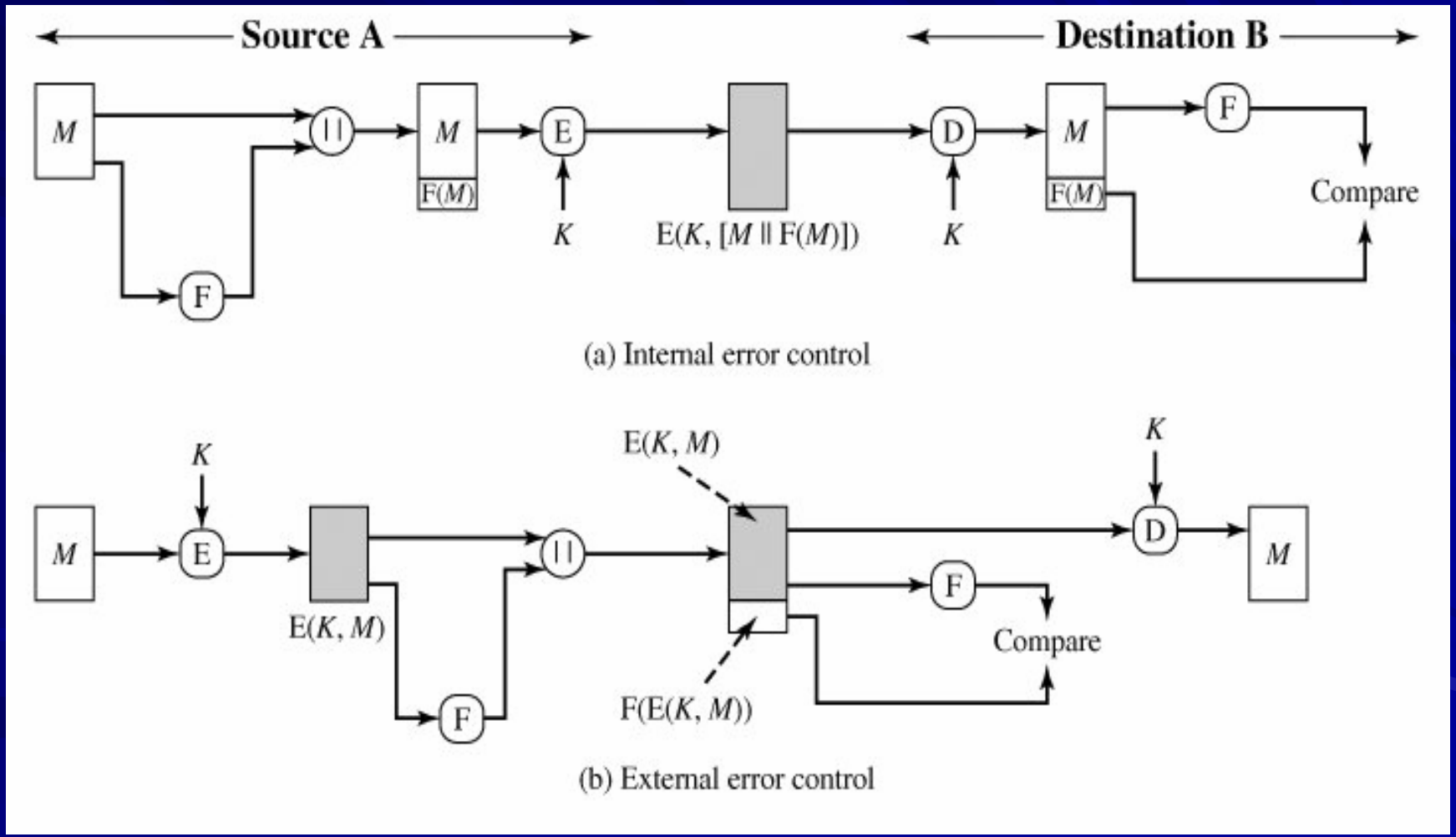
1. Mở đầu
Checksum của gói TCP



TCP Segment

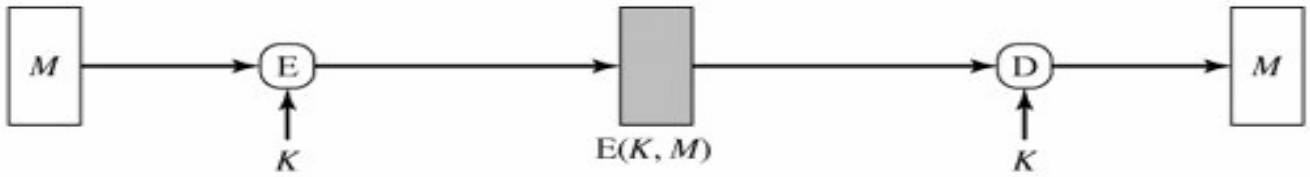
1. Mở đầu

Điều khiển lỗi khi gởi thông điệp

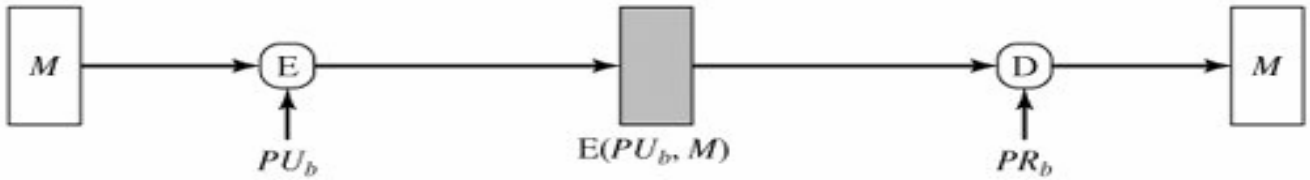


1. Mở đầu

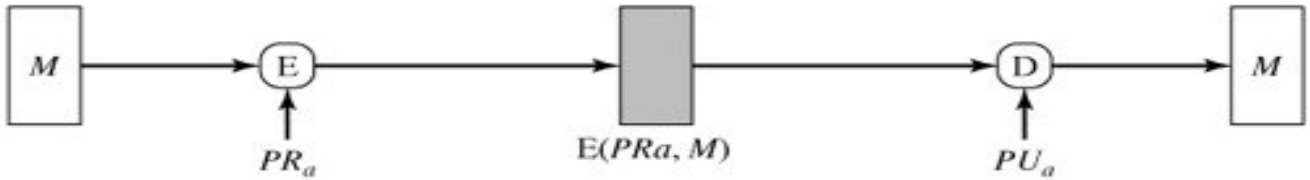
Những công dụng cơ bản của mã hoá thông điệp



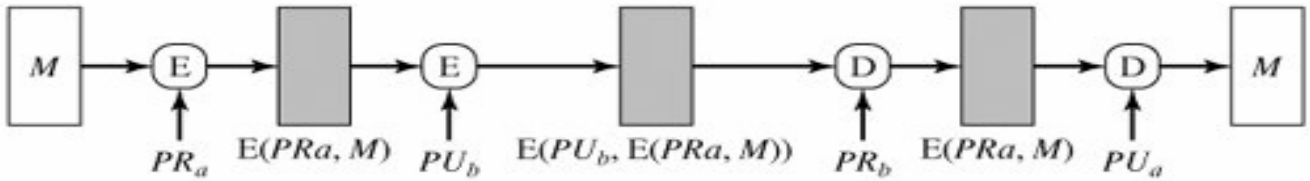
(a) Symmetric encryption: confidentiality and authentication



(b) Public-key encryption: confidentiality



(c) Public-key encryption: authentication and signature



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

1. Mở đầu

Những công dụng cơ bản của mã hoá thông điệp

a. Mã hoá khoá đối xứng (khoá bí mật):

A $\rightarrow$ B: E(K, M)

- Bảo mật: chỉ A và B chia sẻ K
- Chứng thực:
  - Có thể đến chỉ từ A
  - Không thay đổi trong quá trình truyền
  - Yêu cầu một số định dạng và dự phòng
- Không cung cấp chữ ký
  - Người nhận có thể giả mạo thông điệp
  - Người gởi có thể phủ nhận đã gởi thông điệp

1. Mở đầu

Những công dụng cơ bản của mã hoá thông điệp

b. Mã hoá khoá bất đối xứng (khoá công khai)

A $\rightarrow$ B: E(PU_b, M)

- Bảo mật
  - Chỉ B có PR_b giải mã
- Không cung cấp chứng thực
  - Bất cứ ai cũng có thể sử dụng PU_b để mã hoá thông điệp và tự xưng là A.

1. Mở đầu

Những công dụng cơ bản của mã hoá thông điệp

c. Mã hoá khoá công khai: chứng thực và chữ ký số

A $\rightarrow$ B: E(PR_a, M)

- Cung cấp chứng thực và chữ ký số
  - Chỉ A có PR_b để mã hoá
  - Không bị thay đổi trong quá trình truyền
  - Yêu cầu một số định dạng và dự phòng
  - Bất kỳ ai cũng có thể sử dụng PU_A để xác minh chữ ký số

1. Mở đầu

Những công dụng cơ bản của mã hoá thông điệp

d. Mã hoá khoá công khai: bảo mật, chứng thực, và chữ ký số

A $\rightarrow$ B: E(PU_b, E(PR_a, M))

- Cung cấp bảo mật nhờ PU_b.
- Cung cấp chứng thực và chữ ký số nhờ PR_a.

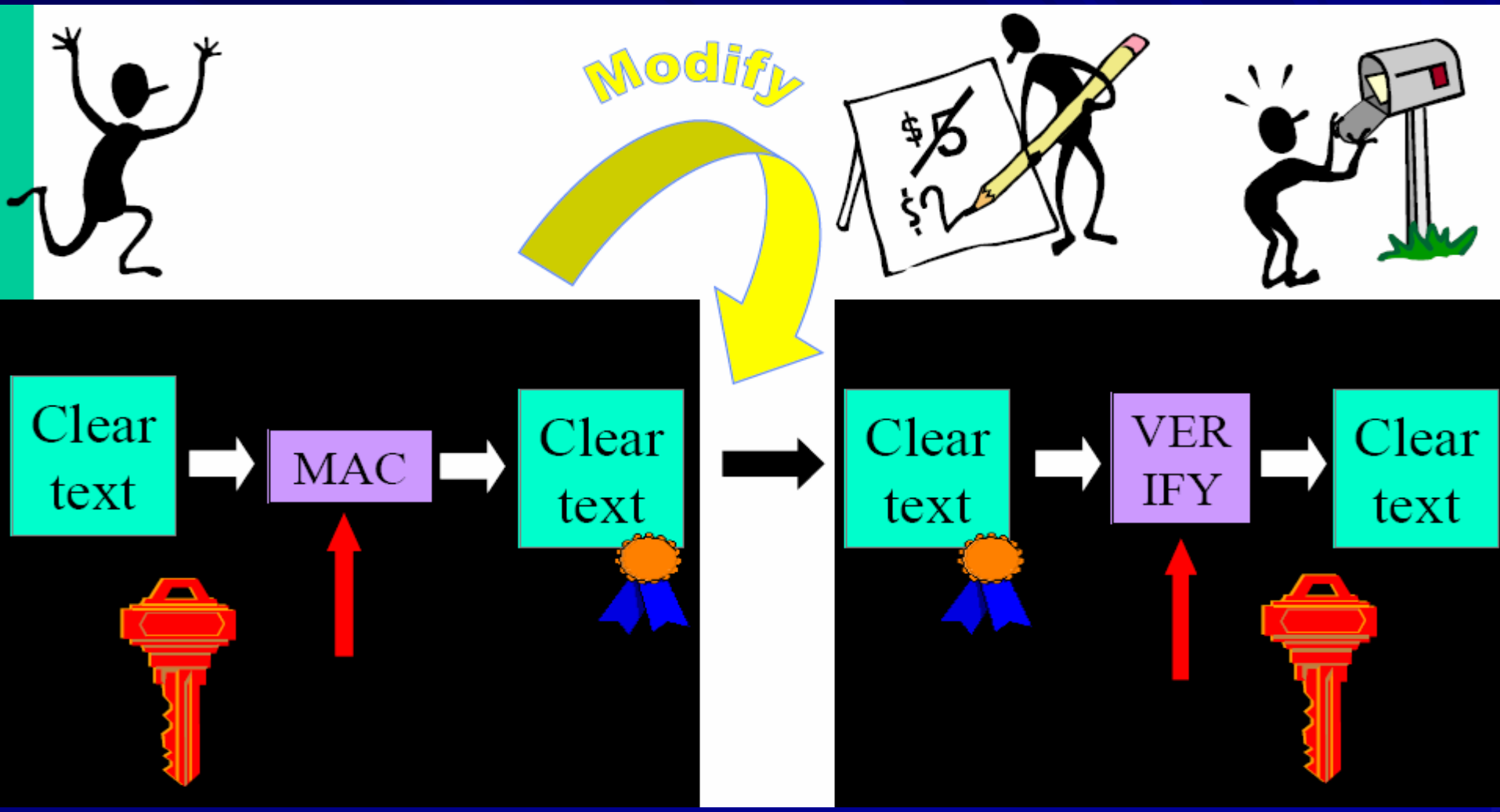
2. Mã chứng thực thông điệp (MAC)

Khái niệm

- Là một kỹ thuật chứng thực liên quan đến việc sử dụng một khoá bí mật để tạo ra một khối dữ liệu có kích thước nhỏ cố định (checksum hoặc MAC) và được thêm vào thông điệp.
- Kỹ thuật này giả sử rằng 2 phía tham gia truyền thông là A và B chia sẻ một khoá bí mật K. Khi A có một thông điệp gởi đến B, A sẽ tính toán MAC như là một hàm của thông điệp và khoá: MAC=C(K, M), với
  - M: thông điệp đầu vào có kích thước biến đổi
  - C: hàm MAC
  - K: khoá bí mật chia sẻ giữa người gởi và người nhận
  - MAC: mã chứng thực thông điệp có chiều dài cố định

2. Mã chứng thực thông điệp (MAC)

Khái niệm



2. Mã chứng thực thông điệp (MAC)

Khái niệm

- Thông điệp cộng với MAC được truyền tới người nhận. Người nhận thực hiện các tính toán tương tự trên các thông điệp đã nhận sử dụng cùng một khóa bí mật, để tạo ra một MAC mới.
- MAC vừa tạo sẽ được so với MAC nhận. Giả sử chỉ người nhận và người gửi biết khóa bí mật:
  - Nếu MAC nhận phù hợp với MAC vừa tính thì thông điệp không bị thay đổi trong quá trình truyền và chắc chắn được gởi tới từ người gởi đã biết.
  - Nếu MAC nhận khác với MAC vừa tính thì thông điệp đã bị thay đổi hoặc bị giả mạo và được gởi từ attacker.

2. Mã chứng thực thông điệp (MAC)

Khái niệm

- Chiều dài thông thường của MAC: 32..96 bit.

  $\rightarrow$ để tấn công cần thực hiện 2^n lần thử với n là chiều dài của MAC (bit).

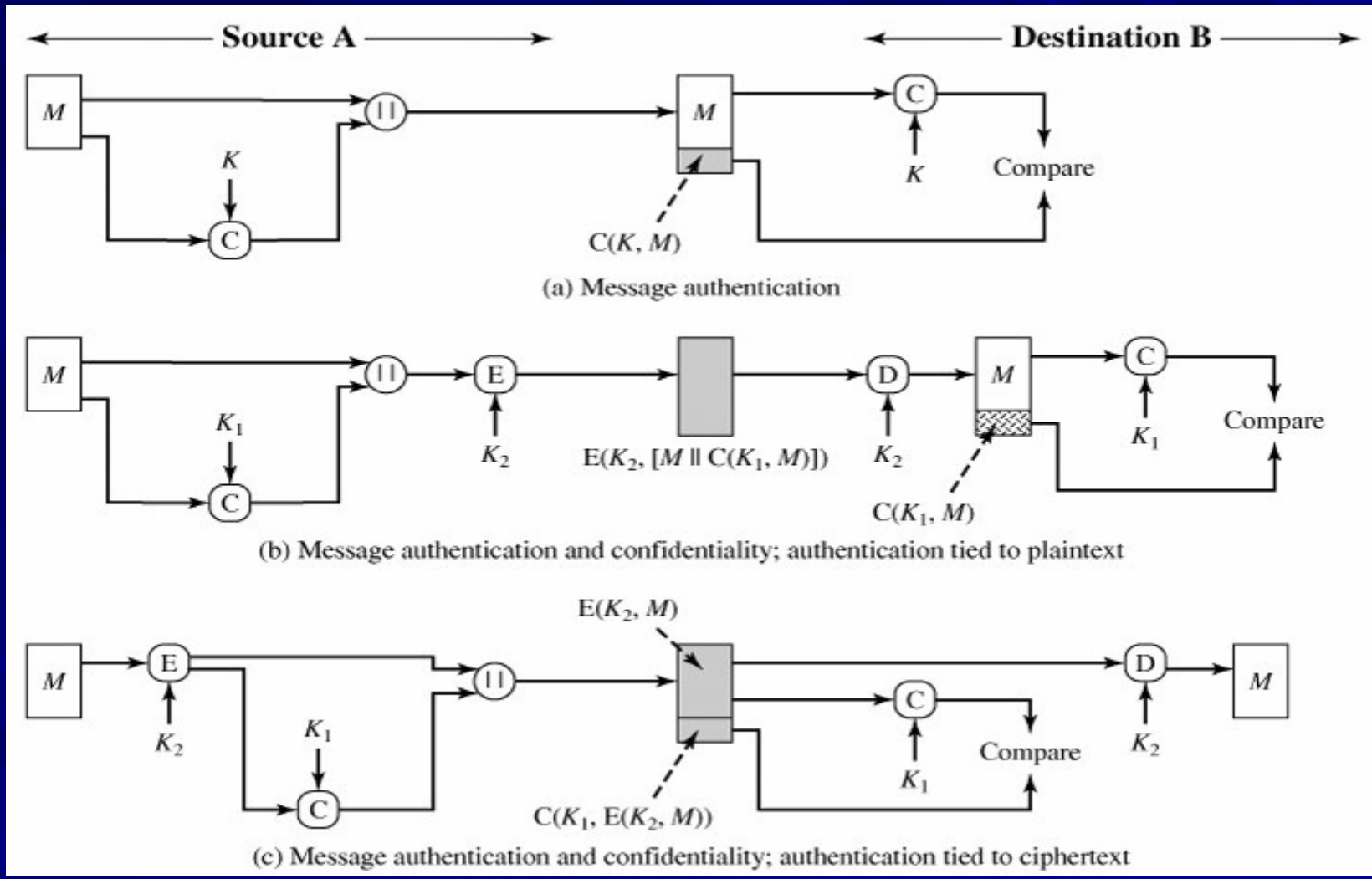
- Chiều dài thông thường của khoá K: 56..160 bit.

  $\rightarrow$ để tấn công cần thực hiện 2^k lần thử với k là chiều dài của khoá K (bit).

- Ứng dụng trong:
  - Banking: sử dụng MAC kết hợp triple-DES
  - Internet: sử dụng HMAC và MAC kết hợp AES

2. Mã chứng thực thông điệp (MAC)

Các công dụng cơ bản của MAC



2. Mã chứng thực thông điệp (MAC)

Các công dụng cơ bản của MAC

a. Chứng thực

$A \rightarrow B: M \,||\, C(K, M)$

- Chứng thực: chỉ A và B chia sẻ K

b. Chứng thực và bảo mật: chứng thực gắn liền với plaintext

$A \rightarrow B: E(K_2, [M \,||\, C(K, M)])$

- Chứng thực: chỉ A và B chia sẻ K_1
- Bảo mật: chỉ A và B chia sẻ K_2

c. Chứng thực và bảo mật: chứng thực gắn liền với ciphertext

$A \rightarrow B: E(K_2, M) \,||\, C(K_1, E(K_2, M))$

- Chứng thực: sử dụng K_1
- Bảo mật: sử dụng K_2

2. Mã chứng thực thông điệp (MAC)

Các yêu cầu đối với MAC

- Khi một thông điệp được mã hoá (để bảo mật) sử dụng mã hoá khoá bí mật hoặc khoá công khai, độ bảo mật thường phụ thuộc vào độ dài bit của khoá. Một cuộc tấn công brute-force phải sử dụng tất cả các khoá có thể. Trung bình cần mất $2^{(k-1)}$ lần thử cho một khoá k-bit.
- Thông thường, với một cuộc tấn công chỉ biết cyphertext C (P_i=D(K_i, C), cần phải thực hiện brute-force với tất cả các K_i cho đến khi nào P_i được tạo ra khớp với một plaintext chấp nhận được.

2. Mã chứng thực thông điệp (MAC)

Các yêu cầu đối với MAC

- Trường hợp của MAC có những khác biệt do MAC là hàm nhiều-một. Giả sử k>n (kích thước khoá lớn hơn kích thước MAC) và $MAC_1 = C(K, M_1)$, việc thám mã phải thực hiện $MAC_i = C(K_i, M_1)$ với tất cả các giá trị có thể của K_i. Ít nhất có một khoá đảm bảo $MAC_i = MAC_1$.
- Lưu ý rằng sẽ có 2^k MACs được tạo ra nhưng chỉ có $2^n < 2^k$ giá trị MAC khác nhau. Do đó, một số khoá sẽ tạo ra các MAC chính xác và attacker không có cách nào để biết được đó là khoá nào.
- Trung bình, có $2^k/2^n = 2^{(k-n)}$ khoá được tạo ra và attacker phải lặp đi lặp lại các cuộc tấn công.

2. Mã chứng thực thông điệp (MAC)

Các yêu cầu đối với MAC

- Vòng 1

  Cho: M_1, $MAC_1 = C(K, M_1)$

  Tính $MAC_i = C(K_i, M_1)$ đối với 2^k khoá

  Số lượng khớp $\approx 2^{(k-n)}$
- Vòng 2

  Cho: M_2, $MAC_2 = C(K, M_2)$

  Tính $MAC_i = C(K_i, M_2)$ đối với $2^{(k-n)}$ khoá kết quả từ Vòng 1

  Số lượng khớp $\approx 2^{(k-2n)}$

  .....

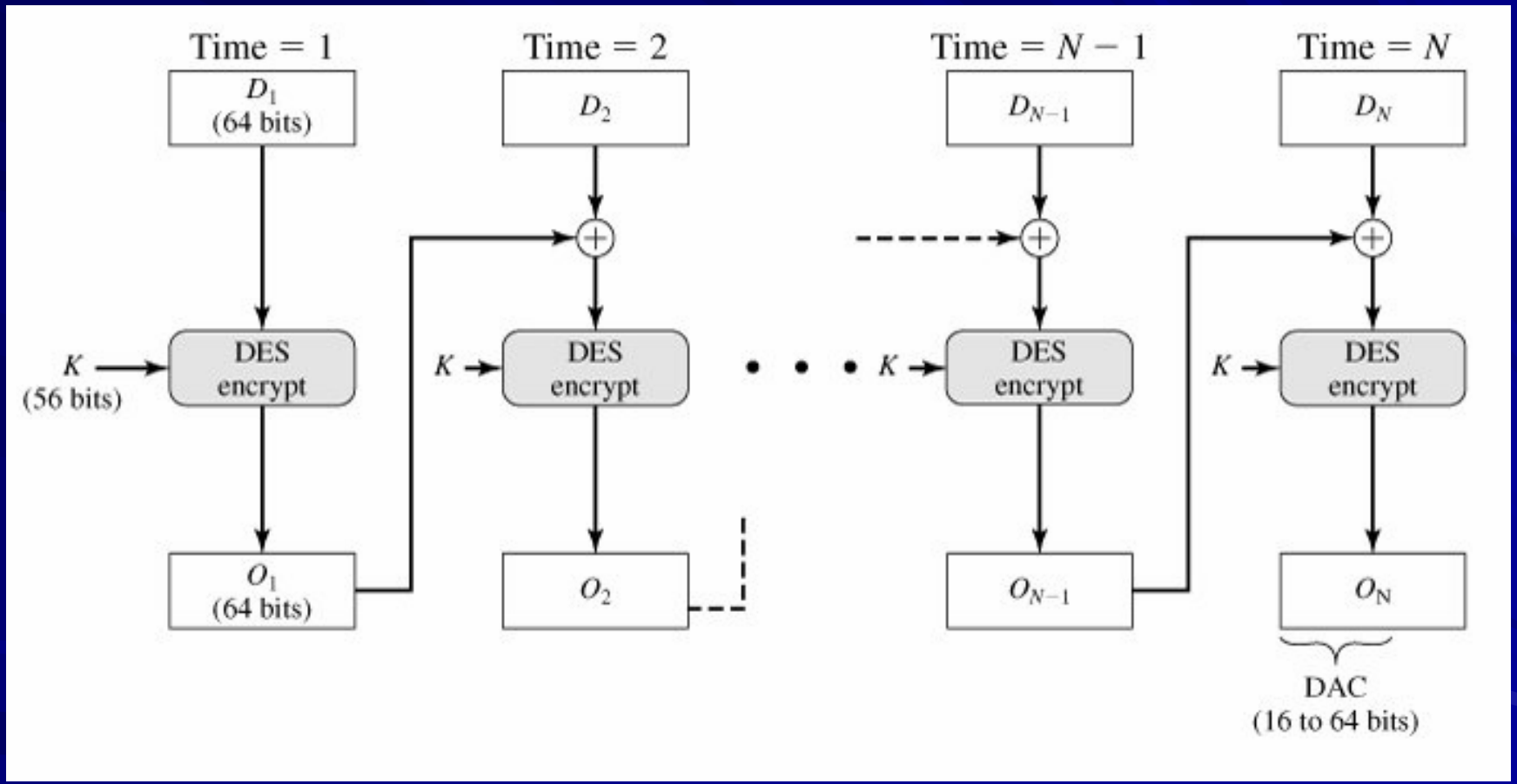
2. Mã chứng thực thông điệp (MAC)

Các yêu cầu đối với MAC

- Trung bình, α vòng sẽ cần thực hiện nếu k = α x n. Ví dụ, nếu một khoá 80 bit được sử dụng và MAC dài 32 bit.
  - Vòng đầu tiên sẽ tạo ra khoảng 2^{48} khoá có thể,
  - Vòng thứ hai sẽ tạo thu hẹp lại còn 2^{16} khả năng,
  - Vòng thứ ba sẽ tạo ra chỉ một khoá duy nhất, chính là khoá của người gởi.

2. Mã chứng thực thông điệp (MAC)

MAC dựa trên giải thuật mã hoá DES



3. Hàm băm

Khái niệm

- Một hàm băm nhận một chuỗi dài ở đầu vào, ngắt nó thành nhiều mảnh, trộn lẫn chúng và tạo ra một chuỗi mới với chiều dài ngắn.
- Không phải mọi hàm băm đều thích hợp cho việc tạo ra một dấu vân tay kỹ thuật số.
- Ví dụ:
  - Xét một hàm băm đơn giản $H_{\oplus}$ sử dụng toán tử XOR để biến đổi một chuỗi đầu vào có độ dài tuỳ ý để thu được một chuỗi 16 bit ở đầu ra.
  - Cho $M = M_1M_2\ldots M_k$, với mỗi M_i (có thể ngoại trừ khối M_k) là một chuỗi nhị phân 16 bit. Nếu M_k ngắn hơn 16 bit, thêm vào cuối một số bit 1 để được khối 16 bit.

3. Hàm băm

Khái niệm

Cho: $H_{\oplus}(M) = M_1 \oplus M2 \oplus \ldots \oplus M_k$.

– Hàm băm này không thích hợp để tạo ra dấu vân tay kỹ thuật số do có thể dễ dàng tìm được các chuỗi với nội dung khác nhau nhưng có cùng giá trị băm.

– Cho hai chuỗi khác nhau như sau:

- S_1: “He likes you but I hate you”
- S_2: “He hates you but I like you”

Mã hoá hai chuỗi này bằng cách sử dụng mã ASCII 8 bit và bỏ các khoảng trắng giữa các từ, ta sẽ thu được $H_{\oplus}(S_1) = H_{\oplus}(S_2)$.

→ Một hàm băm cần phải đáp ứng một số tiêu chuẩn cho trước mới có thể tạo ra dấu vân tay kỹ thuật số.

3. Hàm băm

Tiêu chuẩn xây dựng hàm băm

- Cho H là hàm băm được xây dựng.
- Trước tiên cần thiết lập cận trên Γ cho chiều dài của chuỗi input (là số rất lớn, đơn vị bit).
- γ là chiều dài cố định của chuỗi output ($\gamma < \Gamma$).
- Để sinh ra một dấu vân tay kỹ thuật số tốt, H cần phải có:
  - Thuộc tính một chiều (one-way property)
  - Thuộc tính duy nhất.
- Hàm băm này được gọi là một hàm băm mật mã (Cryptographic Hash Function – CHF).

3. Hàm băm

Tìm kiếm hàm băm

- Mặc dù đã có rất nhiều nỗ lực, người ta vẫn chưa thể xác định được có tồn tại một hàm băm thoả mãn tính chất một chiều và duy nhất hay không?
- Đã có nhiều hàm băm được xây dựng và sử dụng trong thực tế.
- Các hàm băm vẫn có thể chứa những lỗ hổng có thể được khai thác bởi kẻ tấn công.

  $\rightarrow$ Cần xác định các điểm yếu nhằm đưa ra các hàm băm mạnh hơn.

3. Hàm băm

Tìm kiếm hàm băm

- Năm 2004, nhà toán học Trung Quốc Xiaoyun Wang và cộng sự đã chứng minh rằng một số hàm băm được sử dụng rộng rãi lúc đó như MD4, MD5, HACAL-128, RIPEMD… là không đáp ứng tiêu chí kháng đụng độ.
- Năm 2005, họ cũng chứng minh rằng hàm băm sử dụng phổ biến là SHA-1 không kháng đụng độ mạnh như suy nghĩ của mọi người, và phát triển một phương pháp giúp tìm thấy hai chuỗi x và y khác nhau có cùng giá trị băm.

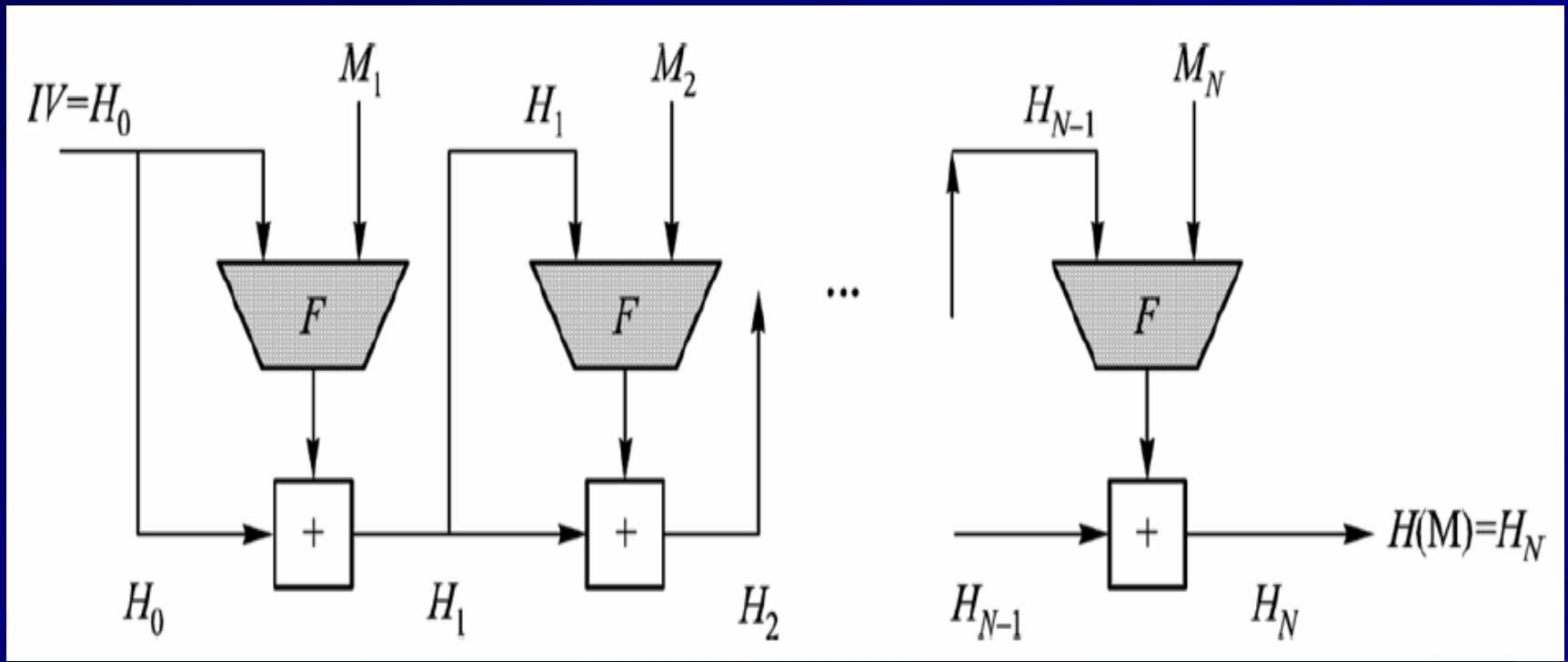
3. Hàm băm

Cấu trúc cơ bản của hàm băm chuẩn

- Các giải thuật băm MD5, Whirlpool, SHA-1, SHA-2… đều có cùng cấu trúc cơ bản được đề xuất bởi Ralph C. Merkle năm 1978.
- Trung tâm của cấu trúc cơ bản này là một hàm nén. Các giải thuật băm khác nhau sử dụng những hàm nén khác nhau.
- Trong cấu trúc cơ bản này, M là khối rõ, IV là một vector khởi tạo, F là một hàm nén, + là một số dạng của toán tử cộng modular.

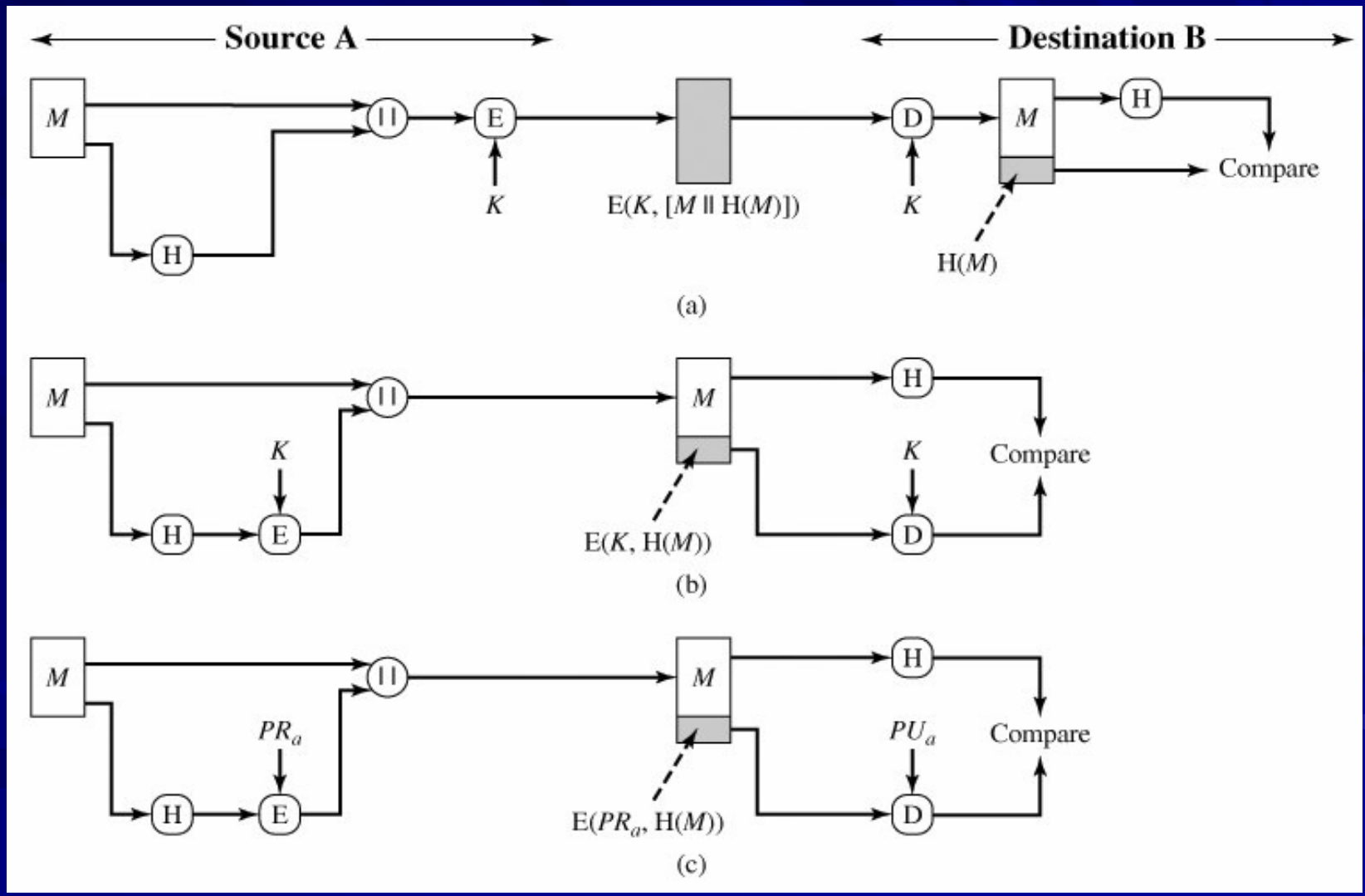
3. Hàm băm

Cấu trúc cơ bản của hàm băm chuẩn



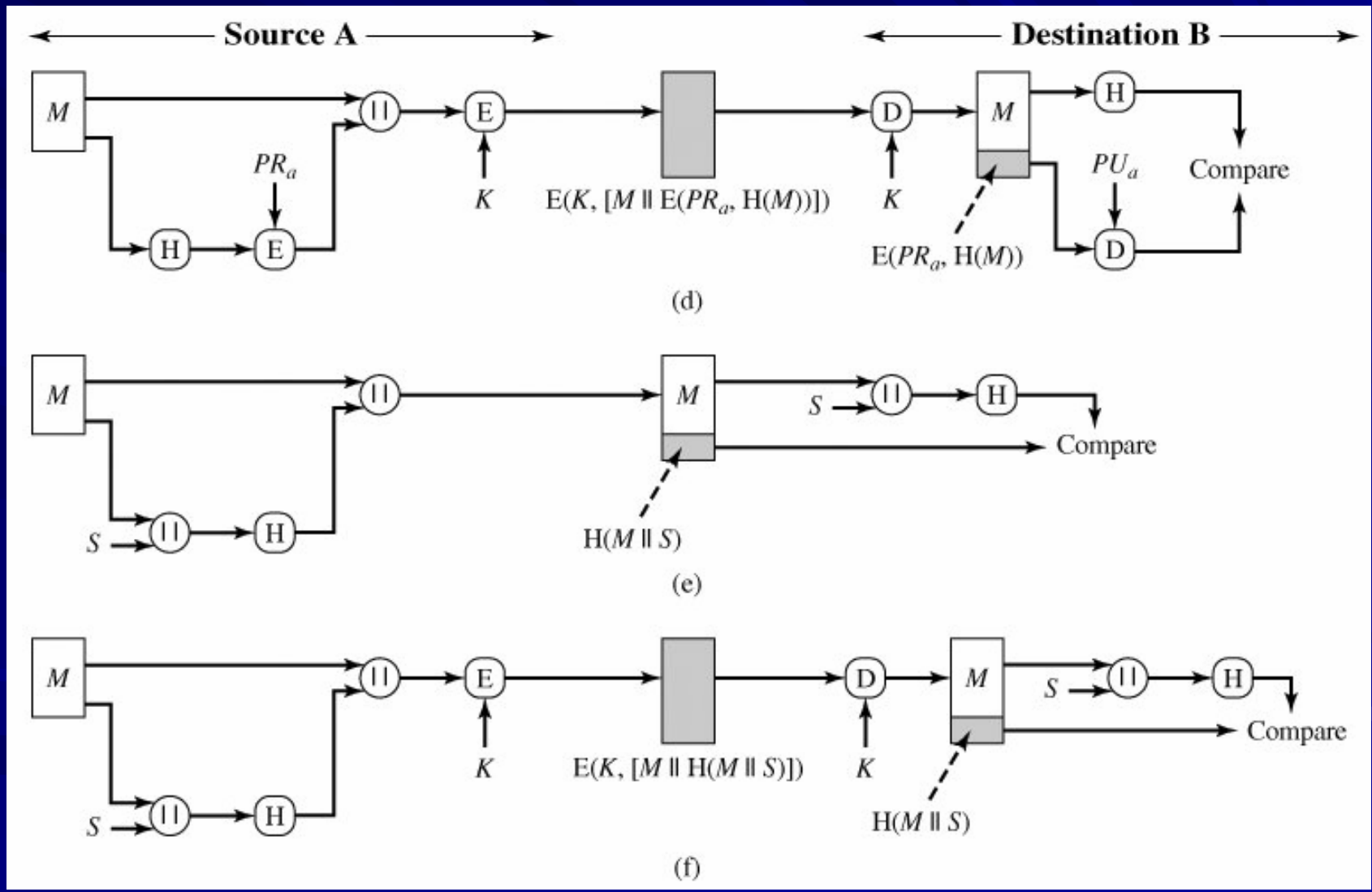
3. Hàm băm

Các công dụng cơ bản của hàm băm



3. Hàm băm

Các công dụng cơ bản của hàm băm



3. Hàm băm

Các công dụng cơ bản của hàm băm

a. **Mã hoá thông điệp cộng với mã băm**

A → B: E(K, [M || H(M)])

- Bảo mật: chỉ A và B chia sẻ K
- Chứng thực: H(M) được bảo vệ bằng mật mã

b. **Mã hoá mã băm chia sẻ với khoá bí mật**

A → B: M || E(K, H(M))

- Chứng thực: H(M) được bảo vệ bằng mật mã

c. **Mã hoá khoá bí mật với mã băm của người gởi**

A → B: M || E(PR_A, H(M))

- Chứng thực và chữ ký số:
  - H(M) được bảo vệ bằng mật mã
  - Chỉ A có thể tạo E(PR_A, H(M))

3. Hàm băm

Các công dụng cơ bản của hàm băm

d. Mã hoá kết quả của (c) với khoá bí mật chia sẻ

$A \rightarrow B$: $E(K, [M \,||\, E(PR_A, H(M))])$

- Bảo mật: chỉ A và B chia sẻ K
- Chứng thực và chữ ký số

e. Tính mã băm của thông điệp cộng với trị bí mật

$A \rightarrow B$: $M \,||\, H(M \,||\, S)$

- Chứng thực: chỉ A và B chia sẻ S

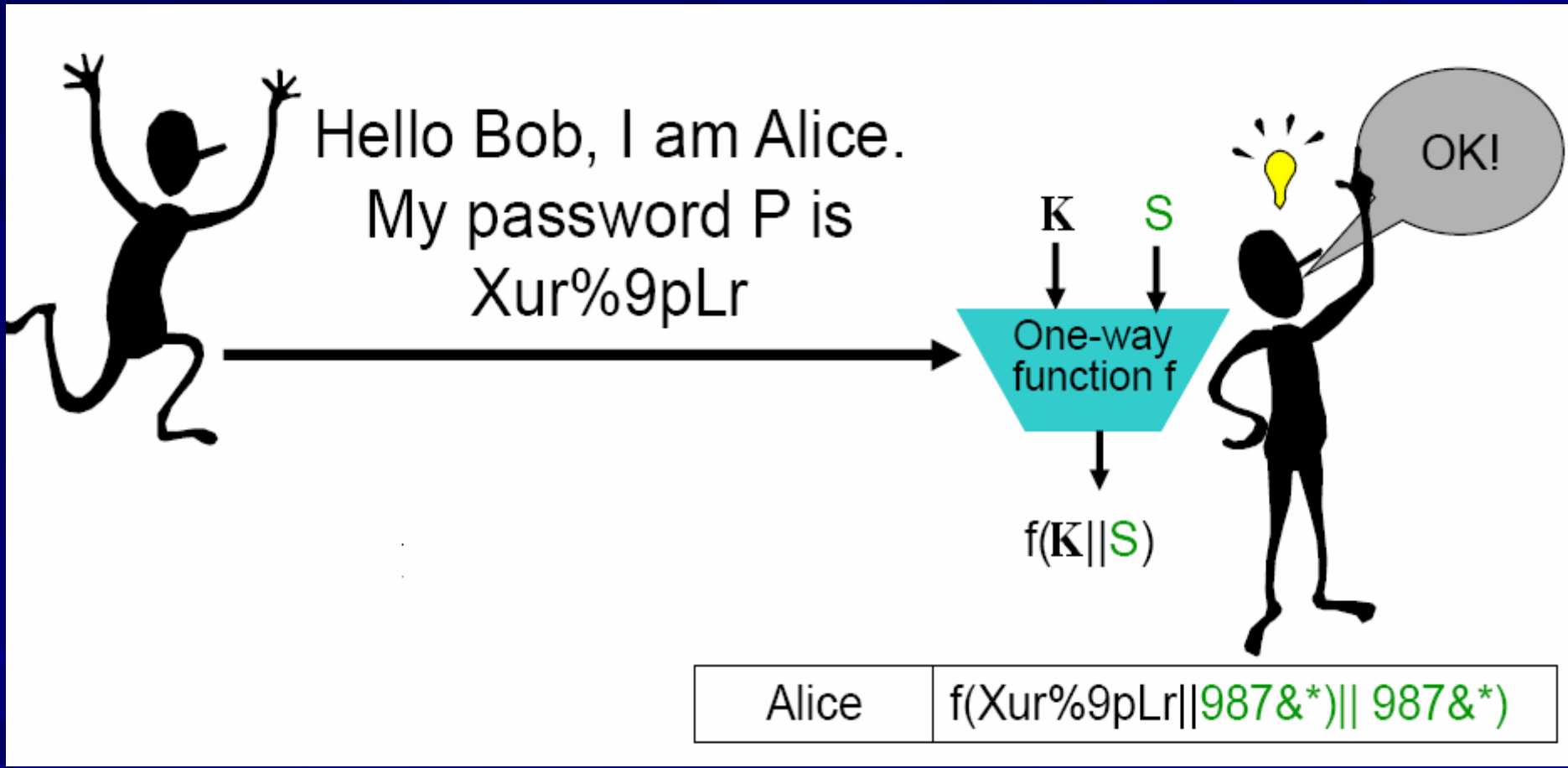
f. Mã hoá kết quả của (e)

$A \rightarrow B$: $E(K, [M \,||\, H(M \,||\, S])$

- Chứng thực: chỉ A và B chia sẻ S
- Bảo mật: chỉ A và B chia sẻ K

3. Hàm băm

Các công dụng cơ bản của hàm băm



Alice	f(Xur%9pLr||987&*)|| 987&*)

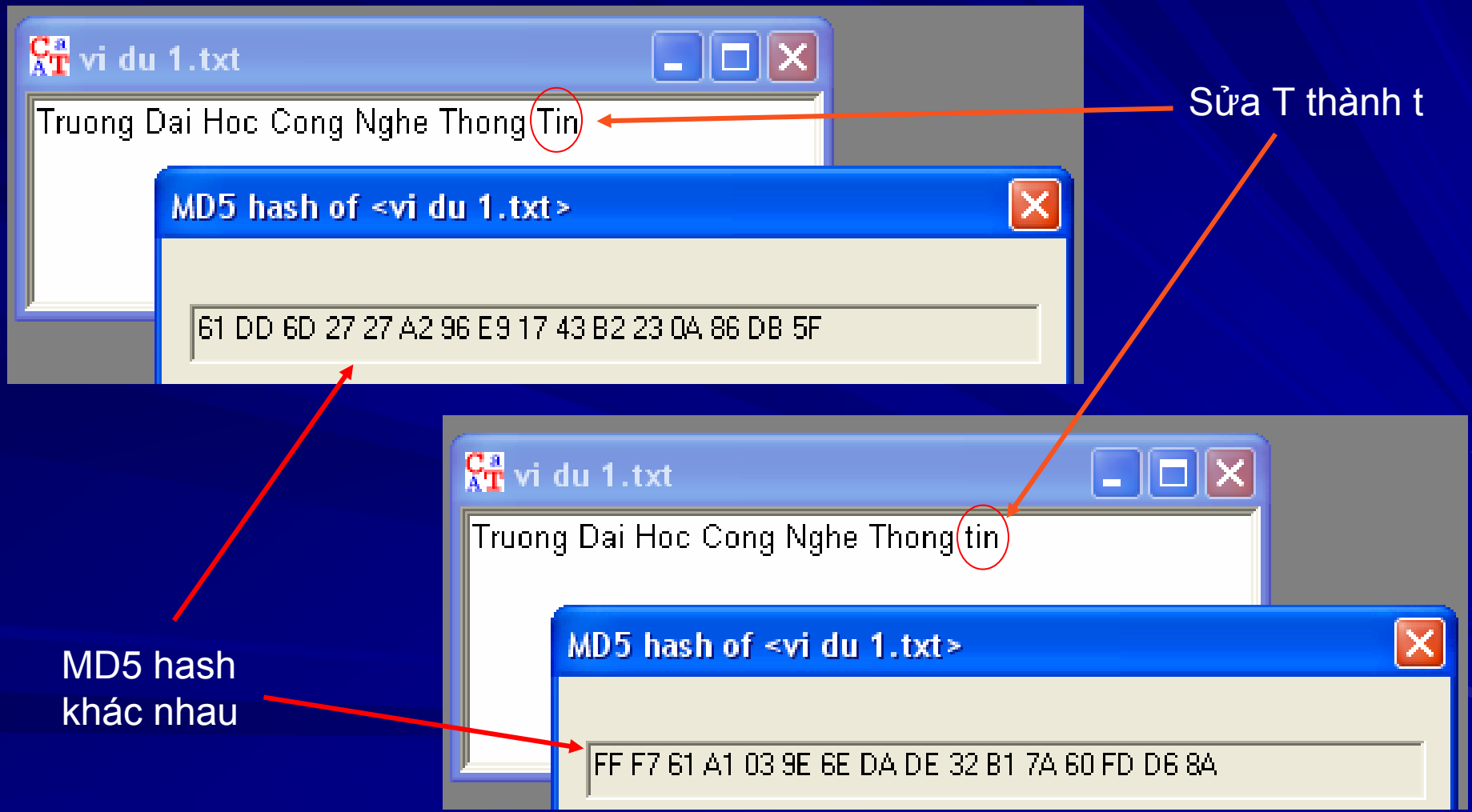
3. Hàm băm

MD5

- MD5 (Message-Digest algorithm 5) là một hàm băm mật mã với giá trị băm dài 128 bit diễn tả bởi một số thập lục phân 32 ký tự (RFC 1321).
- Được dùng chủ yếu để kiểm tra tính toàn vẹn của tập tin trên nguyên tắc hai dữ liệu vào X và Y hoàn toàn khác nhau thì xác suất để có cùng một md5 hash giống nhau là rất nhỏ.
- Được thiết kế bởi giáo sư Ronald Rivest (MIT) vào năm 1991 để thay thế MD4 không còn an toàn.
- Hiện nay, MD5 ít được sử dụng do kích thước bảng băm chỉ có 128 bit dễ bị tấn công brute-force và được thay thế bởi những giải thuật khác như Whirlpool, SHA-1…

3. Hàm băm

MD5


vi du 1.txt
Truong Dai Hoc Cong Nghe Thong Tin
MD5 hash of <vi du 1.txt>
61 DD 6D 27 27 A2 96 E9 17 43 B2 23 0A 86 DB 5F
Sửa T thành t
vi du 1.txt
Truong Dai Hoc Cong Nghe Thong tin
MD5 hash of <vi du 1.txt>
FF F7 61 A1 03 9E 6E DA DE 32 B1 7A 60 FD D6 8A
MD5 hash
khác nhau

3. Hàm băm

SHA

- SHA (Secure Hash Algorithm – Giải thuật băm an toàn) được phát triển bởi cục An ninh quốc gia Mỹ (National Security Agency – NSA).
- Giải thuật an toàn:
  - Cho một giá trị băm nhất định được tạo nên bởi một trong những giải thuật SHA, việc tìm lại được đoạn dữ liệu gốc là không khả thi.
  - Việc tìm được hai đoạn dữ liệu nhất định có cùng kết quả băm tạo ra bởi một trong những giải thuật SHA là không khả thi. Bất cứ thay đổi nào trên đoạn dữ liệu gốc, dù nhỏ, cũng sẽ tạo nên một giá trị băm hoàn toàn khác với xác xuất rất cao.

3. Hàm băm

SHA

- SHA gồm 2 phiên bản:
  - SHA-1: trả lại kết quả dài 160 bit. Được sử dụng rộng rãi để thay thế MD5 trong nhiều ứng dụng và giao thức bảo mật khác nhau, bao gồm TLS, SSL, PGP, SSH, S/MIME, IPSec.
  - SHA-2: gồm 4 giải thuật
    - SHA-224: trả lại kết quả dài 224 bit.
    - SHA-256: trả lại kết quả dài 256 bit.
    - SHA-384: trả lại kết quả dài 384 bit.
    - SHA-512: trả lại kết quả dài 512 bit (γ=512) và có $\Gamma=2^{128}-1$.

3. Hàm băm

SHA-1 và MD5

- SHA-1:
  - (2^{nd}) preimage 2^{160} steps
  - collisions 2^{80} steps

Shortcut: Aug. 2007: 2^{60} steps

- MD5
  - (2^{nd}) preimage 2^{128} steps
  - collisions 2^{64} steps

Shortcut: Aug. 2004: 2^{39} steps
(today: seconds)

4. Chữ ký số

Khái niệm chung

- Sử dụng khoá công khai để tạo chữ ký số:
  - Giả sử A cần gởi cho B một thông điệp mật kèm chữ ký điện tử, A sẽ sử dụng khoá công khai của B để mã hoá thông điệp rồi dùng khoá cá nhân của mình để mã hoá chữ ký, sau đó gởi cả thông điệp lẫn chữ ký cho B. B sẽ dùng khoá công khai của A để giải mã chữ ký, rồi dùng khoá cá nhân của mình để giải mã thông điệp của A.
  - Việc tạo chữ ký và kiểm chứng chữ ký thường được thực hiện nhờ hàm băm.

4. Chữ ký số

Khái niệm chung

Ký vào thông điệp:

- Dùng giải thuật băm để thay đổi thông điệp cần truyền đi để được một message digest (MD5 thu được digest có chiều dài 128-bit hoặc SHA thu được digest 160-bit).
- Sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên. Bước này thường dùng giải thuật RSA. Kết quả thu được gọi là digital signature của thông điệp ban đầu.
- Gộp digital signature vào thông điệp ban đầu ("ký nhận" vào thông điệp). Sau đó, mọi sự thay đổi trên message sẽ bị phát hiện. Việc ký nhận này đảm bảo người nhận tin tưởng thông điệp này xuất phát từ người gửi chứ không phải là ai khác.

4. Chữ ký số

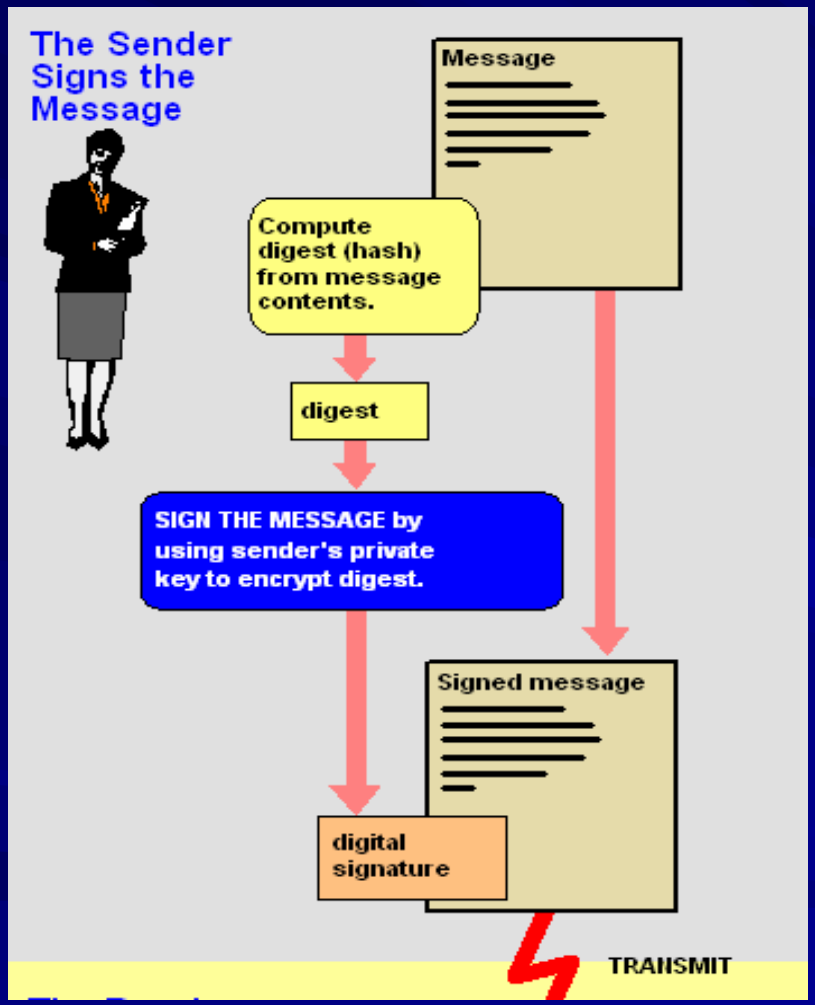
Khái niệm chung

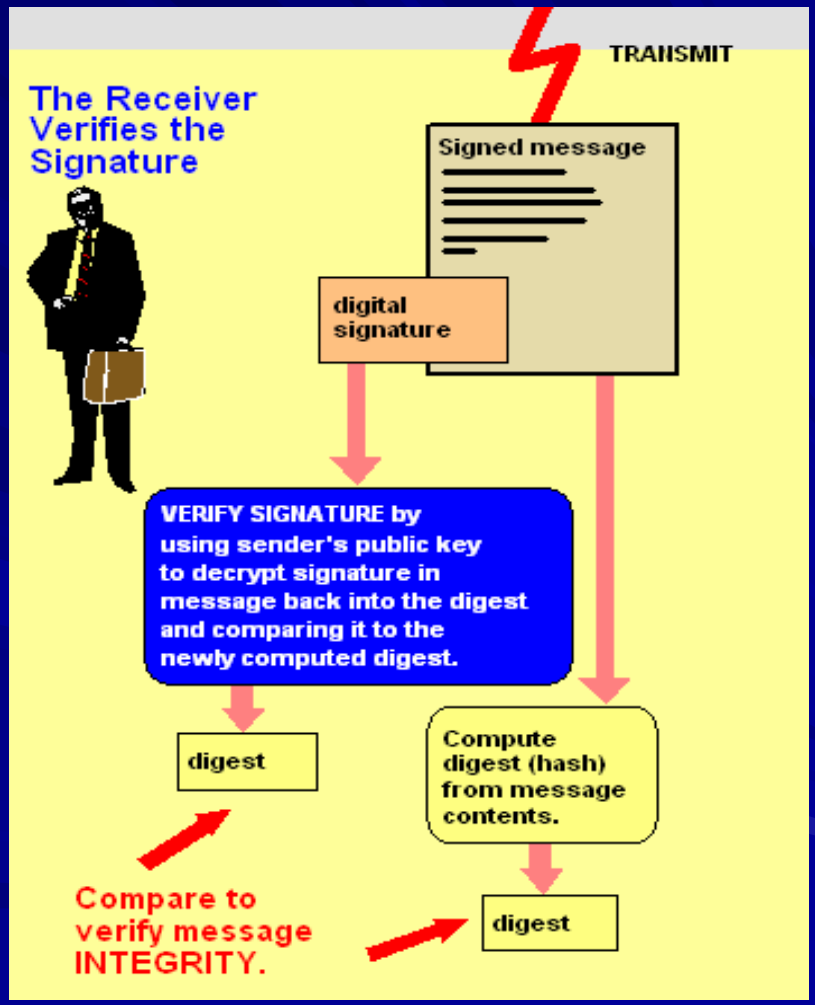
Các bước kiểm tra:

- Dùng public key của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của thông điệp.
- Dùng giải thuật (MD5 hoặc SHA) băm thông điệp nhận được.
- So sánh kết quả thu được ở bước 1 và 2. Nếu trùng nhau, ta kết luận thông điệp này không bị thay đổi trong quá trình truyền và thông điệp này là của người gửi .

4. Chữ ký số

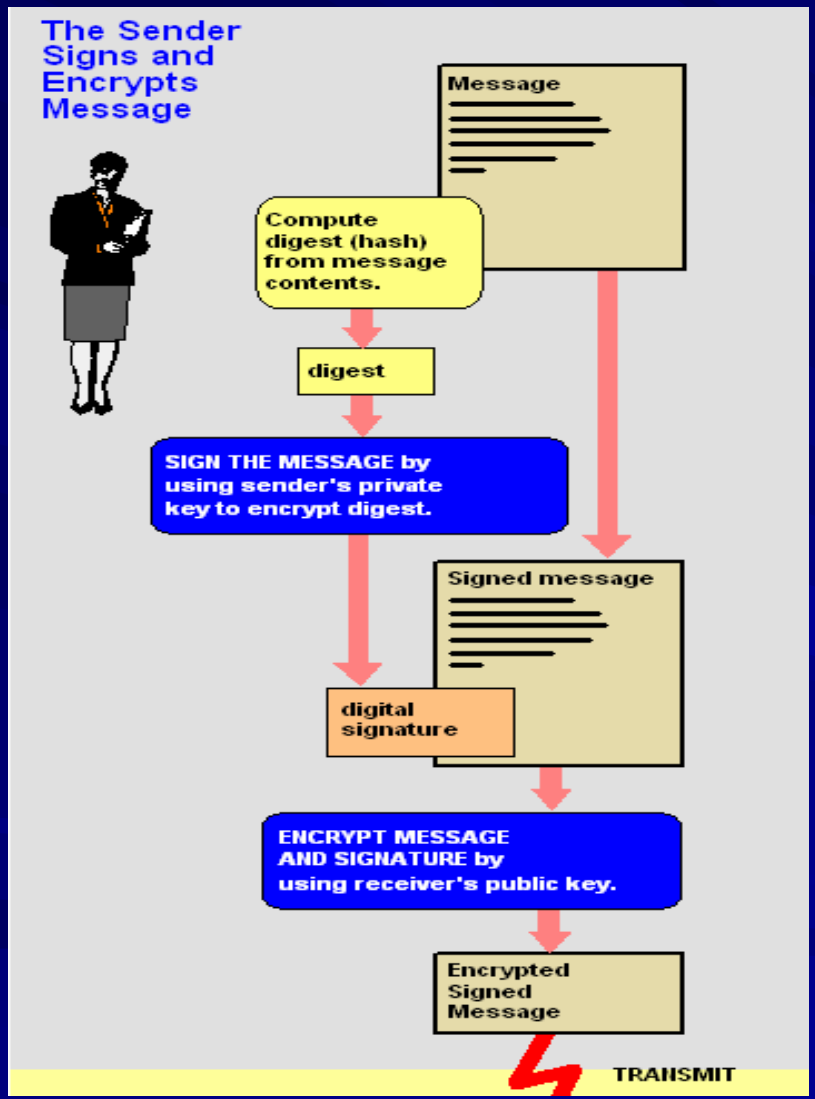
Không mã hoá

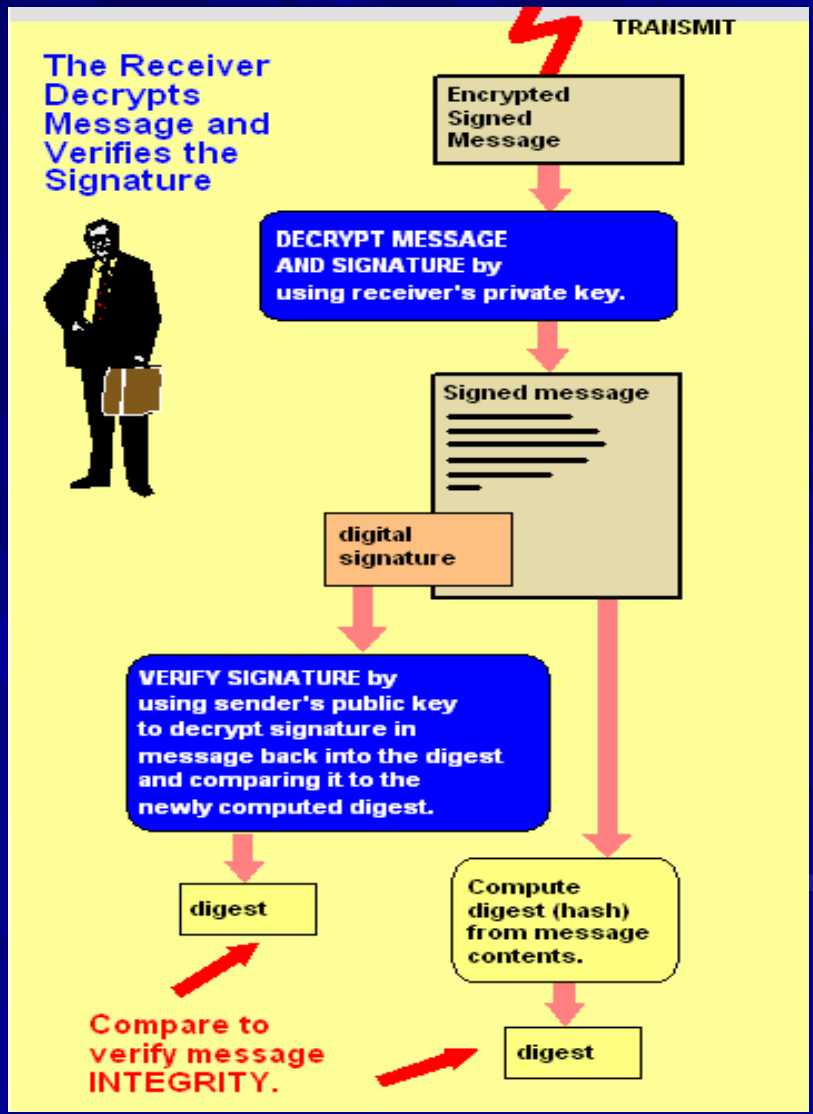




4. Chữ ký số

Có mã hoá





5. Bài tập

1. Tìm hai câu tiếng Anh có ý nghĩa khác nhau nhưng có cùng giá trị băm với 16-bit XOR-hash function $H_{\oplus}$.
2. Cho *h* = 1001101000111 010 là một chuỗi nhị phân 16 bit. Tìm 4 chuỗi nhị phân tương tự có cùng giá trị băm h với 16-bit XOR-hash function $H_{\oplus}$.
3. Mô tả chi tiết giải thuật MD5.

5. Bài tập

4. Vẽ lưu đồ minh hoạ giải thuật SHA-51.
5. Vẽ lưu đồ minh hoạ giải thuật HMAC.
6. Microsoft Windows XP, không giống như UNIX hoặc Linux, lưu user names và user passwords trong registry. Tìm kiếm và mô tả chi tiết tác vụ này. Cho biết độ bảo mật của giải thuật và đề xuất cách thức tấn công.

5. Bài tập

7. Nêu tên các ứng dụng có sử dụng chữ ký số nhằm đảm bảo an toàn thông tin.
8. Phân tích độ an toàn của các giải thuật MD5, SHA.
9. Mô tả các kỹ thuật có thể sử dụng để tấn công vào giải thuật MAC.
10. Chọn một trong số những giải thuật MAC và giải thuật băm để viết một ứng dụng sử dụng giải thuật này.

5. Bài tập

11. Tìm 3 phần mềm có kèm theo mã băm, kiểm tra mã băm (dùng phần mềm hoặc website) để suy ra độ tin cậy của các phần mềm này.
12. Tìm 3 chứng chỉ số đính kèm theo trên các trang web có yêu cầu bảo mật cao.
13. Sử dụng Cryptool, thực hiện một số ví dụ về dữ liệu giả mạo khi sử dụng chứng thực với giải thuật băm.

Thank You !