

Mật mã & Ứng dụng

Trần Đức Khánh

Bộ môn HTTT – Viện CNTT&TT

ĐH BKHN

Chủ đề

- Hệ mật mã cổ điển
 - Hệ mật mã khóa bí mật (đối xứng)
 - Hệ mật mã khóa công khai (bất đối xứng)
 - Hàm băm, chữ ký số
 - Quản lý khóa, giao thức mật mã,...
-

Nhu cầu toàn vẹn thông tin

- Các ứng dụng chú trọng mục tiêu Toàn vẹn
 - Tài liệu được sử dụng giống hệt tài liệu lưu trữ
 - Các thông điệp trao đổi trong một hệ thống an toàn không bị thay đổi/sửa chữa
 - “Niêm phong” tài liệu/thông điệp
 - “Niêm phong” không bị sửa đổi/phá hủy đồng nghĩa với tài liệu/thông điệp toàn vẹn
 - “Niêm phong”: băm (hash), tóm lược (message digest), đặc số kiểm tra (checksum)
 - Tạo ra “niêm phong”: **hàm băm**
-

Hàm băm

- Mục tiêu an toàn
 - Toàn vẹn (Integrity)
-

Hàm băm có khóa

- Đầu vào là một chuỗi có chiều dài biến thiên, và đầu ra có chiều dài cố định

$$h: \sum^* \times K \rightarrow \sum^n$$

- Tin: \sum^*

- Cốt (Digest): \sum^n

- Khóa: K

- h là hàm một chiều (one way function)
 - biết y , rất khó tìm x sao cho $h(x,k)=y$ nhưng rất khó tính
 - h có tính phi đụng độ lỏng (weak collision resistance)
 - cho x , rất khó tìm $y \neq x$ sao cho $h(x,k) = h(y,k)$
 - h có tính phi đụng độ chặt (strong collision resistance)
 - rất khó tìm được $x \neq y$ sao cho $h(x,k) = h(y,k)$
-

Hàm băm không khóa

- Đầu vào là một chuỗi có chiều dài biến thiên, và đầu ra có chiều dài cố định

$$h: \Sigma^* \rightarrow \Sigma^n$$

- Tin: Σ^*

- Cốt (Digest): Σ^n

- h là hàm một chiều (one way function)
 - biết y , rất khó tìm x sao cho $h(x)=y$ nhưng rất khó tính
 - h có tính phi đụng độ lỏng (weak collision resistance)
 - cho x , rất khó tìm $y \neq x$ sao cho $h(x) = h(y)$
 - h có tính phi đụng độ chặt (strong collision resistance)
 - rất khó tìm được $x \neq y$ sao cho $h(x) = h(y)$
-

Kỹ thuật tạo hàm băm

- Dùng các hàm mã hóa
 - CBC
 - RMDP
 - DM
 - Dùng các phép toán số học đồng dư
 - QCMDC
 - DP
 - Dùng các hàm thiết kế đặc biệt
 - MD4/5
 - SHA/SHS
-

Kỹ thuật tạo hàm băm

- Dùng các hàm mã hóa
 - CBC
 - RMDP
 - DM
 - Dùng các phép toán số học đồng dư
 - QCMDC
 - DP
 - Dùng các hàm thiết kế đặc biệt
 - MD4/5
 - SHA/SHS
-

CBC - Chaining Block Cipher

- Mật mã đối xứng
 - Hàm mã hóa E
 - Khóa K
 - Hàm băm
 - $M = M_1M_2...M_n$
 - $H_i = E(K, M_i \text{ xor } H_{i-1})$
 - $H = H_n$
-

RMDP – Rabin, Matyas, Davise, Price

□ Mật mã đối xứng

- Hàm mã hóa E
- Khóa là các khối của tin

□ Hàm băm

- $M = M_1M_2..M_n$
 - $H_0 = r$ (r ngẫu nhiên)
 - $H_i = E(M_i, H_{i-1})$
 - $H = H_n$
-

DM – Davies, Meyer

□ Mật mã đối xứng

- Hàm mã hóa E
- Khóa là các khối của tin

□ Hàm băm

- $M = M_1M_2..M_n$
 - $H_0 = r$ (r ngẫu nhiên)
 - $H_i = E(M_i, H_{i-1}) \text{ xor } H_{i-1}$
 - $H = H_n$
-

Kỹ thuật tạo hàm băm

- Dùng các hàm mã hóa
 - CBC
 - RMDP
 - DM
 - Dùng các phép toán số học đồng dư
 - QCMDC
 - DP
 - Dùng các hàm thiết kế đặc biệt
 - MD4/5
 - SHA/SHS
-

QCMDC – Quadratic Congruential Manipulation Detection Code

- $M = M_1M_2\dots M_n$
 - M_i khối n bit
 - N là số nguyên tố sao cho
 - $N \geq 2^{(n-1)}$
 - Hàm băm
 - $H_0 = r$ (r ngẫu nhiên)
 - $H_i = (H_{i-1} + M_i)^2 \bmod N$
 - $H = H_n$
-

DP – Davies, Price

- $M = M_1M_2\dots M_n$
 - N là số nguyên tố sao cho
 - $N \geq 2^r$
 - Hàm băm
 - $H_0 = 0$
 - $H_i = (H_{i-1} \text{ xor } M_i)^2 \text{ mod } N$
 - $H = H_n$
-

Kỹ thuật tạo hàm băm

- Dùng các hàm mã hóa
 - CBC
 - RMDP
 - DM
 - Dùng các phép toán số học đồng dư
 - QCMDC
 - DP
 - Dùng các hàm thiết kế đặc biệt
 - SHA/SHS
 - MD4/5
-

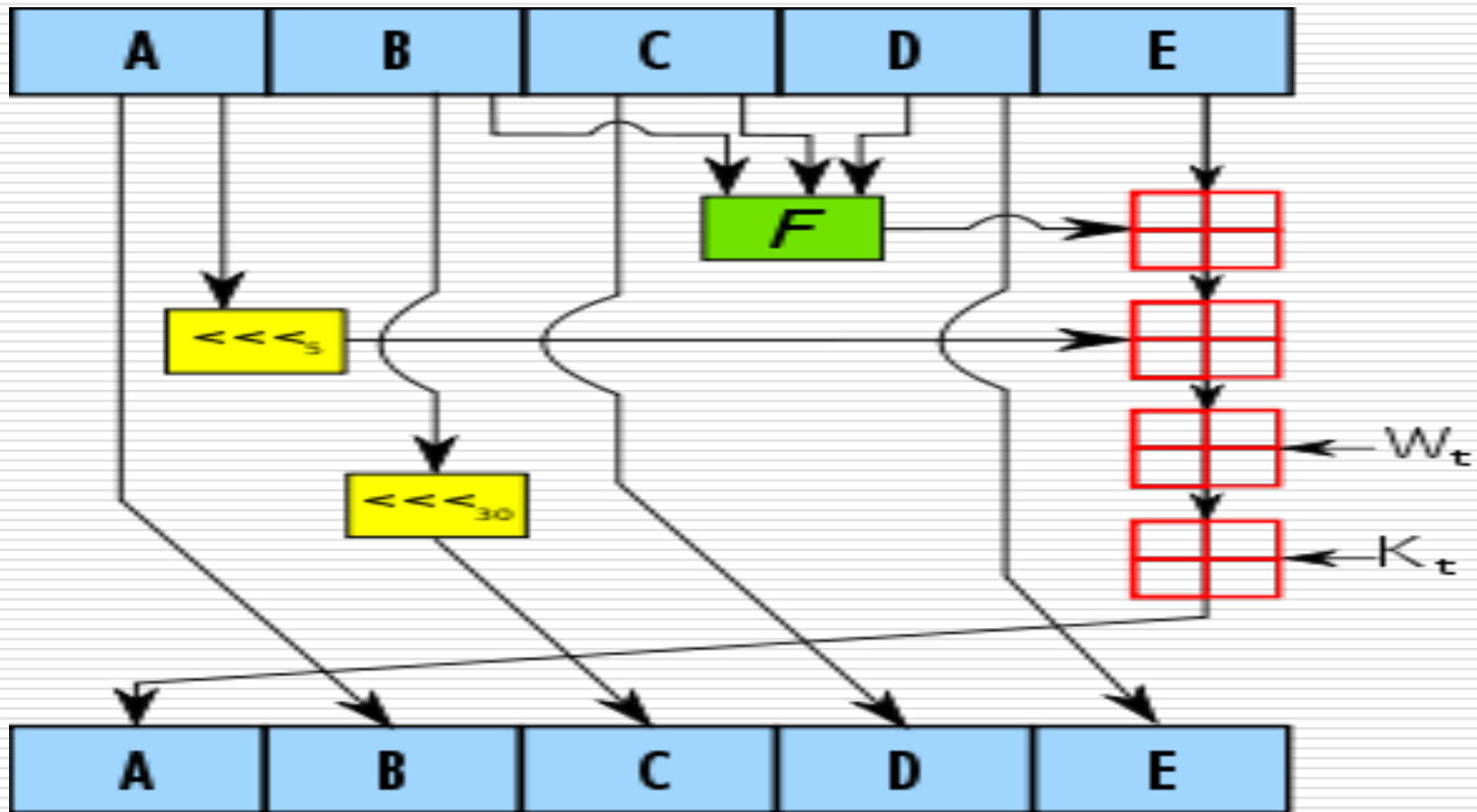
SHA-1

- SHA = Secure Hash Algorithm
 - Được đề xuất và bảo trợ bởi NIST
 - Dùng trong hệ DSS (Digital Signature Standard) của NIST
 - Được sử dụng rộng rãi
 - SSL, PGP, SSH, S/MIME, IPSec
-


SHA-1

- Đầu vào bội số của 512 bit
 - Giá trị băm 160 bit
 - 80 vòng lặp tính toán
-

Vòng lặp SHA-1



Vòng lặp SHA-1

- A,B,C,D,E khối 32 bit
 - Kt hằng số của vòng lặp t
 - W_t được tính từ các khối của Tin
 - \lll dịch chuyển các bit sang trái
 -  cộng modulo 32
 - F là hàm kết hợp các phép toán logic
 - not, and, or, xor
-

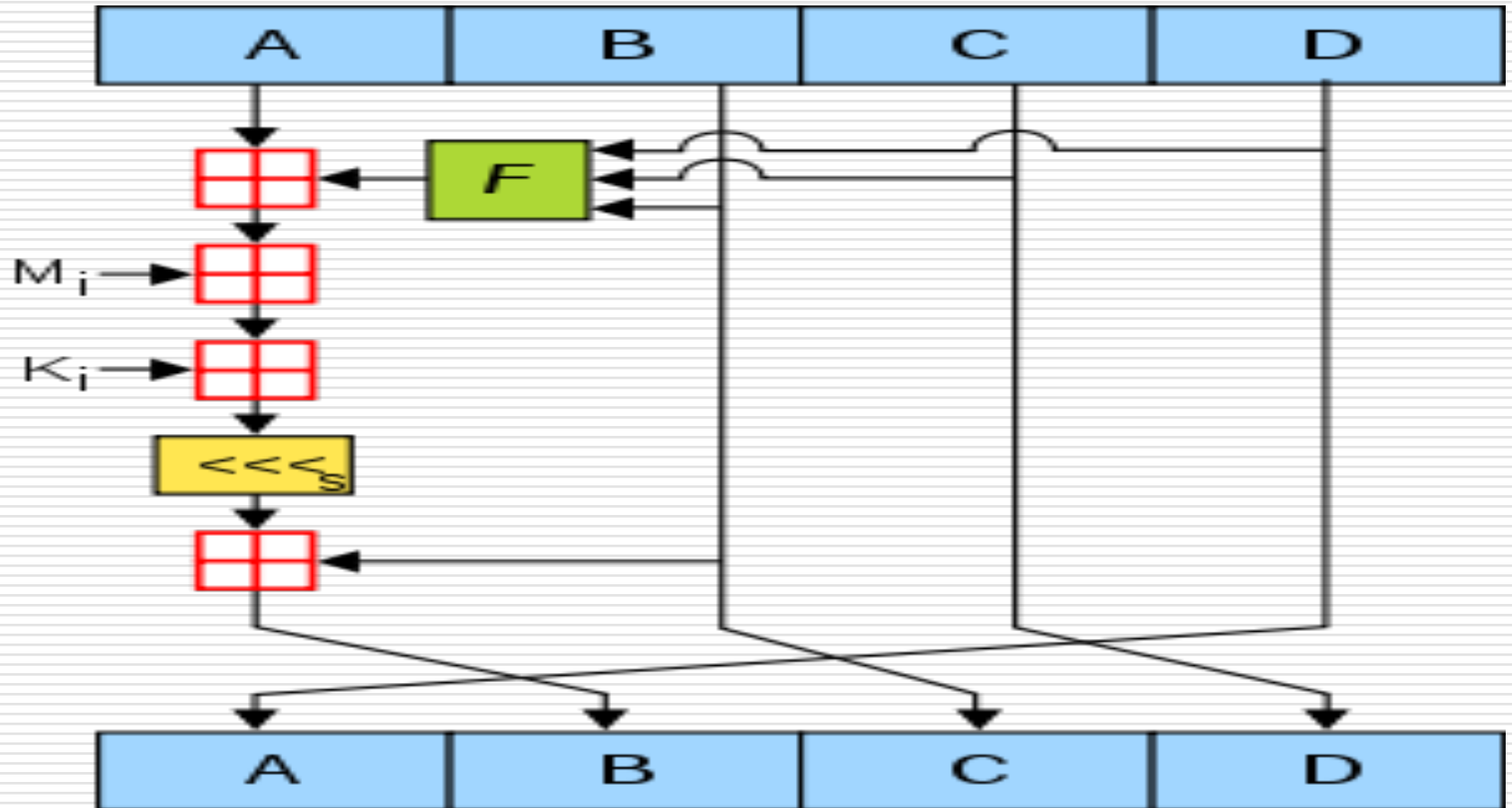
MD5

- MD = Message Digest
 - MD5 được đề xuất bởi Rivest vào năm 1991
 - Được sử dụng rộng rãi
 - Truyền tập tin
 - Lưu trữ mật khẩu
-


MD5

- Đầu vào 512 bit
 - Giá trị băm 128 bit
 - 64 vòng lặp tính toán
-

Vòng lặp MD5



Vòng lặp MD5

- A,B,C,D khối 32 bit
 - Ki hằng số của vòng lặp i
 - Mi khối 32 bit của Tin
 - \lll dịch chuyển các bit
 -  cộng modulo 32
 - F là hàm kết hợp các phép toán logic
 - not, and, or, xor
-

Tấn công Hàm băm

- Đe dọa/mỗi nguy
 - Nghịch lý sinh nhật
 - Trong một nhóm 23 người, xác suất để có hai người có cùng một sinh nhật là không nhỏ hơn $1/2$
 - Tấn công dạng “sinh nhật”
 - Tính N giá trị băm trong thời gian và không gian cho phép
 - Lưu trữ các giá trị băm để tìm ra đụng độ
 - Xác suất đụng độ
 - Nếu $N > 2^{(n/2)}$ giá trị băm, thì xác suất đụng độ là $> 1/2$, trong đó n là độ dài của chuỗi giá trị băm
-

Chữ ký số

- 1976, Diffie & Hellman lần đầu tiên đề cập đến khái niệm Chữ ký số
 - 1989, phiên bản thương mại Chữ ký số đầu tiên trong Lotus Notes, dựa trên RSA
 - Ứng dụng
 - Hợp đồng số
 - Bầu cử điện tử
 - Giao dịch ngân hàng
 - ...
-

Chữ ký số

- Mục tiêu an toàn
 - Xác thực (Authentication)
 - Chống phủ nhận (Non-repudiation)
-

Hệ chữ ký số

- Thuật toán tạo chữ ký
 - Ký hiệu S
 - Đầu vào là một thông tin m
 - Chữ ký $S(m)$
 - Thuật toán kiểm định chữ ký
 - Ký hiệu V
 - Đầu vào là thông tin m và chữ ký kèm theo s
 - $V(m, s) = true$ khi và chỉ khi $s = S(m)$
-

Kỹ thuật tạo Chữ ký số

- Mật mã khóa công khai
 - Mật mã khóa công khai + Hàm băm
 - RSA + Hàm băm
 - ElGamal + Hàm băm
 - DSA
-

Chữ ký số dùng Mật mã khóa công khai

□ RSA

- Chọn ngẫu nhiên 2 số nguyên tố p, q
 - $n = p * q$
 - Chọn e sao cho
 - $1 < e < (p-1) * (q-1)$
 - $\text{ƯSCLN}(e, (p-1) * (q-1)) = 1$
 - Chọn d sao cho
 - $1 < d < (p-1) * (q-1)$
 - $e * d = 1 \text{ mod } (p-1) * (q-1)$
 - Khóa công khai: (n, e)
 - Khóa riêng: (p, q, d)
-

Chữ ký số dùng RSA

- Tin m
 - Khóa công khai (n, e)
 - Khóa riêng (p, q, d)
 - Tạo chữ ký
 - $s = m^d \bmod n$
 - Kiểm định chữ ký
 - $m =? s^e \bmod n$
-

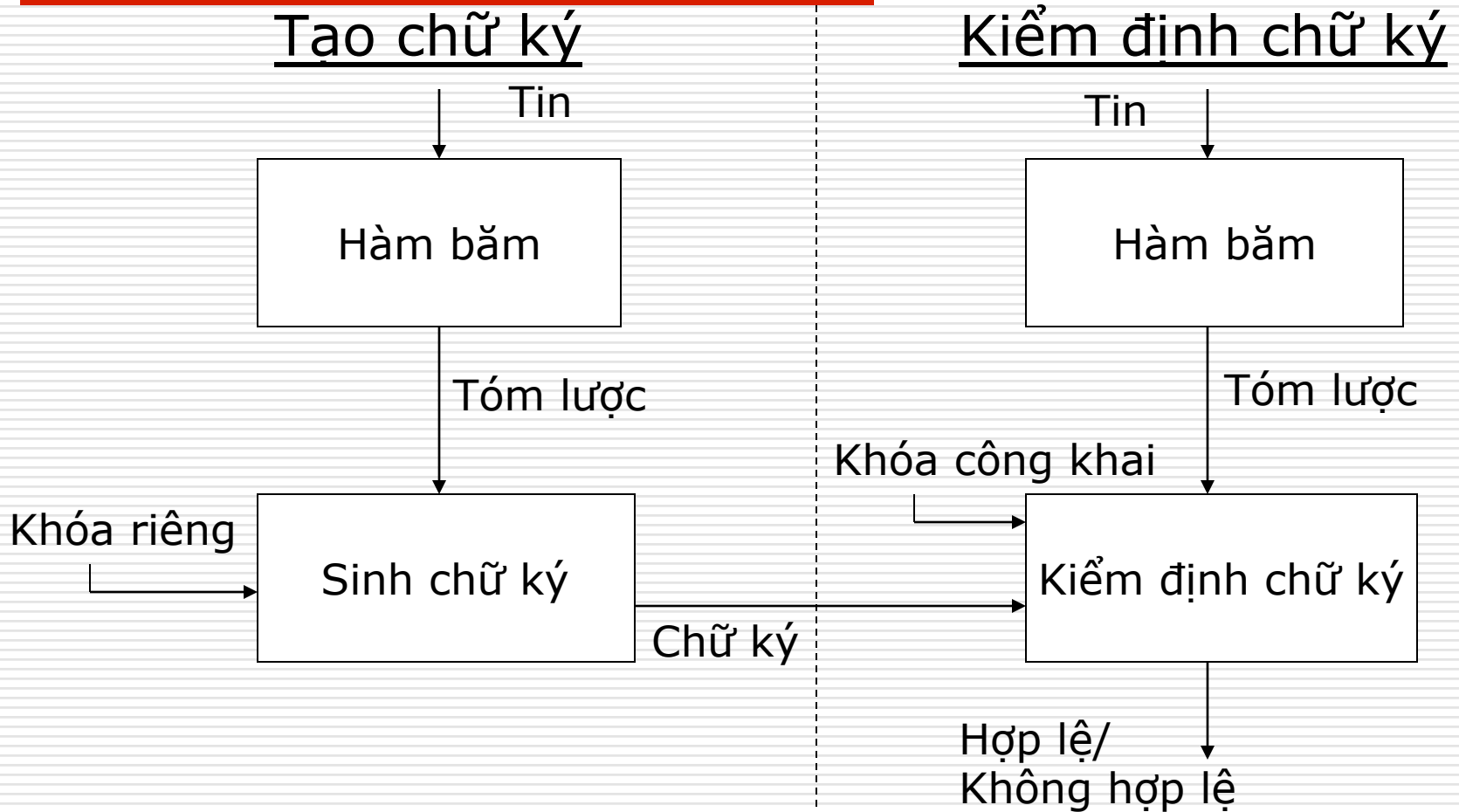
Chữ ký số dùng RSA

- Đe dọa/mối nguy
 - Tấn công dạng “chọn tin”, dựa trên đặc điểm “nhân tính” của RSA
 - Nếu $m1^d \bmod n$ là chữ ký của $m1$, $m2^d \bmod n$ là chữ ký của $m2$, thì $(m1*m2)^d \bmod n$ là chữ ký của $m1*m2$
 - Tấn công dạng “không Tin”
 - Lấy khóa công khai k của Alice
 - Tạo tin m và chữ ký s của m sao cho m và s được công nhận bởi thuật toán kiểm định sử dụng k
-

Chữ ký số dùng Mật mã khóa công khai + Hàm băm

- Tăng cường độ an toàn bằng kết hợp
 - Hệ mật mã khóa công khai
 - Hàm băm
 - Thuật toán tạo chữ ký
 - Hàm mã hóa sử dụng khóa riêng
 - Hàm băm
 - Thuật toán kiểm định chữ ký
 - Hàm giải mã sử dụng khóa công khai
 - Hàm băm
-

Chuẩn Chữ ký số - DSS



Chữ ký số RSA + Hàm băm

- Các thông số
 - Hàm băm h
 - 2 số nguyên tố p, q
-

Chữ ký số RSA + Hàm băm

□ Tạo khóa

- $n = p * q$
 - Chọn e sao cho
 - $1 < e < (p-1) * (q-1)$
 - $\text{ƯSCLN}(e, (p-1) * (q-1)) = 1$
 - Chọn d sao cho
 - $1 < d < (p-1) * (q-1)$
 - $e * d = 1 \text{ mod } (p-1) * (q-1)$
 - Khóa công khai
 - (n, e)
 - Khóa riêng
 - (p, q, d)
-

Chữ ký số RSA + Hàm băm

□ Tạo chữ ký

- Tin m

- Chữ ký

- $s = h(m)^d \bmod n$

Chữ ký số RSA + Hàm băm

- Kiểm định chữ ký
 - Chữ ký s
 - Tin m
 - Kiểm định
 - $h(m) \stackrel{?}{=} s^e \bmod n$
-

Chữ ký số ElGamal + Hàm băm

- Các thông số
 - Hàm băm h
 - Số nguyên tố p
 - Số nguyên g sao cho
 - $g^c = b \pmod p$
trong đó b, p nguyên tố cùng nhau
-

Chữ ký số ElGamal + Hàm băm

□ Tạo khóa

- Chọn a sao cho $0 < a < p-1$

- $A = g^a \text{ mod } p$

- a được gọi là logarit rời rạc của A

- Khóa công khai

- (p, g, A)

- Khóa riêng

- a

Chữ ký số ElGamal + Hàm băm

□ Tạo chữ ký

■ Tin m

■ Chọn k sao cho

□ $0 < k < p-1$

□ k nguyên tố cùng nhau với $p-1$

■ Chữ ký

□ $r = g^k \bmod p$

□ $s = k^{-1} * (h(m) - a*r) \bmod (p-1)$

Chữ ký số ElGamal + Hàm băm

- Kiểm định chữ ký
 - Chữ ký (r,s)
 - Tin m
 - Kiểm định
 - $0 < r < p$
 - $0 < s < p-1$
 - $A^r * r^s \stackrel{?}{=} g^{h(m)} \text{ mod } p$
-

Chữ ký số DSA

- Các thông số
 - Hàm băm h
 - Số nguyên tố q
 - Số nguyên p sao cho
 - $p-1$ là bội số của q
 - Số nguyên g sao cho
 - $g = x^{((p-1)/q)} \bmod p$
trong đó $x < p$
-

Chữ ký số DSA

- Tạo khóa
 - Chọn $a < q$
 - $A = g^a \text{ mod } p$
 - Khóa công khai
 - (p, q, g, A)
 - Khóa riêng
 - a
-

Chữ ký số DSA

□ Tạo chữ ký

- Tin m

- Chọn k sao cho $0 < k < q$

- Chữ ký

- $r = (g^k \bmod p) \bmod q$

- $s = k^{-1} * (h(m) + a*r) \bmod q$

Chữ ký số DSA

□ Kiểm định chữ ký

- Chữ ký (r, s)

- Tin m

- Kiểm định

- $0 < r < q$

- $0 < s < q$

- $r = ((g^{(s^{-1}) * h(m) \bmod q} A^{(r * s^{-1}) \bmod q}) \bmod p) \bmod q$
