Bài 6
Xác thực thông điệp

Thời lượng: 4 tiết

Lương Thái Lê

Nội dung

1. Xác thực thông điệp
   - Mã xác thực
2. Hàm băm
3. Chữ ký điện tử
   - Chuẩn chữ ký điện tử (DSS)
   - Chữ ký điện tử Elgamal
   - Chữ ký diện tử Schnorr

Xác thực thông điệp(Message Authentication)

- ***Nhằm xác định tính toàn vẹn của mẩu tin, xác thực danh tính người gửi là hợp lệ, và đảm bảo không chối từ***
- Mã hóa đối xứng cũng cung cấp chức năng xác thực (giữa những người chia sẻ khóa bí mật)
- Mã khóa công khai cũng có thể dùng để xác thực (khi người gửi mã hóa bằng khóa riêng – chữ ký số)

(c) Mã hóa khóa công khai: xác thực và chữ ký số

Hai cấp độ xác thực

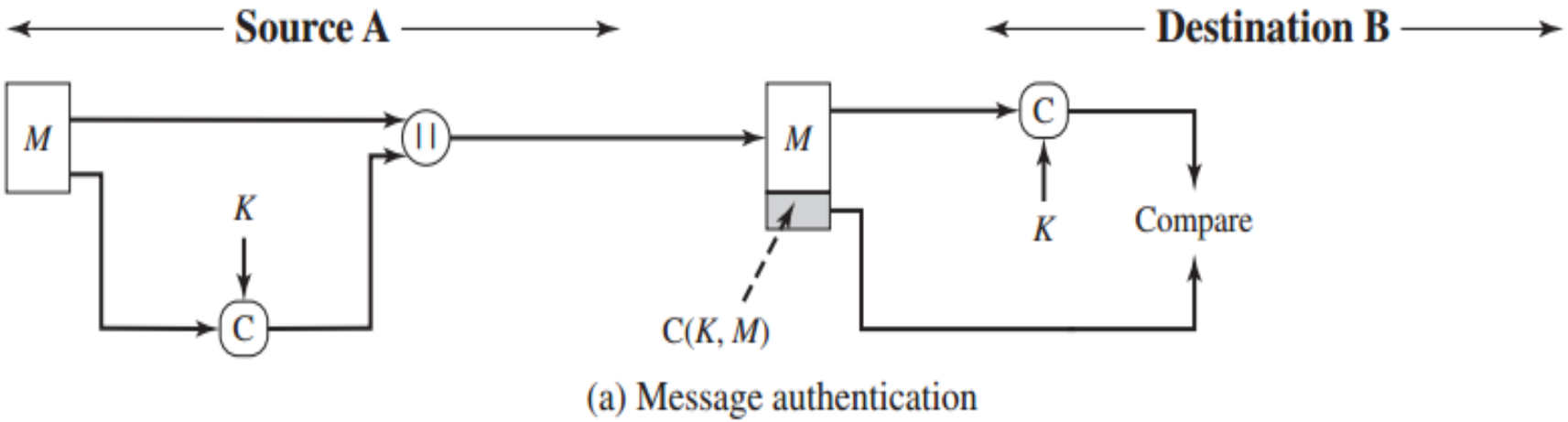
- Cơ chế xác thực thông điệp có hai cấp độ:

1. Mức thấp: tạo ra một **chứng thực (authenticator)** để xác thực một tin nhắn, gồm các loại:
   - Mã xác thực thông điệp (Message authentication code-MAC)
   - Hàm băm (Hash function)
   - Mã hóa thông điệp (Message encryption)
2. Mức cao: hàm ở mức thấp được dùng như là một **yếu tố** trong giao thức xác thực ở mức cao để giúp người nhận xác thực thông điệp.

Mã xác thực thông điệp – MAC (message authentication code)

- MAC cung cấp sự tin cậy, xác thực
- MAC là một block thông tin nhỏ có kích thước cố định được sinh bởi thuật toán đòi hỏi sử dụng khóa bí mật:
  - Phụ thuộc vào cả mẩu tin và khoá
  - Giống như mã nhưng không cần phép toán ngược lại
  - Bổ sung vào mẩu tin như chữ ký
- MAC tương tự mã hóa nhưng không cần giải ngược

Sơ đồ tạo MAC để xác thực



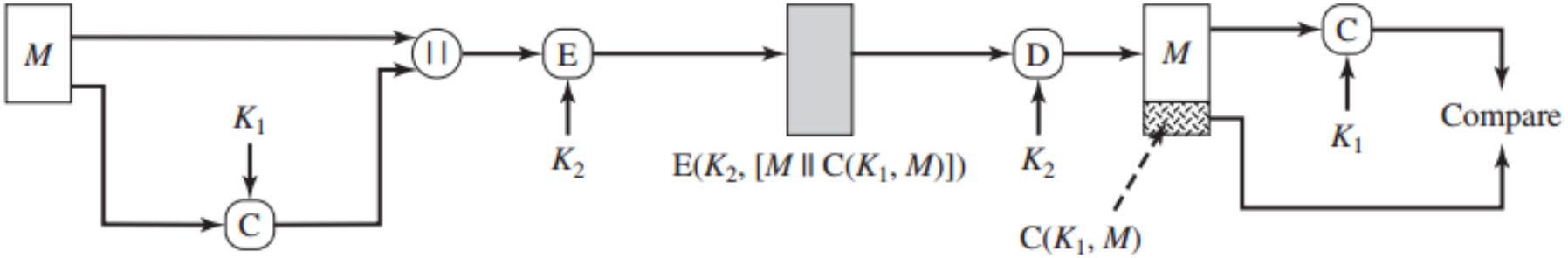
(a) Message authentication

- A và B dùng chung khóa bí mật K
- A tạo MAC = C(K,M)
- Lưu ý rằng MAC không phải là chữ ký điện tử

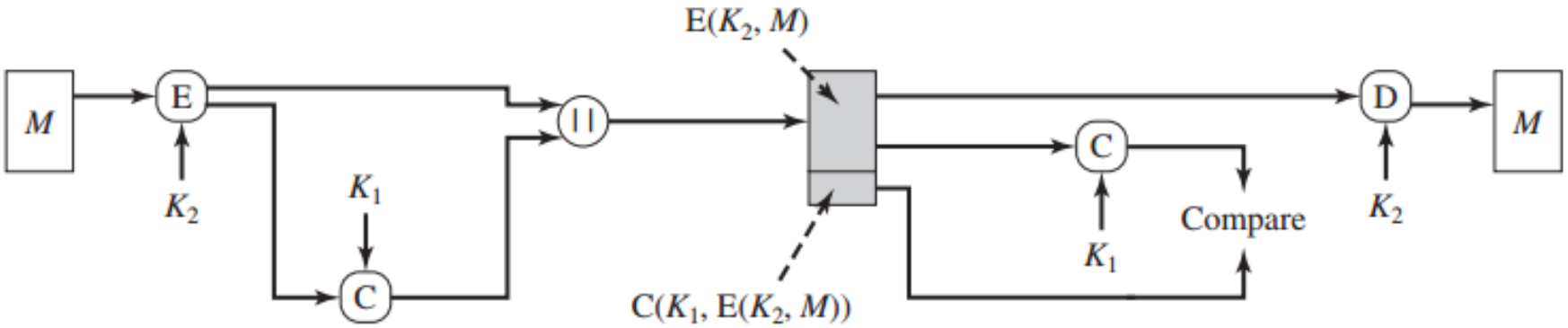
Tại sao: MAC không là chữ ký điện tử?

Trả lời: Không, vì hai người nhận, gửi đều có thể tạo ra

Sử dụng MAC kèm với Mã hóa



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



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

- Nên MAC trước và mã hóa sau

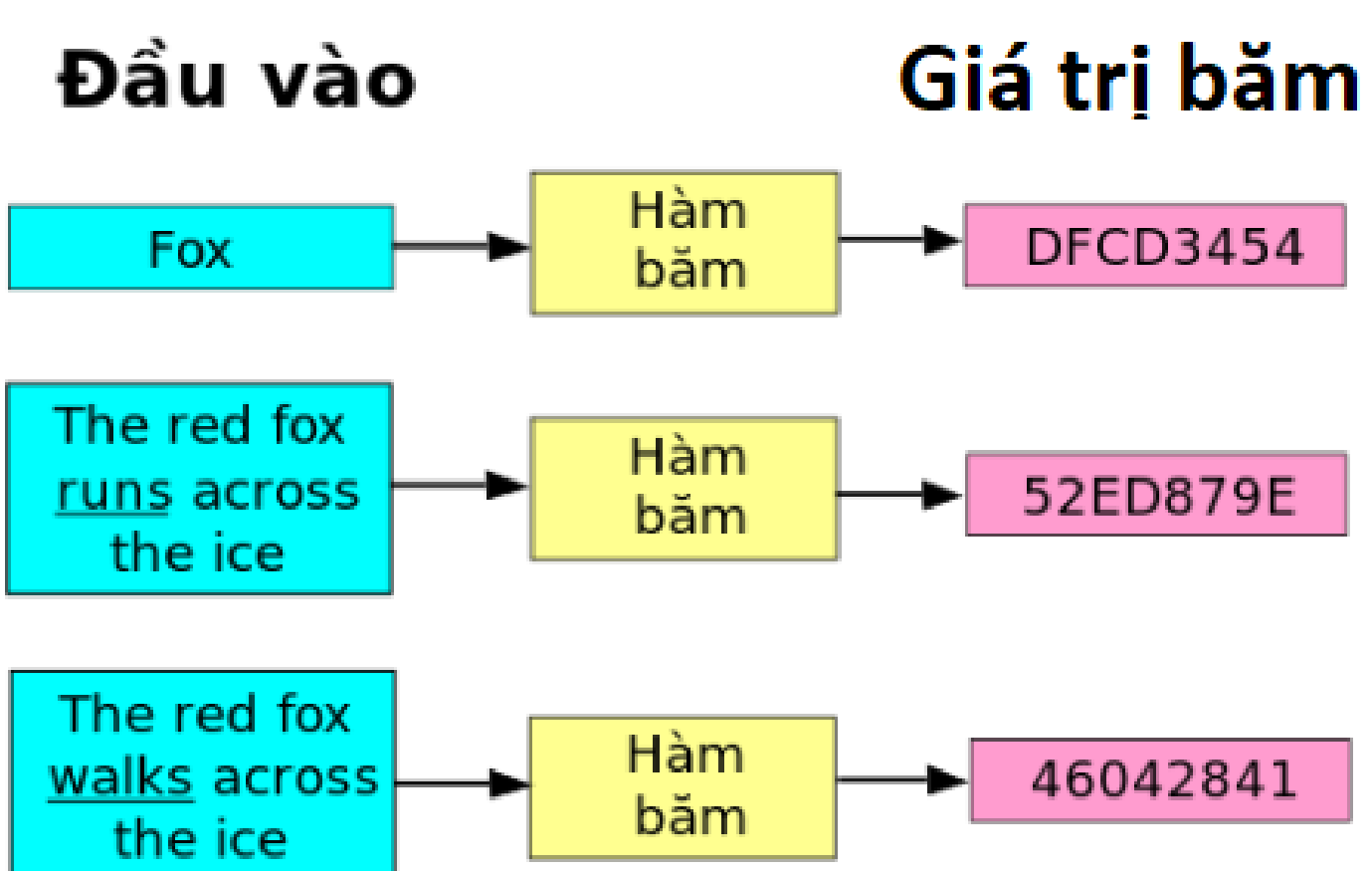
Các tính chất của MAC

- Nén bản tin M có độ dài tùy ý
- Sử dụng khoá mật K
- Tạo dấu xác thực có độ dài cố định
- Là hàm nhiều - một: có thể có nhiều mẩu tin có cùng MAC
- Yêu cầu với MAC
  - Biết mẩu tin và MAC, không thể tìm được mẩu tin khác có cùng MAC
  - Các MAC cần phải phân bố đều
  - MAC phải phụ thuộc như nhau vào tất cả các bit trong mẩu tin
- Ví dụ về MAC :
  - sử dụng khối cuối cùng của mã khối làm MAC của mẩu tin
  - M bit trái nhất ($16 \leq M \leq 64$) của khối cuối cùng

Nội dung

1. Xác thực thông điệp – Mã xác thực
2. Hàm băm
3. Chữ ký điện tử
   - Chuẩn chữ ký điện tử (DSS)
   - Chữ ký điện tử Elgamal
   - Chữ ký diện tử Schnorr

Một ví dụ hàm băm



Hàm băm (Hash functions)

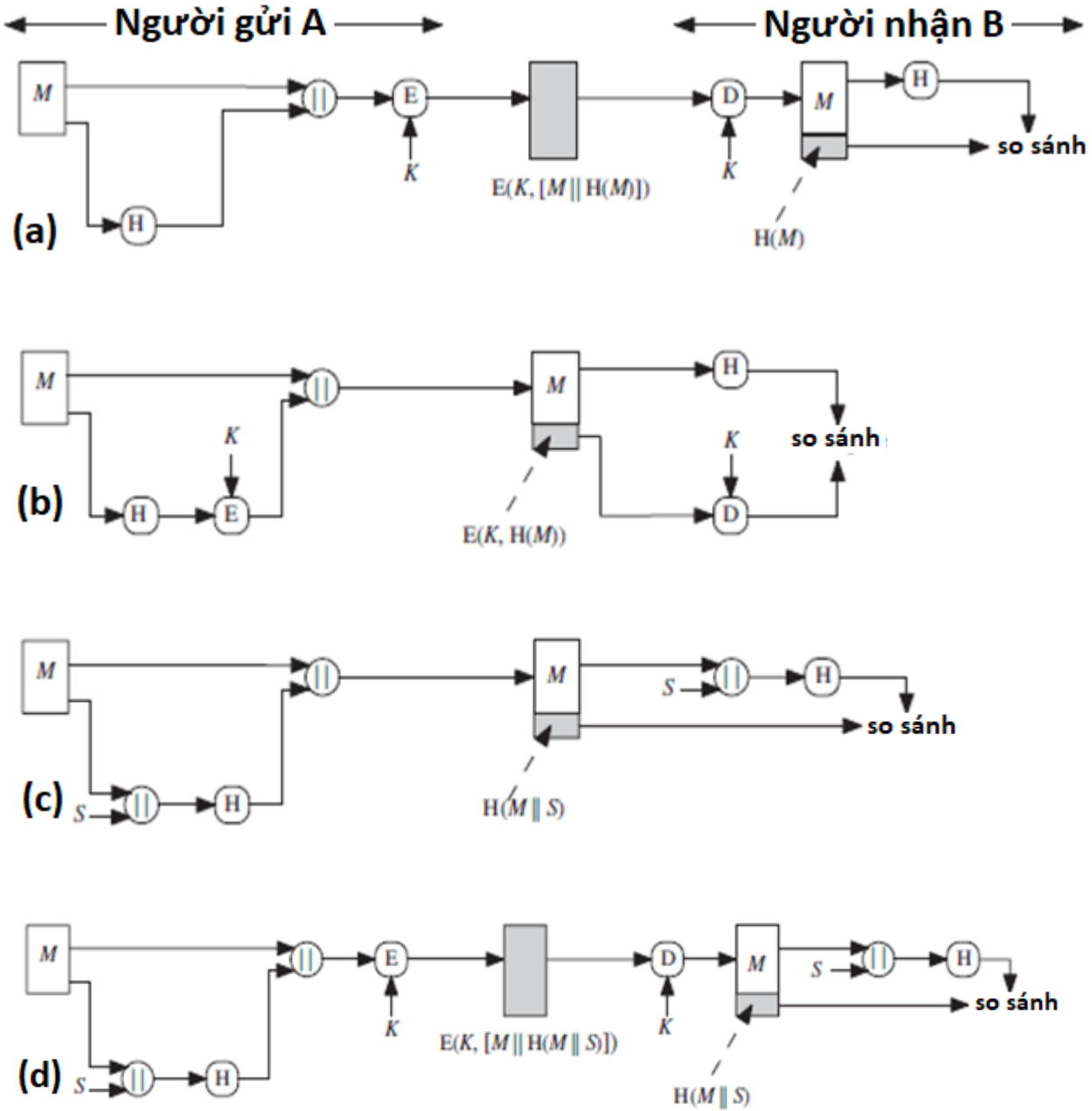
- Hàm Hash tạo nên dấu vân tay (tức là thông tin đặc trưng) của một tệp, mẩu tin hay dữ liệu

$$h = H(M)$$

=>nén mẩu tin bất kỳ về dấu vân tay kích thước cố định (128 bit – 1024 bit)

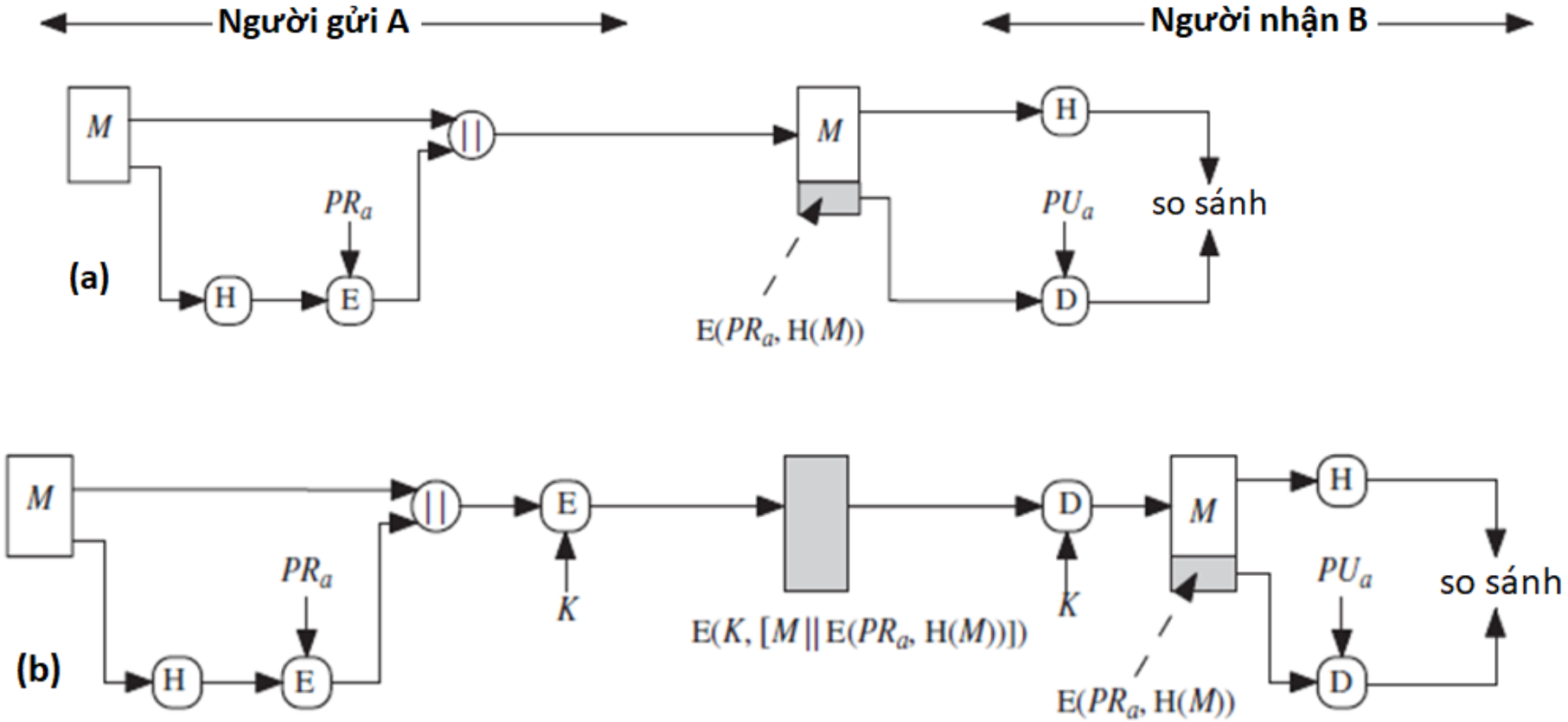
- Hàm hash là công khai và không dùng khoá
- Hash chỉ phụ thuộc mẩu tin, còn MAC phụ thuộc thêm vào khoá
- Hash được sử dụng để phát hiện thay đổi của mẩu tin và được dùng để tạo chữ ký.
- Hàm băm hay dùng: MD5, SHA…
- *Ví dụ một hàm băm đơn giản: biểu diễn mẩu tin dưới dạng bit sau đó chia chúng thành các khối bit có kích thước bằng kích thước mong muốn của Hash. Rồi dựa trên phép toán XOR các bit thông tin ở cùng vị trí tương ứng của các khối, kết quả nhận được là Hash của cả mẩu tin*

Hàm băm trong xác thực thông điệp



1. Một số ví dụ về sử dụng hàm băm để xác thực thông điệp

Hàm băm ứng dụng trong chữ ký số



2. Các ví dụ về sử dụng hàm băm làm chữ ký số

- Sử dụng khóa mật

Các tính chất của hàm Hash

- Có thể áp dụng cho mọi mẩu tin có kích thước tuỳ ý
- Tạo đầu ra h có kích thước cố định
- Dễ tính h = H(M) cho mọi mẫu tin M
- Cho trước h không thể tìm được (rất khó) x sao cho H(x) = h

=> Tính chất 1 chiều

- Cho x không thể tìm được y sao cho H(y) = H(x)

=> Chống đỡ va chạm yếu

- Không thể tìm được x, y sao cho H(y) = H(x)

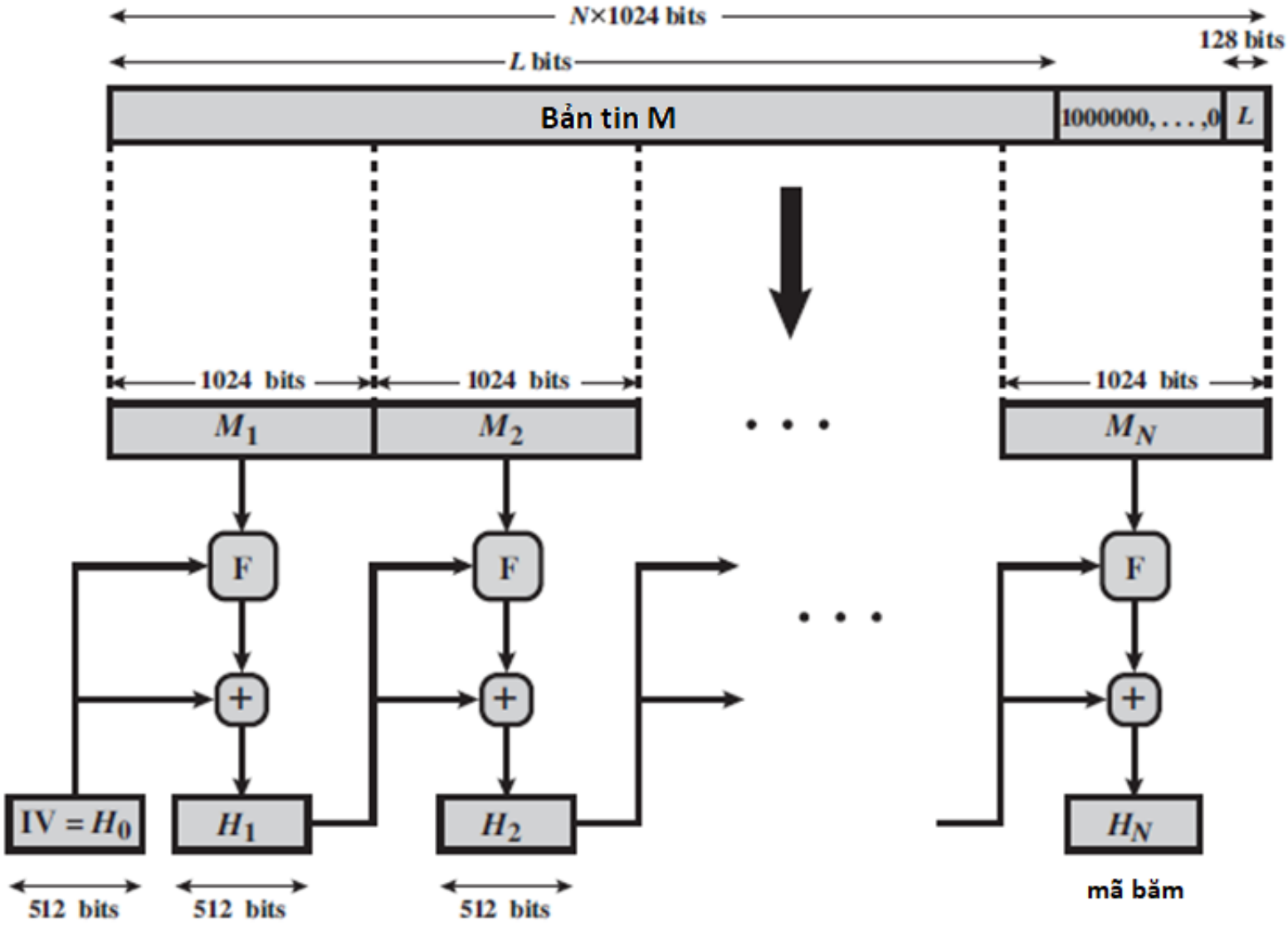
=> Chống đỡ va chạm mạnh

Thuật toán băm an toán SHA (Secure Hash Algorithm)

- 1993: SHA (SHA-0) .
- 1995: SHA-1 mã băm 160 bit.
- 2002: SHA-2 gồm: SHA-256, SHA-384, SHA-512 với số bit tương ứng.

Bảng So sánh các tham số SHA (Đơn vị tính là bits)					
	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Mã băm	160	224	256	384	512
Input M	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
block size	512	512	512	1024	1024
word size	32	32	32	64	64
Số lần lặp	80	64	64	80	80

SHA-512



+ phép cộng mod 2^{64}

Quá trình sinh mã băm mật mã sử dụng SHA-512

Thao tác trên 1 khối 1024 bit

- Khởi tạo các từ

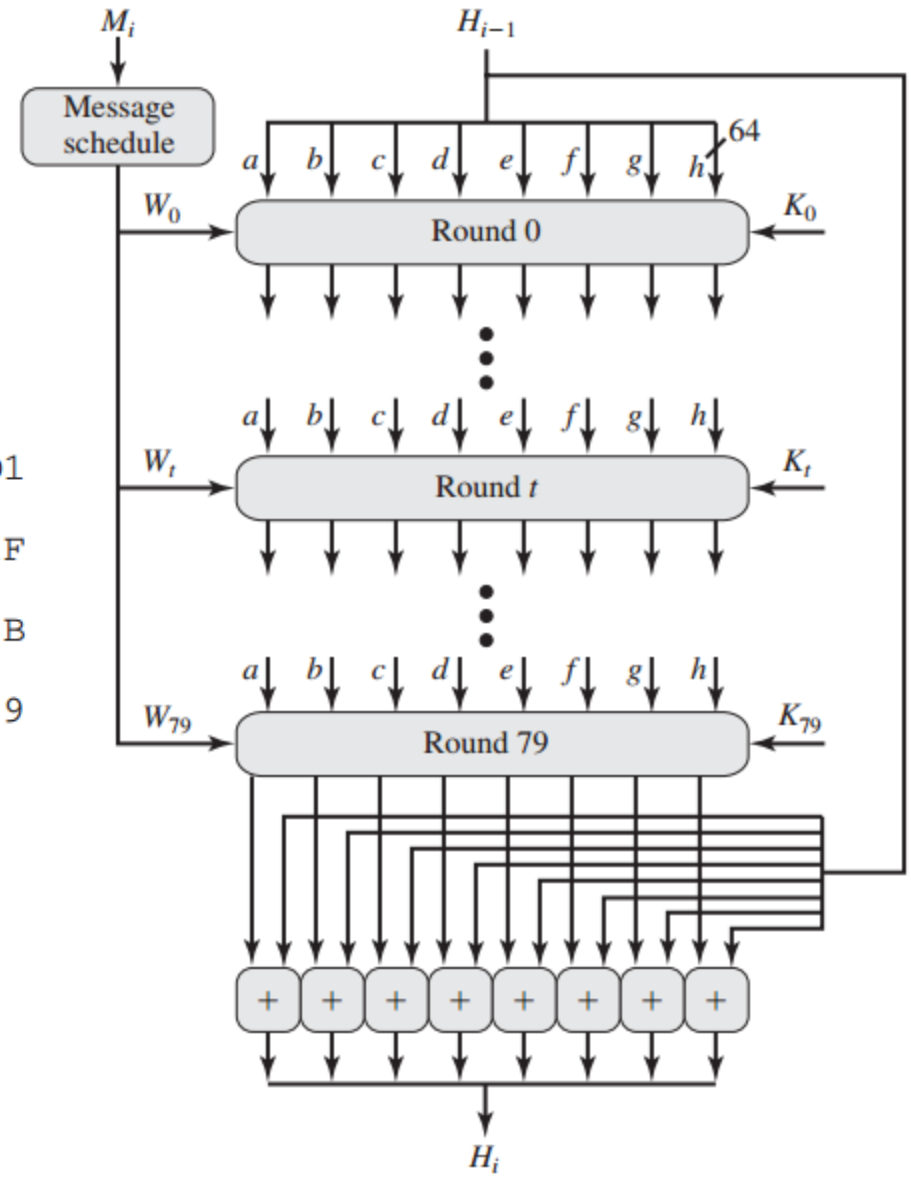
```
a = 6A09E667F3BCC908   e = 510E527FADE682D1
b = BB67AE8584CAA73B   f = 9B05688C2B3E6C1F
c = 3C6EF372FE94F82B   g = 1F83D9ABFB41BD6B
d = A54FF53A5F1D36F1   h = 5BE0CD19137E2179
```

- Tóm tắt thuật toán SHA-512

$$H_0 = \text{IV}$$

$$H_i = \text{SUM}_{64}(H_{i-1}, \text{abcdefgh}_i)$$

$$MD = H_N$$



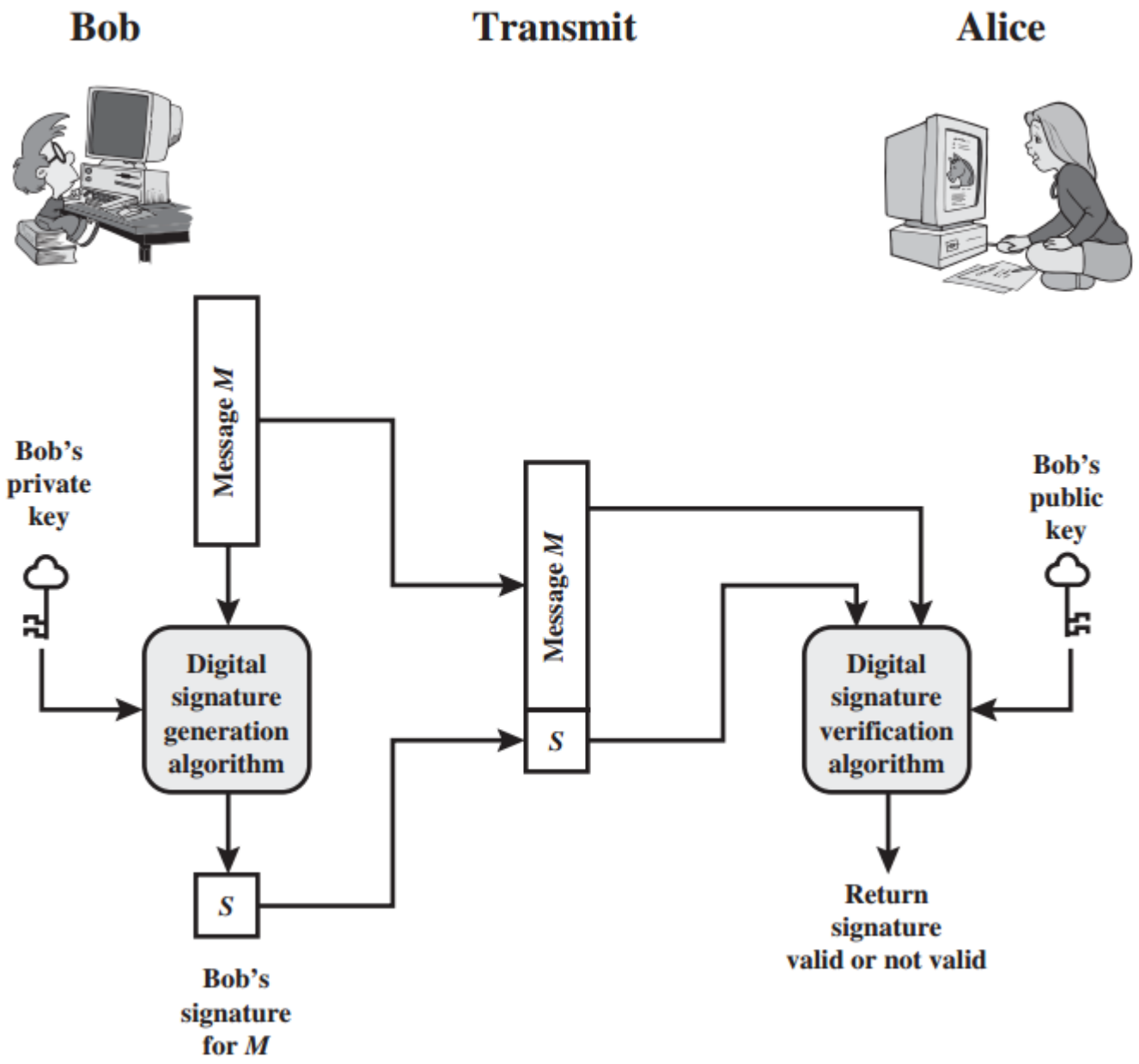
Nội dung

1. Xác thực thông điệp – Mã xác thực
2. Hàm băm
3. Chữ ký điện tử
   - Chuẩn chữ ký điện tử (DSS)
   - Chữ ký điện tử Elgamal
   - Chữ ký diện tử Schnorr

Chữ ký điện tử

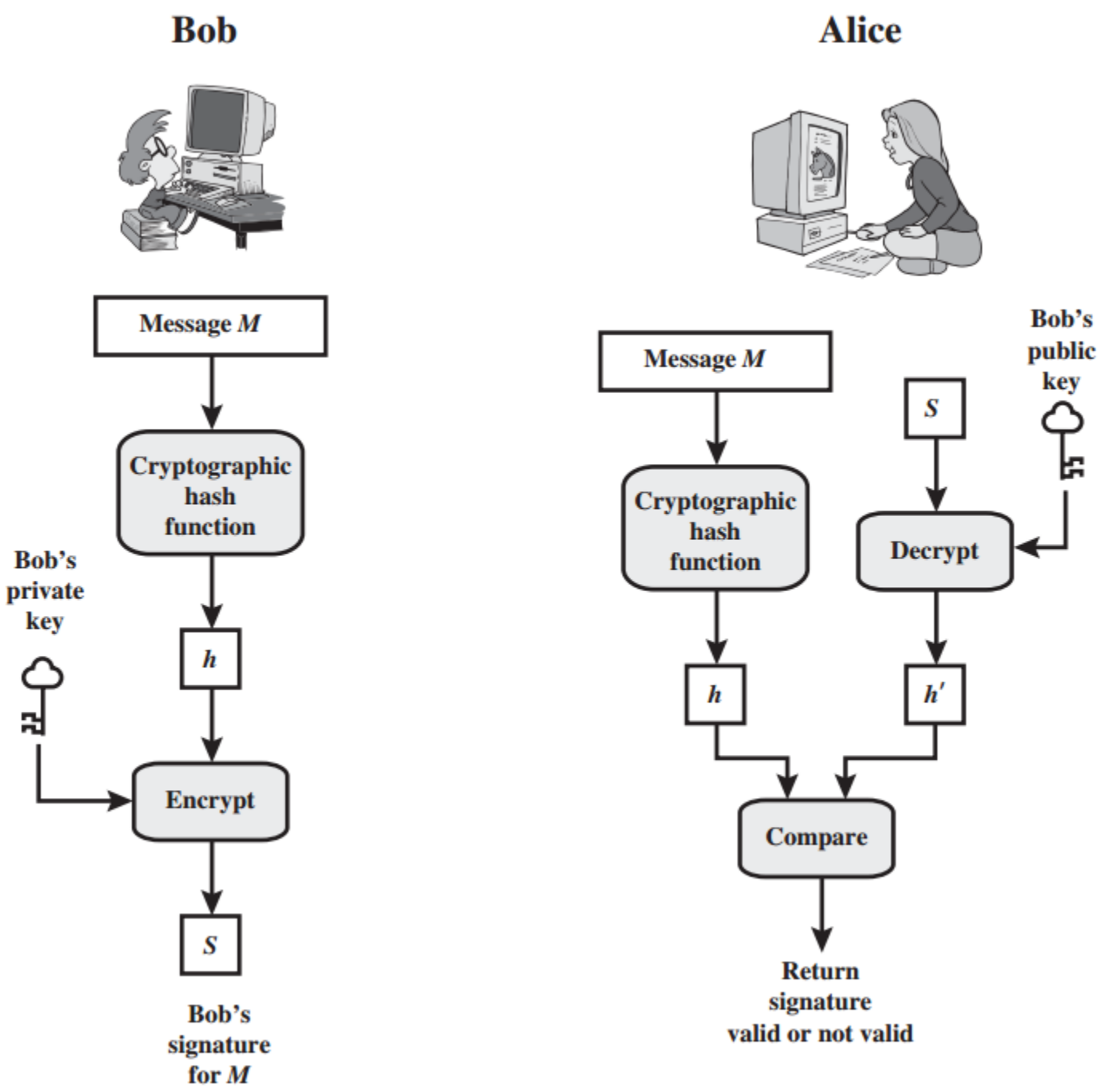
- Là cơ chế xác thực cho phép người tạo thông điệp đính kèm theo một đoạn mã (một chữ ký).
- Thường được tạo bởi hàm băm rồi mã hóa sử dụng khóa riêng.
- Cung cấp các khả năng để
  - Kiểm chứng tác giả, ngày và giờ ký
  - Đảm bảo tính toàn vẹn cho thông điệp
- Chuẩn chữ ký số (digital signature standard - DSS) do NIST đưa ra. Chuẩn này sử dụng thuật toán SHA

Chữ ký điện tử sử dụng mã khóa công khai



Các yêu cầu của chữ ký điện tử

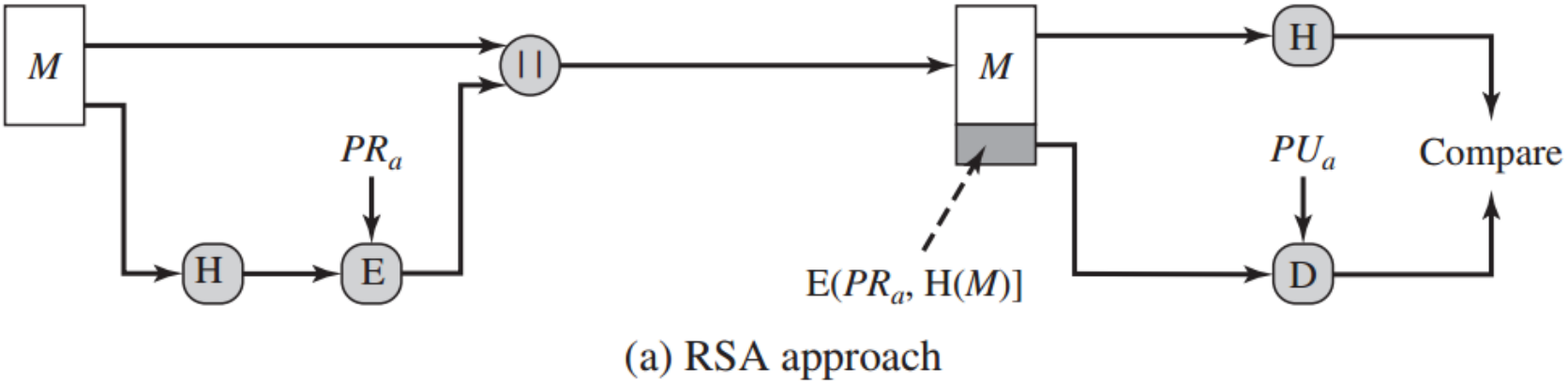
- Cần phải xác định được tác giả (chứa thông tin đặc trưng về tác giả) và ngày giờ ký
- Cần đảm bảo nội dung thông điệp khi ký: chứa nội dung của thông điệp
- Cần phải tương đối dễ dàng tạo ra
- Dễ dàng đoán nhận và kiểm chứng
- Không thể tính toán giả mạo được
  - Với bản tin mới và chữ ký đã có
  - Với chữ ký giả mạo cho 1 bản tin
- Có thể lưu trữ bản sao của chữ ký điện tử


Bob
Alice
Message M
Cryptographic hash function
Bob's private key
h
Encrypt
S
Bob's signature for M
Message M
Cryptographic hash function
h
S
Bob's public key
Decrypt
h'
Compare
Return signature valid or not valid

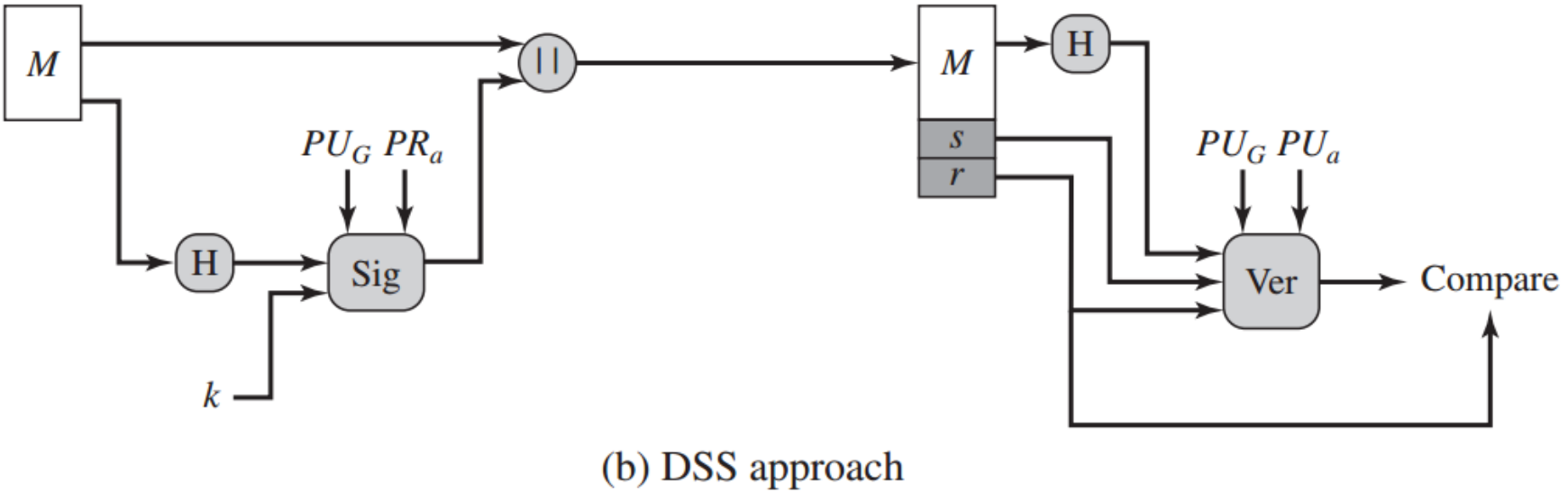
Chuẩn chữ ký điện tử (DSS)
Digital Signature Standard

- DSS được đề xuất năm 1991
- Sử dụng thuật toán hash SHA
- DSS giới thiệu DSA (Digital signature algorithm) là thuật toán chữ ký điện tử.
- DSS chỉ cung cấp thuật toán chữ ký số (không có mã hóa hay trao đổi khóa)
- Việt nam cũng có văn bản công nhận tính pháp lý của chữ ký điện tử.

Hai cách tiếp cận



(a) RSA approach



(b) DSS approach

Thuật toán chữ ký điện tử (DSA)

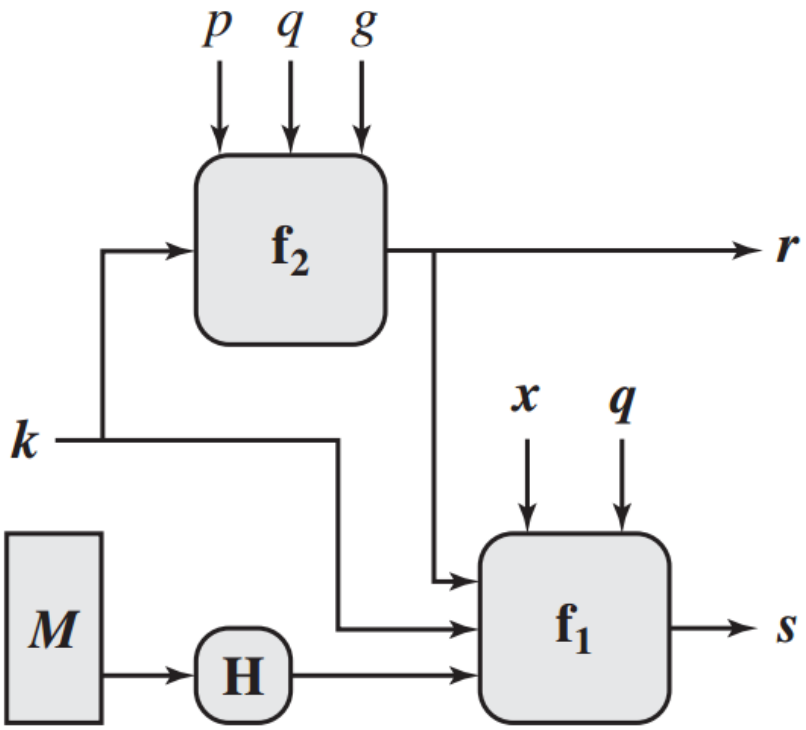
(Digital Signature Algorithm)

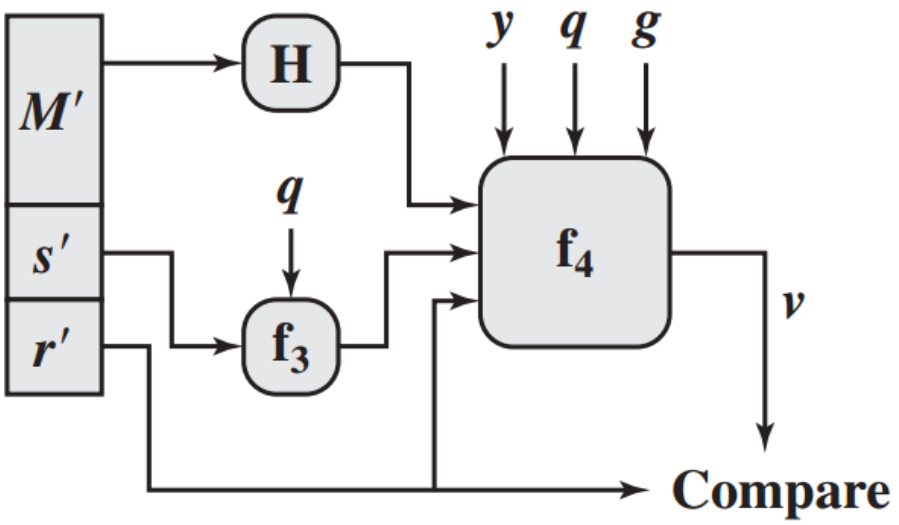
1. Các giá trị công khai chung
p: số nguyên tố trong đó $2^{L-1} < p < 2^L$, với $512 \leq L \leq 1024$ và L là một bội số của 64;
q: Ước số nguyên tố của (p – 1), q có độ dài 160 bit
$g = h^{(p-1)/q} \bmod p$, trong đó h là số nguyên $1 < h < (p-1)$ sao cho $h^{(p-1)/q} \bmod p > 1$.

2. Người dùng
Khóa riêng: x thỏa $0 < x < q$
Khóa công khai: $y = g^x \bmod p$
Số bí mật cho mỗi tin nhắn: k thỏa $0 < k < q$

3. Ký chữ ký số
$r = (g^k \bmod p) \bmod q$ $s = [k^{-1}(H(M) + xr)] \bmod q$ Chữ ký số = (r, s)

Mô hình Ký và kiểm tra của DSA





$s = \mathrm{f}_1(\mathrm{H}(M), k, x, r, q) = (\mathrm{k}^{-1}\,(\mathrm{H}(M) + xr)) \bmod q$

$r = \mathrm{f}_2(k, p, q, g) = (g^k \bmod p) \bmod q$

(a) Signing

$w = \mathrm{f}_3(s', q) = (s')^{-1} \bmod q$

$v = \mathrm{f}_4(y, q, g, \mathrm{H}(M'), w, r')$

$= ((g^{(\mathrm{H}(M')w) \bmod q}\, y^{r'w \bmod q}) \bmod p) \bmod q$

(b) Verifying

Kiểm chứng chữ ký DSA
DSA Signature Verification

Đầu vào cho xác minh	**4. Xác minh chữ ký**
M: tin nhắn được ký H(M): mã băm của M sử dụng SHA-1 M', r', s': là các phiên bản nhận được của M, r, s.	$w = (s')^{-1} \bmod q$ $u_1 = [H(M')w] \bmod q$ $u_2 = (r')w \bmod q$ $v = [(g^{u1} y^{u2}) \bmod p] \bmod q$ Kiểm tra: v = r'

Ví dụ: Tạo chữ ký điện tử (DSA)

- Chọn p = 23, q = 11, h = 7
- g = h^2 mod 23 = 3
- Chọn x = 5, y = 3^5 mod 23 = 13
- k = 6, H(M) = 9

$$r = (g^k (\mathrm{mod}\ p))(\mathrm{mod}\ q)$$

- r = (3^6 mod 23) mod 11 = (4^2) mod 11 = 5

$$s = (k^{-1}(H(M) + x.r))(\mathrm{mod}\ q)$$

- s = (6^{-1}.(9 + 5.5))mod 11 = 2
- Chữ ký điện tử (5,2)

Kiểm tra chữ ký (DSA)

$w = s^{-1} (\mathrm{mod}\ q)$

$u1 = (H(M).w) (\mathrm{mod}\ q)$

$u2 = (r.w) (\mathrm{mod}\ q)$

$v = (g^{u1}.y^{u2} (\mathrm{mod}\ p))\ (\mathrm{mod}\ q)$

- $w = 2^{-1} \bmod 11 = 6$
- $u_1 = (9.6) \bmod 11 = 10$
- $u_2 = (5.6) \bmod 11 = 8$
- $v = (3^{10}.13^8 \bmod 23) \bmod 11 = (4^3.3.13^8 \bmod 23) \bmod 11 = (16) \bmod 11 = 5$
- v = 5 = r, chữ ký đúng

Câu hỏi: Kết quả kiểm tra chữ ký có phụ thuộc vào số ngẫu nhiên k không? Dùng sô k để làm gì?

Trả lời: không, dùng nó để tạo nhãn đặc trưng cho lần gửi như thời gian

Nội dung

1. Xác thực thông điệp – Mã xác thực
2. Hàm băm
3. Chữ ký điện tử
   - Chuẩn chữ ký điện tử (DSS)
   - Chữ ký điện tử Elgamal
   - Chữ ký diện tử Schnorr

Chữ ký số ElGamal

1. Các giá trị công khai chung	**Ví dụ**
q là số nguyên tố	q = 19
a là một căn nguyên thủy của q (a < q).	a = 10

2. Người gửi tạo khóa	**Ví dụ**
Chọn $X_A < q - 1$	$X_A = 16$
Tính $y_A = a^{XA} \bmod q$	$Y_A = 10^{16} \bmod 19 = 4$
Khóa công khai PU = {q, a, Y_A}	{19, 10, 4}
Khóa riêng X_A	16

Thực hiện ký (Elgamal)

3. Người gửi kí vào M	**Ví dụ**
Tính m = H(M); $0 \leq m \leq q-1$	m = H(M) = 14
Chọn K, Gcd(K,q-1) = 1 và $0 \leq K \leq q-1$	K = 5, gcd(5, 18) = 1
Tính $S_1 = a^K \bmod q$;	$S_1 = 10^5 \bmod 19 = 3$
Tính $K^{-1} \bmod (q-1)$	$5^{-1} \bmod 18 = 11$
Tính $S_2 = K^{-1}(m - X_A S_1) \bmod (q-1)$	$S_2 = 11(14 - 16*3) \bmod 18 = 4$
Chữ ký số (S_1, S_2)	(3, 4)

Xác minh chữ ký (Elgamal)

4. Người nhận xác minh chữ ký của người gửi	**Ví dụ**
Chữ ký nhận được (S_1, S_2)	(3, 4)
Tính $V_1 = a^m \bmod q$	$V_1 = 10^{14} \bmod 19 = 16$
Tính $V_2 = (Y_A)^{S1}(S_1)^{S2} \bmod q$	$V_2 = 4^3 * 3^4 \bmod 19 = 16$
Nếu $V_1 = V_2$ thì chữ ký là hợp lệ.	chữ ký số là hợp lệ

Tóm tắt

Đã xem xét:

- Khái niệm mã công khai
- Mã công khai RSA
- Trao đổi khóa Diffie-Hellman
- Xác thực thông điệp, mã xác thực MAC
- Hàm băm an toàn SHA
- Chữ ký điện tử DSA

Câu hỏi trắc nghiệm

Câu 1: Xét khoá công khai, tìm kết luận sai trong các khẳng định sau

A. Khoá công khai thông báo cho mọi người biết
B. Người sử dụng phải giữ bí mật khoá riêng của mình
C. Tính an toàn dựa vào độ khó của bài toán cho khoá công khai tìm khoá riêng
D. Không có thuật toán tính được khoá riêng khi biết khoá công khai

Câu 2: Xét khoá công khai, tìm kết luận đúng trong các khẳng định sau

A. Khoá riêng thông báo cho mọi người biết
B. Người sử dụng phải giữ bí mật khoá riêng của mình
C. Tính an toàn dựa vào độ khó của bài toán cho khoá riêng tìm khoá công khai
D. Không có thuật toán tính được khoá riêng khi biết khoá công khai

Câu hỏi trắc nghiệm 2

Câu 3: Xét mã RSA, tìm kết luận sai trong các khẳng định sau

A. Độ an toàn dựa vào độ khó của bài toán phân tích 1 số ra thừa số
B. Tính an toàn dựa vào độ khó bài toán nhân hai số nguyên tố rất lớn
C. Dựa trên lũy thừa trường hữu hạn các số nguyên modulo nguyên tố
D. Sử dụng các số rất lớn 1024 bit

Câu 4: Xét mã RSA, tìm kết luận sai trong các khẳng định sau

A. Chỉ dùng mã các dữ liệu nhỏ
B. Kết hợp với mã đối xứng
C. Tính an toàn dựa vào độ khó bài toán logarit rời rạc
D. Kết hợp hàm hash tạo chữ ký điện tử

Câu hỏi trắc nghiệm 3

Câu 5: Trao đổi khoá Diffie Hellman là thủ tục giữa 2 người sử dụng để

A. trao đổi khoá công khai
B. trao đổi khoá mật bằng khoá công khai
C. trao đổi xác nhận khoá công khai (gồm khoá công khai và danh tính)
D. trao đổi khoá mật mới bằng khoá mật cũ

Câu 6: Sự an toàn của trao đổi khoá Diffie Hellman dựa trên

A. việc trao đổi trên kênh riêng của 2 người sử dụng
B. thông qua bên đối tác thứ ba tin cậy
C. độ khó của bài toán logarit rời rạc
D. độ mật của khoá dùng chung cũ

Câu hỏi trắc nghiệm 4

Câu 7: Tìm khẳng định sai trong các câu sau về mã xác thực bản tin

A. Mã xác thực là bản nén của một bản tin về kích thước cố định
B. Mã xác thực phụ thuộc vào bản tin và khoá
C. Mã xác thực có vai trò như chữ ký điện tử
D. Cả bên nhận và bên gửi đều biết thuật toán nén và khoá

Câu 8: Tìm khẳng định đúng trong các câu sau về mã xác thực bản tin

A. Mã xác thực có thể giải mã để nhận lại bản tin
B. Mã xác thực phụ thuộc vào bản tin và khoá
C. Mã xác thực có vai trò như chữ ký điện tử
D. Bên nhận không biết thuật toán mã xác thực và khoá

Câu hỏi trắc nghiệm 5

Câu 9: Tìm khẳng định sai trong các câu sau về hàm hash

A. Hash phụ thuộc vào bản tin và khoá
B. Hash là bản nén của một bản tin về kích thước cố định
C. Hash được coi là dấu vân tay xác định tính toàn vẹn của bản tin
D. Hash dùng kết hợp với khoá công khai tạo chữ ký điện tử trên bản tin

Câu 10: Tìm khẳng định đúng trong các câu sau về hàm hash

A. Hash phụ thuộc vào bản tin và khoá
B. Hash có vai trò như chữ ký điện tử trên bản tin
C. *Hash được coi là dấu vân tay xác định tính toàn vẹn của bản tin
D. Có thể giải mã Hash để khôi phục lại bản tin

Câu hỏi trắc nghiệm 6

Câu 11: Tìm khẳng định đúng trong các câu sau về hàm hash

A. Hash phụ thuộc vào bản tin và khoá
B. Hash có vai trò như chữ ký điện tử trên bản tin
C. Dễ dàng tìm 2 bản tin có cùng Hash
D. *Hash dùng kết hợp với khoá công khai tạo chữ ký điện tử trên bản tin

Câu 12: Tìm khẳng định sai về chữ ký điện tử trong các câu sau

A. Chữ ký điện tử phụ thuộc bản tin và người ký
B. Chữ ký điện tử xác nhận người gửi và nội dung gửi
C. Dùng chữ ký điện tử chống từ chối người gửi
D. *Người nhận có thể tạo ra chữ ký điện tử của người gửi trên bản tin để so sánh

Câu hỏi trắc nghiệm 7

Câu 13: Tìm khẳng định đúng về chữ ký điện tử trong các câu sau

A. Chữ ký điện tử chỉ phụ thuộc vào người ký, không phụ thuộc bản tin
B. * Chữ ký điện tử xác nhận người gửi và nội dung gửi
C. Dùng chữ ký điện tử chống từ chối người nhận
D. Người nhận có thể tạo ra chữ ký điện tử của người gửi trên bản tin để so sánh

Câu 14: Xét chuẩn chữ ký điện tử DSS, khẳng định nào là sai

A. Chọn bộ tham số (p, q, g) gồm 2 số nguyên tố và một căn nguyên tố
B. Mỗi người sử dụng chọn khoá riêng và tính khoá công khai
C. Khi gửi bản tin ký, chọn số ngẫu nhiên và tính hai thành phần chữ ký
D. *Người nhận chỉ dùng một thành phần chữ ký tính thành phần kia rồi so sánh với thành phần thứ hai đính kèm

Câu hỏi trắc nghiệm 8

Câu 15: Chữ ký điện tử DSA, khẳng định nào là đúng

A. Chữ ký người gửi giống nhau trên mọi bản tin
B. Người nhận cũng có thể tạo chữ ký như người gửi
C. *Khi gửi bản tin ký, chọn số ngẫu nhiên và tính hai thành phần chữ ký
D. Người nhận chỉ dùng một thành phần chữ ký tính thành phần kia rồi so sánh với thành phần thứ hai đính kèm

Đáp án câu hỏi trắc nghiệm

- Câu 1
  - D, có thuật toán, nhưng tính rất khó, lâu
- Câu 2
  - B, Người sử dụng phải giữ bí mật khoá riêng của mình
- Câu 3
  - B, An toàn dựa vào bài toán khó phân tích ra tíach hai số nguyên tố rất lớn
- Câu 4
  - C, Tính an toàn dựa vào độ khó bài toán câu 3
- Câu 5
  - B, *trao đổi khoá mật bằng khoá công khai
- Câu 6
  - C, * độ khó của bài toán logarit rời rạc
- Câu 7
  - C, * Mã xác thực không phải là chữ ký điện tử, cả hai người đều có thể tạo ra

Đáp án câu hỏi trắc nghiệm 2

- Câu 8
  - B, Mã xác thực phụ thuộc vào bản tin và khoá
- Câu 9
  - A, *Hash chỉ phụ thuộc vào bản tin
- Câu 10
  - C, Hash được coi là dấu vân tay xác định tính toàn vẹn của bản tin
- Câu 11
  - D, *Hash dùng kết hợp với khoá công khai tạo chữ ký điện tử trên bản tin
- Câu 12
  - D, *Người nhận có thể tạo ra chữ ký điện tử của người gửi trên bản tin để so sánh
- Câu 13
  - B, Chữ ký điện tử xác nhận người gửi và nội dung gửi
- Câu 14
  - D, *Người nhận chỉ dùng một thành phần chữ ký tính thành phần kia rồi so sánh với thành phần thứ hai đính kèm
- Câu 15
  - C, * Khi gửi bản tin ký, chọn số ngẫu nhiên và tính hai thành phần chữ ký

Glossary - Từ điển thuật ngữ

- **Mã khoá đối xứng** còn được gọi là mã khoá đơn hay mật. Ở đây chỉ dùng một khoá, dùng chung cả người nhận và người gửi. Khi khoá này được dùng, việc trao đổi thông tin về khoá sẽ được thỏa thuận trước**.**
- **Mã khoá công khai** ra đời vào đầu những năm 1970. Có thể nói đây là bước tiến quan trọng nhất trong lịch sử 3000 năm mã hoá. Ở đây người ta sử dụng 2 khoá: một khoá riêng và một khoá công khai. Hai khoá này khác nhau, không đối xứng với nhau, do đó mã khoá công khai, còn được gọi là mã không đối xứng.
- **RSA** là mã công khai được sáng tạo bởi Rivest, Shamir & Adleman ở MIT (Trường Đại học Công nghệ Massachusetts) vào năm 1977. RSA là mã công khai được biết đến nhiều nhất và sử dụng rộng rãi nhất hiện nay. Nó dựa trên các phép toán lũy thừa trong trường hữu hạn các số nguyên theo modulo nguyên tố.
- **Trao đổi khoá Diffie Hellman** là sơ đồ khoá công khai đầu tiên được đề xuất bởi Diffie và Hellman năm 1976 cùng với khái niệm khoá công khai. Đây là phương pháp thực tế trao đổi công khai các khoá mật đối xứng.

Glossary - Từ điển thuật ngữ - tiếp

- **Xác thực mẩu tin** liên quan đến các khía cạnh sau khi truyền tin trên mạng
  - Bảo vệ tính toàn vẹn của mẩu tin: bảo vệ mẩu tin không bị thay đổi hoặc có các biện pháp phát hiện nếu mẩu tin bị thay đổi trên đường truyền.
  - Kiểm chứng danh tính và nguồn gốc: xem xét mẩu tin có đúng do người xưng tên gửi không hay một kẻ mạo danh nào khác gửi.
  - Không chối từ bản gốc: trong trường hợp cần thiết, bản thân mẩu tin chứa các thông tin chứng tỏ chỉ có người xưng danh gửi, không một ai khác có thể làm điều đó. Như vậy người gửi không thể từ chối hành động gửi, thời gian gửi và nội dung của mẩu tin.
- **Mã xác thực thông điệp:** Sinh ra bởi một thuật toán mà tạo ra một khối thông tin nhỏ có kích thước cố định: phụ thuộc vào cả mẩu tin và khoá nào đó, giống như mã nhưng không cần phải giải mã, bổ sung vào mẩu tin như chữ ký để gửi kèm theo làm bằng chứng xác thực.

Glossary - Từ điển thuật ngữ - tiếp

- **Hash – băm:** nén mẩu tin bất kỳ về kích thước cố định. Giả thiết là hàm hash là công khai và không dùng khoá. Hash chỉ phụ thuộc mẩu tin. Hash được sử dụng để phát hiện thay đổi của mẩu tin. Hash có thể sử dụng nhiều cách khác nhau với mẩu tin, Hash thường được kết hợp dùng để tạo chữ ký trên mẩu tin.
- **SHA:** thuật toán băm an toàn (Secure Hash Algorithm). SHA có nguồn gốc từ Viện chuẩn công nghệ quốc gia Hoa kỳ - NIST & NSA vào năm 1993, sau đó được nâng cấp vào 1995 theo chuẩn US và chuẩn là FIPS 180-1 1995 và Internet RFC3174. Nó được sử dụng với sơ đồ chữ ký điện tử DSA.
- **Chữ ký điện tử:** được xem như mẩu tin có kích thước cố định được xác thực cung cấp các khả năng để
- kiểm chứng tác giả, ngày và giờ ký, xác thực nội dung mẩu tin, được kiểm chứng bởi bên thứ 3 để chống từ chối. Vì vậy bao gồm hàm xác thực và một số khả năng bổ sung
- **DSS :** Chuẩn chữ ký điện tử, được **c**hính phủ Mỹ ủng hộ từ sơ đồ chữ ký điện tử FIPS 186. Sử dụng thuật toán hash SHA và thuật toán DSS. Tạo 320 bit chữ ký và độ an toàn 512-1024 bit, an toàn phụ thuộc vào độ khó của tính logarit rời rạc.

FAQ – Câu hỏi thường gặp

1. Mã công khai là gì? Khóa riêng và khóa công khai dành cho ai?
2. Tại sao biết khóa công khai lại không biết được khóa riêng? An toàn khóa công khai dựa vào đâu?
3. Nêu cách mã công khai dùng trong bảo mật mẩu tin? Tại sao chỉ dùng mã hóa thông điệp có kích thước nhỏ
4. Nêu cách khóa công khai xác thực người gửi? Và nếu muốn bảo mật cho người nhận thi cần phải làm gi?
5. Nêu các đặc trưng của RSA? an toàn dựa vào đâu? Mô tả sơ đồ sinh khóa RSA trên thực tế?
6. Nêu cách mã và giải mã RSA? Muốn tăng tốc độ cần phải làm gì?
7. Nêu các cách tấn công thám mã RSA

FAQ – Câu hỏi thường gặp (tiếp)

- Thuật toán Diffie-Hellman dùng để làm gì? Mô tả việc sinh khóa công khai.
- Nêu cách 2 người sử dụng tính khóa mật dùng chung? Độ an toán D-H dựa trên cơ sở nào?
- Thế nào là xác thực thông điệp?
- Có các cách nào xác thực thông điệp. Ưu, nhược dùng Mac
- Định nghĩa Hash. Các tính chất cần có của hash.
- Thế nào là nghịch lý ngày sinh nhật. Tấn công dựa vào nó như thế nào
- Mô tả các thao tác của hàm băm SHA1?
- Nêu định nghĩa chữ ký điện tử? Các loại chữ ký?
- Môt tả quá trình sinh khóa, ký và kiểm tra chữ ký DSA?

Trả lời câu hỏi:

1. Mã công khai là mã dùng 2 khóa khác nhau cho 1 NSD; khóa công khai dành cho mọi người mã hoá gửi thông điệp cho người đó hoặc giải mã thông điệp từ người đó, mã riêng dành riêng cho người đó ký hoặc giải mã.
2. Do thuật toán tính khóa riêng từ khóa công khai là bài toán khó, đòi hỏi nhiều thời gian, độ an toàn dựa vào độ khó của bài toán này
3. NSD B dùng khóa công khai của A, mã hóa và gửi cho A. Mã mẩu tin ngắn, vì thời gian mã hóa và giải mã lâu.
4. NSD A mã hóa thông điệp bằng khóa riêng của mình, rồi gửi cho B. Nếu muốn chỉ B nhận được thì sau khi mã bằng khoá riêng của mình A mã hóa tiếp bằng khóa công khai của B.
5. RSA có kích thước khóa riêng và khóa công khai cỡ 512 đến 1024 bit. Độ an toàn dựa vào phân tích 1 số lớn cỡ 1024 thành 2 số cỡ 512 bit. Chọn hai số p, q nguyên tố cùng nhau. Chọn: $e.d=1 \bmod \phi(N)$ với $0 \le d \le \phi(N)$

Trả lời câu hỏi – (tiếp 2)

6. Mã: tính $C = M^e \bmod n$, giải mã: tính $M = C^d \bmod n$. Muốn nhanh sử dụng Định lý phần dư Trung hoa.
7. Tấn công RSA có 3 dạng
   - Phân tích n = p.q, sau đó tính ø(n) và d
   - Tìm n trực tiếp và tính d
   - Tìm d trực tiếp
8. Là sơ đồ trao đổi dùng khoá công khai, có thể thiết lập khoá chung dựa trên khóa riêng của hai đối tác. Chỉ có 2 đối tác tính được khóa chung đó,
9. Giá trị khoá phụ thuộc vào thông tin khoá công khai của đối tác và khoá riêng của mình. Độ an toàn dựa trên độ khó của bài toán tính logarit rời rạc
10. Xác thực mẩu tin liên quan đến
    - Bảo vệ tính toàn vẹn của mẩu tin
    - Kiểm chứng danh tính và nguồn gốc
    - Không chối từ bản gốc

Trả lời câu hỏi – (tiếp)

11. Có 2 hàm lựa chọn: Mã xác thực mẩu tin (MAC), Hàm hash. Sinh ra bởi một thuật toán mà tạo ra một khối nhỏ kích thước cố định, phụ thuộc vào cả mẩu tin và khoá nào đó, giống như mã nhưng không cần phép toán ngược lại. Thuật toán MAC ít công khai, phổ cập, nhiều khi không cần khóa
12. Hash: nén mẩu tin bất kỳ về kích thước cố định như nên dấu vân tay của mẩu tin, giả thiết là hàm hash là công khai và không dùng khoá
13. Nghịch lý ngày sinh nhật: trong lớp có ít nhất 23 sinh viên, để xác xuất có 2 bạn trùng ngày sinh nhật lớn hơn hoặc bằng 0.5. Tấn công ngày sinh nhật hoạt động như sau
    - Kẻ thám mã tạo ra $2^{m/2}$ biến thể của mẩu tin đúng mà tất cả đều có bản chất ngữ nghĩa như nhau và tạo ra $2^{m/2}$ biến thể khác nhau của mẩu tin lừa dối
    - Hai tập tin được so sánh với nhau để tìm cặp có cùng bản hash. Người dùng ký vào mẩu tin đúng, sau đó bị thay thế bằng mẩu tin giả mà cũng có chữ ký đúng.

Trả lời câu hỏi – (tiếp)

14. Tạo nên giá trị Hash 160 bit. Xem bài giảng

15. Chữ ký điện tử cung cấp các khả năng để
    - Kiểm chứng tác giả, ngày và giờ ký
    - Xác thực nội dung mẩu tin
    - Được kiểm chứng bởi bên thứ 3 để chống từ chối

    Có chữ ký trực tiếp và chữ ký có trọng tài

16. DSA tạo 320 bit chữ ký

- Với lựa chọn 512-1024 bit an toàn hơn
- Nhỏ và nhanh hơn RSA
- Có sơ đồ chữ ký điện tử - xem bài giảng
- An toàn phụ thuộc vào độ khó của tính logarit rời rạc

$q = 13$, $p = 4q + 1 = 53$ and $g = 16$.