TRƯỜNG ĐẠI HỌC KỸ THUẬT – CÔNG NGHỆ CẦN THƠ

AN TOÀN CÁC HỆ THỐNG THÔNG TIN

ThS. Nguyễn Văn Kha

dzokha1010@gmail.com

Chương 4
CHỮ KÝ ĐIỆN TỬ VÀ CHỨNG CHỈ SỐ

4.1. Khái niệm chữ ký điện tử

4.2. Chữ ký số

3.3. Chứng chỉ số

3.4. Ứng dụng hàm băm

4.1. Khái niệm chữ ký điển tử

Chữ ký điện tử (Electronic Signature hay E-Signature) là thông tin đi kèm theo dữ liệu (văn bản, hình ảnh, video...) nhằm mục đích xác định người chủ của dữ liệu đó.

Chữ ký điện tử có giá trị pháp lý tương đương như chữ ký viết tay, miễn là nó tuân theo các yêu cầu của quy chế cụ thể mà nó được tạo ra.

4.1. Khái niệm chữ ký điển tử (tt)

Sự khác biệt cơ bản giữa chữ ký điện tử và chữ ký thông thường (chữ ký tay)?

- Do con người tác động lên giấy, có sẳn, độc lập, rất khó để giả mạo.
- Trong thế giới số hóa, văn bản số hóa

4.1. Khái niệm chữ ký điển tử (tt)

Có 03 loại chữ ký điện tử

- Chữ ký điện tử đơn giản: hình ảnh quét chữ ký, tên đã đánh máy hoặc biểu diễn kỹ thuật số đơn giản của chữ ký.

- Chữ ký điện tử nâng cao: sử dụng kỹ thuật mật mã để cung cấp mức độ đảm bảo an ninh cao, sử dụng hạ tầng khoá công khai để chứng thực số.

- Chữ ký điện tử đủ điều kiện: đòi hỏi nhà cung cấp dịch vụ tin cầy đủ điều kiện và một chứng chỉ kỹ thuật số. Đáp ứng các tiêu chuẩn pháp lý nghiêm ngặt.

4.1. Khái niệm chữ ký điển tử (tt)

Chữ ký điện tử là một khái niệm pháp lý khác biệt với chữ ký số (Digital Signature), Chữ ký số là một cơ chế mã hóa thường được sử dụng để triển khai chữ ký điện tử.

Chữ ký số là một loại chữ ký điện tử cụ thể, sử dụng các kỹ thuật mã hóa (ví dụ: RSA hoặc DSA) để tạo ra chữ ký số độc nhất liên quan đến nội dung của tài liệu và khóa riêng của người ký.

4.2. Chữ ký số
4.2.1. Tổng quan về xác thực và chữ ký số

Xác thực và chữ ký điện tử là một trong những lĩnh vực hấp dẫn và phức tạp nhất của mật mã học

Xác thực là một thủ tục để xác minh rằng tin nhắn đã nhận đến từ nguồn gửi và không bị thay đổi. Xác thực tin nhắn cũng có thể xác minh trình tự và thời gian để đảm bảo tính kịp thời.

Chữ ký số là một kỹ thuật xác thực phổ biến, giúp xác thực tin nhắn và chống lại sự từ chối trách nhiệm từ phía nguồn gửi.

4.2. Chữ ký số
4.2.1. Tổng quan về xác thực và chữ ký số

Các rủi ro có thể xảy ra khi truyền thông qua mạng:

1. Tiết lộ: Phát hành nội dung tin nhắn (TN) cho bất kỳ người hoặc quy trình nào không sở hữu khóa.
2. Phân tích lưu lượng: Khám phá mô hình lưu lượng giữa các bên. Trong ứng dụng hướng kết nối, tần suất và thời lượng kết nối có thể được xác định.
3. Giả mạo: Chèn TN vào mạng từ một nguồn gian lận.
4. Sửa đổi nội dung: Thay đổi nội dung của TN.
5. Sửa đổi trình tự: Bất kỳ sửa đổi nào đối với trình tự TN giữa các bên.
6. Sửa đổi thời gian: Trì hoãn hoặc phát lại TN.
7. Từ chối nguồn: Từ chối truyền TN bởi nguồn.
8. Từ chối đích: Từ chối nhận TN bởi đích.

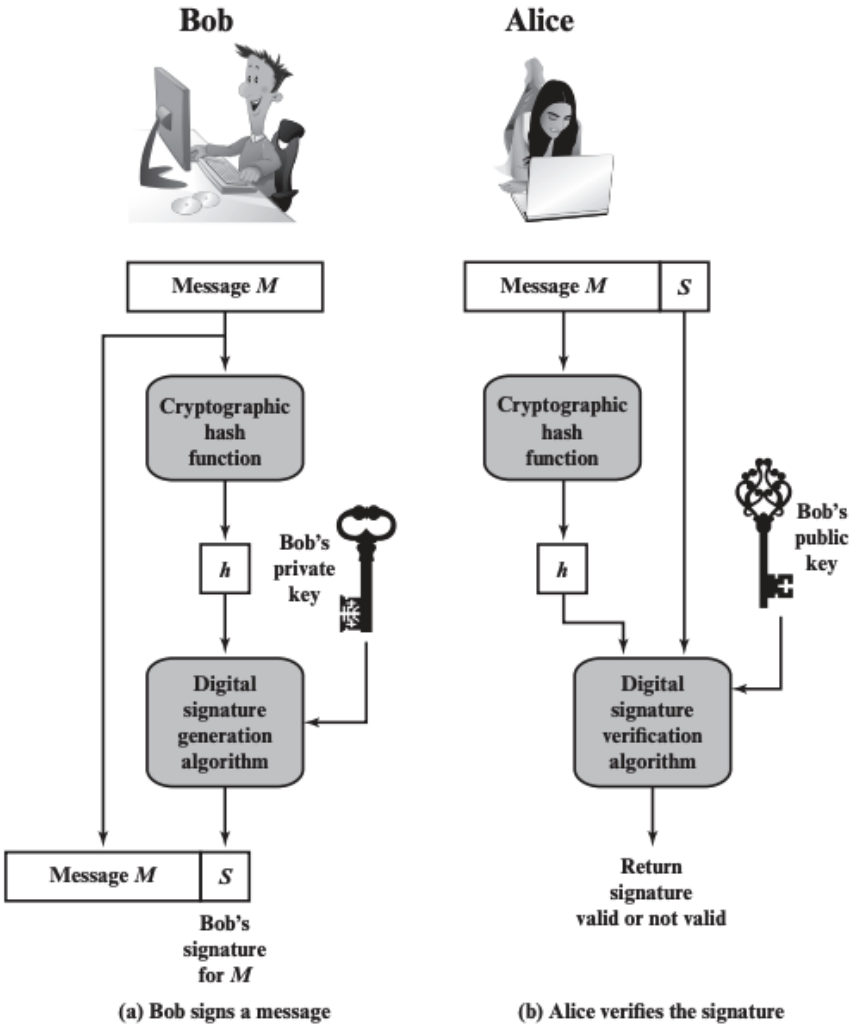
4.2. Chữ ký số
4.2.1. Tổng quan về xác thực và chữ ký số

Chữ ký số là giải pháp xử lý trong tình huống không có sự tin tưởng hoàn toàn giữa người gửi và người nhận,

Chữ ký số phải có các thuộc tính sau:

- Nó phải xác minh tác giả và ngày giờ của chữ ký.
- Nó phải xác thực nội dung tại thời điểm ký.
- Nó phải có thể được bên thứ ba xác minh để giải quyết tranh chấp.

4.2. Chữ ký số
4.2.1. Tổng quan về xác thực và chữ ký số



- Bước 1: Bob tạo gía trị băm cho tin TN
- Bước 2: Bob tạo chữ ký điện tử sử dụng gía trị băm và khoá riêng.
- Bước 3: Bob gửi TN kèm theo chữ ký
- Bước 4: Khi Alice nhận TN và chữ ký, đầu tiên Alice tính toán giá trị băm cho TN
- Nước 5: Alice xác minh chữ ký số bằng giá trị băm và khoá công khai của Bob.

Quy trình xây dựng và sử dụng chữ ký số

4.2. Chữ ký số
4.2.1. Tổng quan về xác thực và chữ ký số (tt)

Các cuộc tấn công nhằm vào chữ ký số:

- Tấn công khóa: kẻ tấn công (C) cố gắng xác định khoá riêng của A.
- Tấn công tin nhắn đã biết: C dựa vào các tập hợp các tin nhắn và chữ ký được thu thập để phá vỡ hệ thống
- Tấn công tin nhắn được chọn chung: C chọn một danh sách các tin nhắn trước khi cố gắng phá vỡ lược đồ chữ ký của A. Sau đó, C lấy từ A các chữ ký hợp lệ cho các tin nhắn đã chọn. Cuộc tấn công này nhằm vào hệ thống, vì nó không phụ thuộc vào khóa công khai của A; cùng một cuộc tấn công được sử dụng với tất cả mọi người.
- Tấn công tin nhắn được chọn có hướng: Tương tự như cuộc tấn công chung, nhưng C chỉ chọn các tin nhắn sau khi biết khóa công khai của A. Tuy nhiên, C chưa xem bất kỳ chữ ký nào trước khi đưa ra danh sách tin nhắn cần ký.
- Tấn công tin nhắn được chọn thích ứng: C có thể yêu cầu từ A các chữ ký của các tin nhắn phụ thuộc vào các cặp chữ ký-tin nhắn đã lấy trước đó

4.2. Chữ ký số
4.2.1. Tổng quan về xác thực và chữ ký số (tt)

Các trường hợp phá vỡ chữ ký số:

- Phá vỡ hoàn toàn: C xác định khóa riêng của A.
- Làm giả phổ quát: C tìm ra một thuật toán tạo chữ ký hiệu hiệu quả, cho phép tạo chữ ký hợp lệ cho bất kỳ thông điệp mà không cần thiết khoá riêng của A.
- Làm giả có chọn lọc: C làm giả chữ ký cho một thông điệp cụ thể do C chọn, nghĩa là họ chỉ cần tạo được chữ ký hợp lệ cho một thông điệp mà họ chọn.
- Làm giả hiện sinh: C làm giả chữ ký cho ít nhất một thông điệp. C không kiểm soát được thông điệp. Do đó, việc làm giả này chỉ có thể là một phiền toái nhỏ đối với A.

4.2. Chữ ký số
4.2.1. Tổng quan về xác thực và chữ ký số

Yêu cầu đối với chữ ký số:

- Chữ ký phải là một mẫu bit phụ thuộc vào thông điệp được ký.
- Chữ ký phải sử dụng một số thông tin mà chỉ người gửi biết để ngăn chặn cả việc làm giả và phủ nhận.
- Việc tạo ra chữ ký số phải tương đối dễ dàng.
- Việc nhận dạng và xác minh chữ ký số phải tương đối dễ dàng.
- Việc làm giả chữ ký số phải không khả thi về mặt tính toán, bằng cách xây dựng một thông điệp mới cho một chữ ký số hiện có hoặc bằng cách xây dựng một chữ ký số gian lận cho một thông điệp nhất định.
- Việc lưu giữ một bản sao của chữ ký số trong bộ nhớ phải thực tế.

4.2. Chữ ký số
4.2.2. Chữ ký RSA

+ Thuật toán RSA tạo khoá

Lựa chọn khóa chung và khóa riêng: 2 số nguyên tố p và q

Tính $n = p*q$ và $z = (p - 1)(q - 1)$.

Chọn e là số nguyên tố cùng nhau z: $gcd(e,z) = 1$, $1 < e < z$

Tìm d: $e*d \bmod z = 1$.

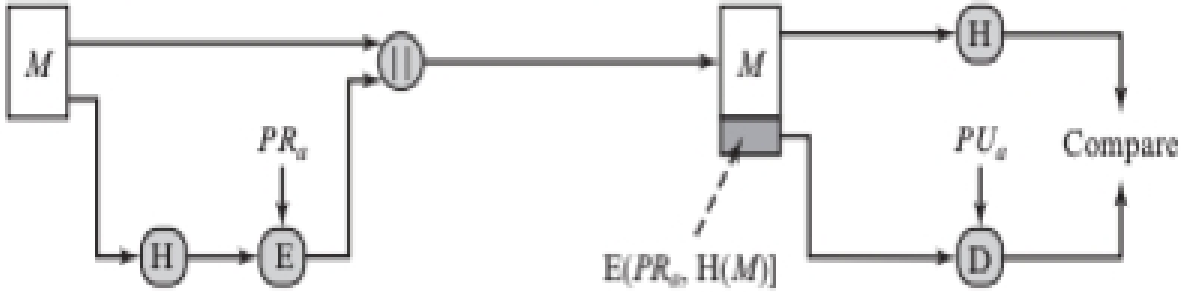
Khoá công khai PK = {n, e}; Khoá riêng SK = {n,d}

+ Thuật toán mã hóa và giải mã

Ciphertext $c = m^e \bmod n$

Plaintext $m = c^d \bmod n$

4.2. Chữ ký số
4.2.2. Chữ ký RSA



Phía gửi: Ký số

(M, E(PR$_a$,H(M))

M: thông điệp cần ký

E (PR$_a$,H(M)) là chữ ký

- Dữ liệu đầu vào tạo chữ ký:

+ Giá trị băm H

+ Khóa riêng SK của người gửi (PRa)

Phía nhận: Xác minh

- Giá trị băm H'

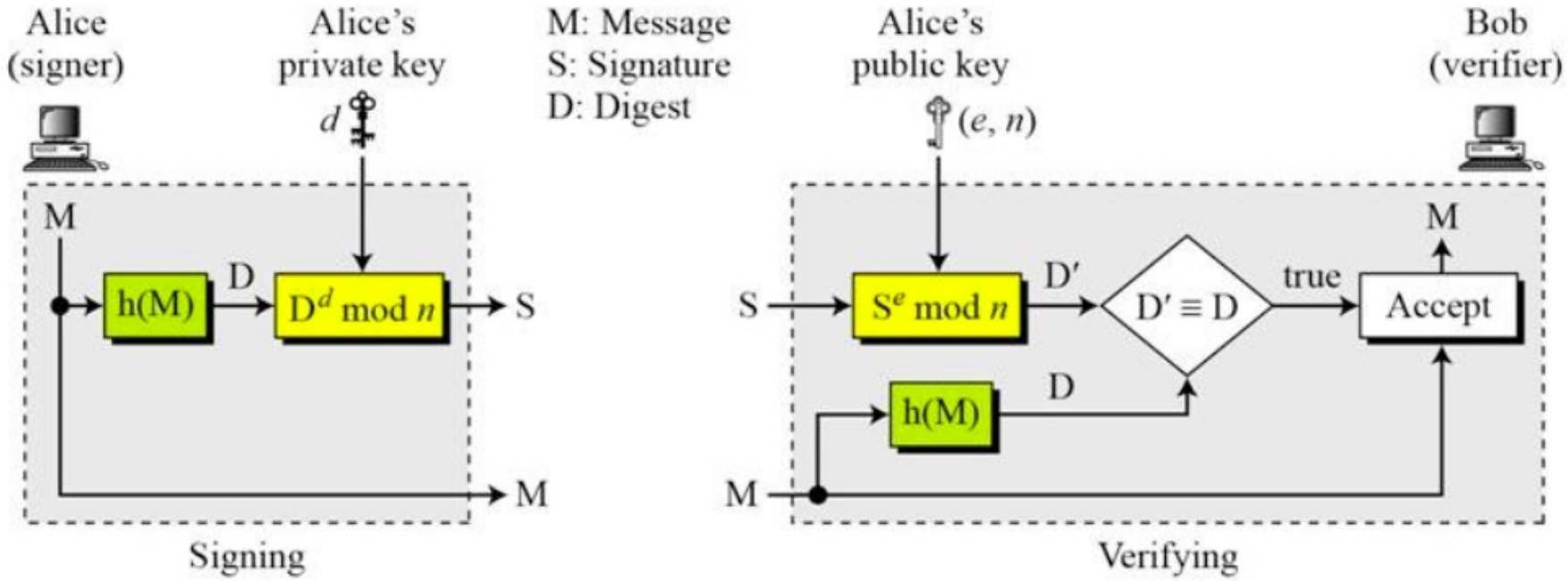
- Dữ liệu đầu vào hàm xác minh:

+ Chữ ký số E(PRa,H(M))

+ Khoá công khai PK hay (PU$_a$)

- Kết quả: H' = H xác minh hợp lệ

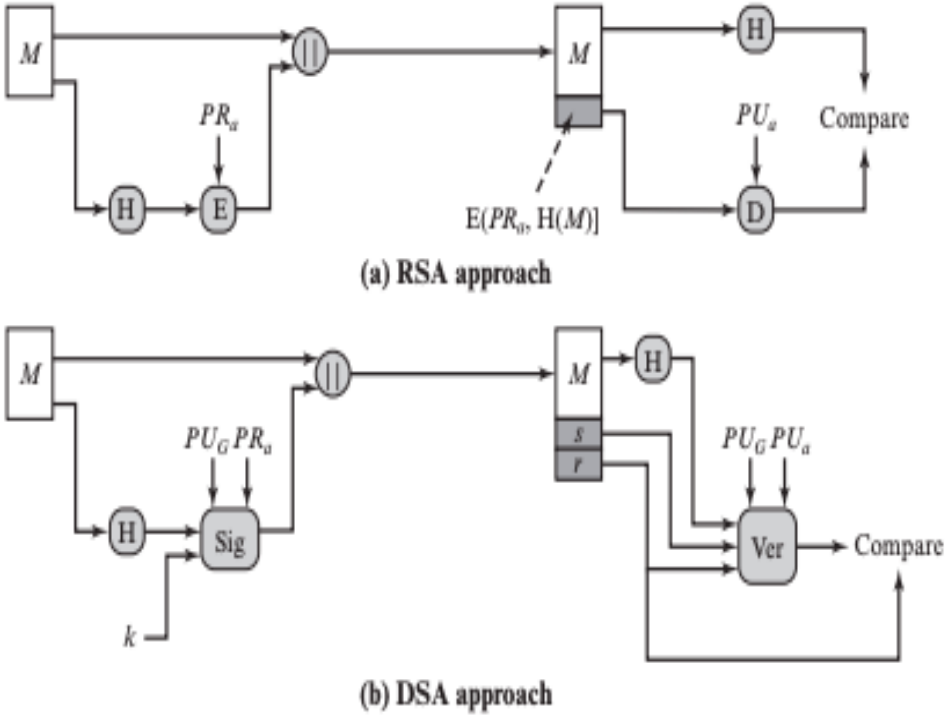
4.2. Chữ ký số
4.2.2. Chữ ký RSA



Mô tả chức năng ký và xác minh của RSA

4.2. Chữ ký số
4.2.3. Chữ ký DSA

Lược đồ



Phía gửi: Ký số

- Dữ liệu đầu vào tạo chữ ký:
  - Giá trị băm
  - Số ngẫu nhiên k được tạo cho chữ ký cụ thể này.
  - Khóa riêng của người gửi (PR_a)
  - Khóa công khai toàn cầu (PU_G): một tập hợp các tham số được một nhóm các nguyên tắc giao tiếp biết đến.
- Kết quả: Chữ ký bao gồm hai thành phần, được gắn nhãn là s và r.

Phía nhận: Xác minh

- Dữ liệu đầu vào hàm xác minh: (Giá trị băm, PU_G, $PU_{a)}$
- Kết quả: một giá trị bằng với thành phần chữ ký r nếu chữ ký hợp lệ.

4.2. Chữ ký số
4.2.3. Chữ ký DSA (tt)

Thuật toán

Khoá toàn cầu PU_G

- Chọn số nguyên tố p: $2^{L-1} < p < 2^L$; $512 <= L <= 1024$
- Chọn một số nguyên tố q N bit, chia hết cho p; $2^{N-1} < q < 2^N$
- $g = h^{(p-1)/q} \bmod p > 1$

Khoá riêng x: $0 < x < q$

Khóa công khai y: $g^x \bmod p$

Khoá bí mật k: $0 < k < q$

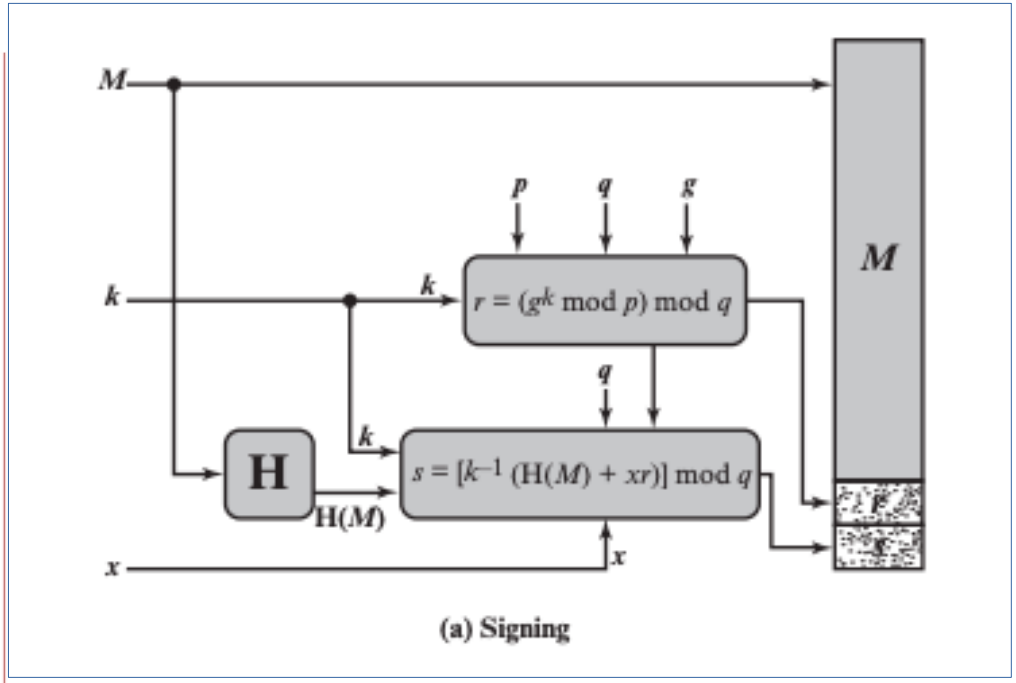
Chữ ký DSA

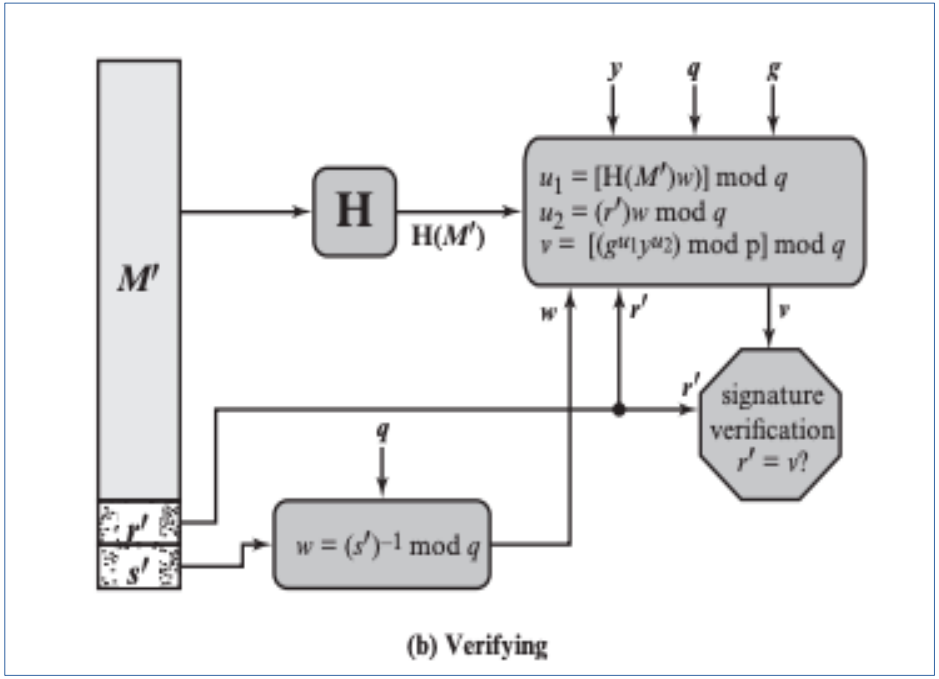
- $R = (g^k \bmod p) \bmod q$
- $S = [k^{-1} (H(M) + xr)] \bmod q$
- Signature = (r,s)

Xác minh

- $W = (s')^{-1} \bmod q$
- $U_1 = [H(M')w] \bmod q$
- $U_2 = (r')w \bmod q$
- $V = [(g^{u1}y^{u2}) \bmod p] \bmod q$
- TEST: v = r'

4.2. Chữ ký số
4.2.3. Chữ ký DSA (tt)





Mô tả chức năng ký và xác minh

4.3. Chứng chỉ số
4.3.1. Khái niệm

Chứng chỉ số (Digital Certificate), hay còn gọi là chứng chỉ khóa công khai, là một tệp kỹ thuật số chứa các thông tin quan trọng như: tên người dùng, khóa công khai của họ, ngày cấp, tên của cơ quan cấp chứng chỉ (CA - Certificate Authority) và thời hạn hiệu lực của khóa. Để giảm dung lượng, CA không mã hóa toàn bộ chứng chỉ mà chỉ mã hóa giá trị băm của nó bằng khóa riêng. Quá trình này được gọi là ký chứng chỉ. Chứng chỉ này cho phép người dùng trên mạng xác thực khóa công khai của nhau.

Để xác thực chứng chỉ, CA sử dụng chứng chỉ khóa công khai và công khai khóa của mình trên trang web để người dùng có thể kiểm tra tính hợp lệ

4.3. Chứng chỉ số
4.3.1. Khái niệm (tt)

Cơ sở hạ tầng khoá công khai (PKI – Public Key Infrastructure) hỗ trợ và quản lý các chứng chỉ khoá công khai và mạng lưới CA. Cụ thể PKI thiết lập các chức năng sau:

1. Xác định tính hợp pháp của người dùng trước khi cấp chứng chỉ khóa công khai cho họ.

2. Cấp chứng chỉ khóa công khai theo yêu cầu của người dùng.

3. Kéo dài thời gian hiệu lực của chứng chỉ khóa công khai theo yêu cầu của người dùng.

4. Thu hồi chứng chỉ khóa công khai theo yêu cầu của người dùng hoặc khi khóa riêng tương ứng bị xâm phạm.

5. Lưu trữ và quản lý chứng chỉ khóa công khai.

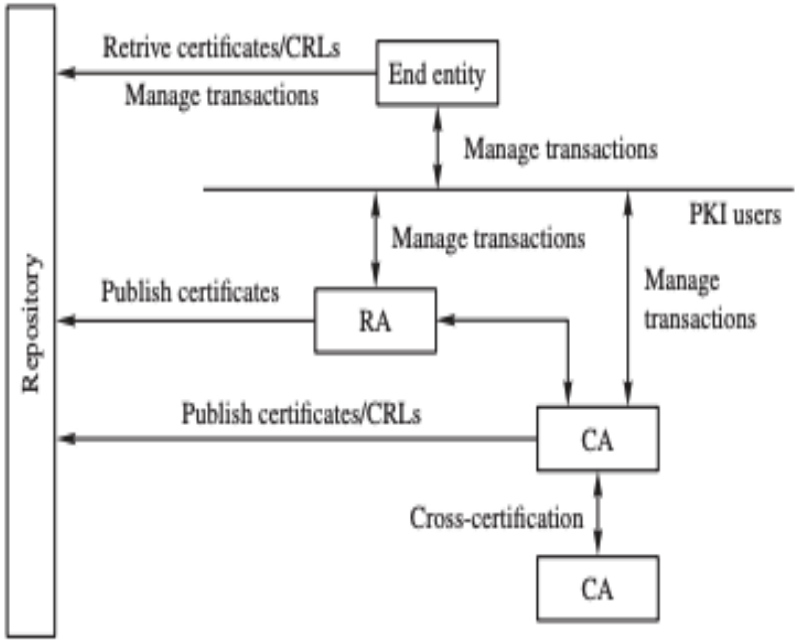
6. Ngăn chặn người ký chữ ký số từ chối chữ ký của họ.

7. Hỗ trợ các mạng CA để cho phép các CA khác nhau xác thực các chứng chỉ khóa công khai do các CA khác cấp

4.3. Chứng chỉ số
4.3.1. Cơ sở hạ tầng khoá công khai X.509

X.509 là một cơ sở hạ tầng khóa công khai do Ngành tiêu chuẩn hóa viễn thông của Liên minh viễn thông quốc tế (ITU) thiết lập vào năm 1988. Nó cũng được gọi là tiêu chuẩn PKIX. PKIX bao gồm bốn thành phần cơ bản sau: thực thể cuối, cơ quan cấp chứng chỉ (CA), cơ quan đăng ký (RA - Registration Authority) và kho lưu trữ. Một thực thể có nghĩa là bất kỳ người dùng nào của chứng chỉ khóa công khai hoặc bất kỳ thiết bị nào (ví dụ: máy chủ và bộ định tuyến) hỗ trợ PKIX. Các thành phần này có các chức năng sau:

4.3. Chứng chỉ số
4.3.1. Cơ sở hạ tầng khoá công khai X.509 (tt)



Kiến trúc PKIX

Quản lý giao dịch giữa thực thể cuối, CA, RA và kho lưu trữ bao gồm các mục sau:

1. Đăng ký: Người dùng đăng ký với CA hoặc RA để được cấp chứng chỉ.

2. Khởi tạo: Người dùng có được thông tin ban đầu, bao gồm khóa công khai của CA/RA và thuật toán chữ ký.

3. Phát hành và công bố chứng chỉ: CA hoặc RA phát hành và công bố chứng chỉ trong kho lưu trữ.

4. Phục hồi khóa: CA hoặc RA cung cấp các cơ chế cần thiết để người dùng phục hồi khóa riêng đã mất.

5. Tạo khóa: CA hoặc RA định kỳ tạo cặp khóa mới cho người dùng.

6. Thu hồi chứng chỉ: Người dùng yêu cầu CA hoặc RA thu hồi chứng chỉ nếu gặp sự cố với khoá riêng.

7. Chứng nhận chéo: Các CA có thể xác thực các chứng chỉ của nhau.

4.3. Chứng chỉ số
4.3.1. Cơ sở hạ tầng khoá công khai X.509 (tt)

Định dạng chứng chỉ X.509 (Version 3 phát hành 1996) là định dạng chứng chỉ phổ biến nhất được sử dụng hiện nay. Nó bao gồm:

1. Phiên bản (Version): Xác định phiên bản chứng chỉ.

2. Số Serial: Mã số duy nhất của chứng chỉ trong CA.

3. Thuật toán (Algorithm): Hàm băm và thuật toán mã hóa khóa công khai được sử dụng để ký số cho chứng chỉ.

4. Người phát hành (Issuer): Tên của CA cấp chứng chỉ.

5. Thời hạn hiệu lực (Validity Period): Thời gian chứng chỉ có giá trị.

6. Chủ thể (Subject): Tên của người sở hữu chứng chỉ.

7. Khóa công khai (Public key): Thông tin khóa công khai và thuật toán liên quan.

8. Phần mở rộng (Extension): Thông tin bổ sung về mục đích của khoá (Chỉ có trong Version 3)

9. Thuộc tính (Properties): Chữ ký chứng chỉ (giá trị băm được mã hóa) và thông tin khác.

4.4. Ứng dụng hàm băm
4.4.1. Giới thiệu hàm băm

Một hàm băm lấy một chuỗi dài làm đầu vào, chia nó thành nhiều phần, trộn chúng lại và tạo ra một chuỗi mới có độ dài ngắn hơn. Không phải mọi hàm băm đều phù hợp để tạo dấu vân tay kỹ thuật số (Digital Fingerprint).

Để phù hợp tạo dấu vân tay, hàm băm phải đáp ứng một số tiêu chí:

- Thuộc tính một chiều đảm bảo rằng việc tính toán dấu vân tay kỹ thuật số cho một chuỗi nhất định là dễ dàng nhưng việc tìm một chuỗi có dấu vân tay nhất định là khó.
- Thuộc tính duy nhất tính toán đảm bảo rằng rất khó để tìm ra hai chuỗi khác nhau có cùng dấu vân tay. Có hai loại duy nhất tính toán; đó là khả năng chống va chạm và khả năng chống va chạm mạnh.

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

MD5 được Ronald Rivest tại MIT phát triển vào năm 1992.

Thuật toán này lấy một thông điệp đầu vào có độ dài tùy ý và tạo ra giá trị băm 128 bit của thông điệp đó. Thông điệp đầu vào được xử lý theo các khối 512 bit có thể chia thành mười sáu khối con 32 bit.

Digest là một tập hợp bốn khối 32 bit, nối lại với nhau để tạo thành một mã băm 128 bit duy nhất.

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

a) Nối thêm các bit đệm

Thông điệp được đệm sao cho độ dài của nó (tính bằng bit) bằng 448 modulo 512; nghĩa là, thông điệp được đệm chỉ thiếu 64 bit để trở thành bội số của 512.

Việc đệm này được hình thành bằng cách thêm một bit "1" vào cuối tin nhắn, sau đó các bit "0" được thêm vào khi cần sao cho độ dài (tính bằng bit) của tin nhắn được đệm trở nên bằng 448 (512 − 64), modulo 512.

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

b) Độ dài nối thêm

Một biểu diễn 64 bit của độ dài thông điệp gốc được thêm vào kết quả của bước trước đó. Nếu độ dài ban đầu lớn hơn 264, thì chỉ có bậc thấp của 64 bit được sử dụng để thêm hai từ 32 bit.

Độ dài của thông điệp kết quả là bội số chính xác của 512 bit. Tương đương, thông điệp này có độ dài là bội số chính xác của mười sáu từ 32 bit. Giả sử M[0 ... N − 1] biểu thị từ của thông điệp kết quả, với N là bội số nguyên của 16.

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

c) Khởi tạo thanh ghi MD

Bộ đệm bốn từ biểu diễn bốn thanh ghi 32 bit (A, B, C và D). Bộ đệm 128 bit này được sử dụng để tính toán Digest thông điệp. Các thanh ghi này được khởi tạo thành các giá trị sau theo hệ thập lục phân (byte bậc thấp trước).

A = 01 23 45 67

B = 89 ab cd ef

C = fe dc ba 98

D = 76 54 32 10

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

d) Các hàm F,G, H, I

F, G, H và I là bốn hàm MD5 cơ bản. Mỗi hàm lấy ba từ 32 bit làm đầu vào và tạo ra một từ 32 bit làm đầu ra. Chúng được biểu thị, một từ cho mỗi vòng, như sau:

$F(X, Y, Z) = (X \wedge Y) \vee (\neg X \wedge Z)$

$G(X, Y, Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$

$H(X, Y, Z) = X \oplus Y \oplus Z$

$I(X, Y, Z) = Y \oplus (X + \neg Z)$

Trong đó:

$X \wedge Y = (x_1 \wedge y_1)(x_2 \wedge y_2)...(x_l \wedge y_l)$, Với $0 \wedge 0 = 0, 1 \wedge 1 =$

$X \vee Y = (x_1 \vee y_1)(x_2 \vee y_2)...(x_l \vee y_l)$, Với $1 \vee 1 = 1, 0 \vee 0 =$

$\neg X = \neg x_1 \neg x_2 ... \neg x_l$, Với $\theta = 1, \neg = 0$

XYZ	FGHI
000	0001
001	1010
010	0110
011	1001
100	0011
101	0101
110	1100
111	1110

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

e) Các phép biến đổi FF,GG, HH, II cho vòng lặp 1,2,3,4

M(k), $0 \leq k \leq 15$ là các khối con của thông điệp, <<<s là dịch chuyển trái s bit

$$FF(a, b, c, d, M[k], s, i): a = b + ((a + F(b, c, d) + M[k] + T[i] <<< s)$$

$$GG(a, b, c, d, M[k], s, i): a = b + ((a + G(b, c, d) + M[k] + T[i] <<< s)$$

$$HH(a, b, c, d, M[k], s, i): a = b + ((a + H(b, c, d) + M[k] + T[i] <<< s)$$

$$II(a, b, c, d, M[k], s, i): a = b + ((a + I(b, c, d) + M[k] + T[i] <<< s)$$

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

f) Tính toán 4 vòng (64 bước)

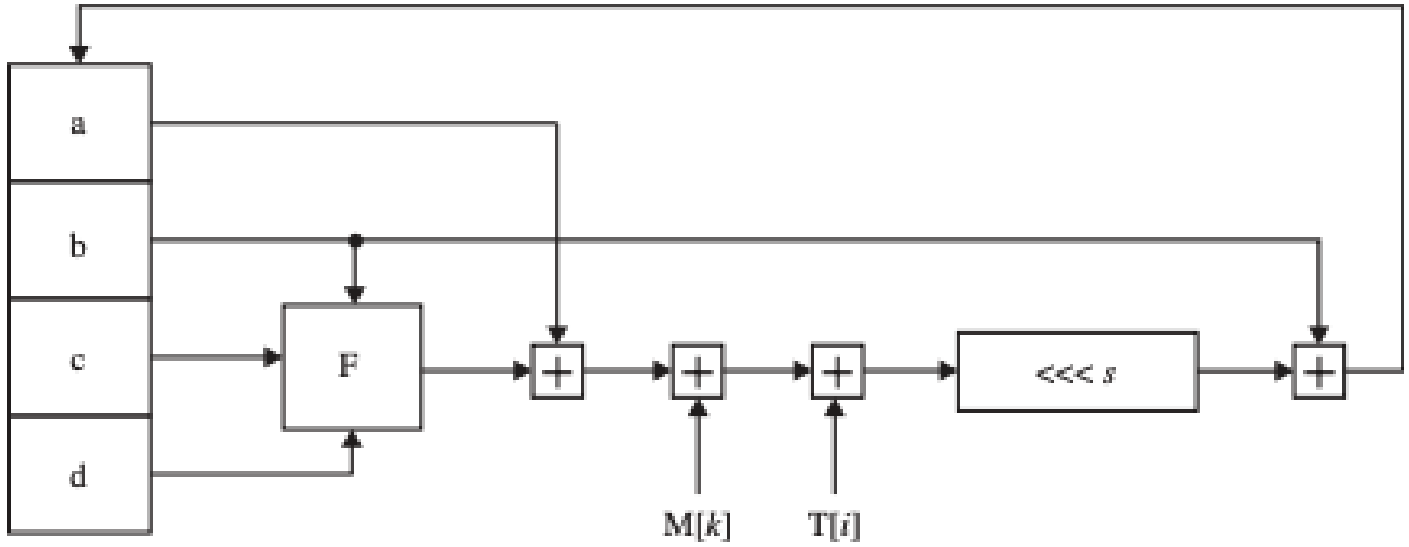
Vòng 1, FF[a,b,c,d,M(k),s,i]

FF[a, b, c, d, M[0], 7, 1], FF[d, a, b, c, M[1], 12, 2], FF[c, d, a, b, M[2], 17, 3],
FF[b, c, d, a, M[3], 22, 4], FF[a, b, c, d, M[4], 7, 5], FF[d, a, b, c, M[5], 12, 6],
FF[c, d, a, b, M[6], 17, 7], FF[b, c, d, a, M[7], 22, 8], FF[a, b, c, d, M[8], 7, 9],
FF[d, a, b, c, M[9], 12, 10], FF[c, d, a, b, M[10], 17, 11], FF[b, c, d, a, M[11], 22, 12],
FF[a, b, c, d, M[12], 7, 13], FF[d, a, b, c, M[13], 12, 14], FF[c, d, a, b, M[14], 17, 15],
FF[b, c, d, a, M[15], 22, 16]

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

f) Tính toán 4 vòng (64 bước)

Hoạt động của MD vòng 1, các vòng 2,3,4 cũng tương tự



$$a = b + ((a + F(b, c, d) + M[k] + T[i]) <<< s)$$

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

f) Tính toán 4 vòng (64 bước)

Vòng 2, GG[a,b,c,d,M(k),s,i]

GG[a, b, c, d, M[1], 5, 17], GG[d, a, b, c, M[6], 9, 18], GG[c, d, a, b, M[11], 14, 19], GG[b, c, d, a, M[0], 20, 20], GG[a, b, c, d, M[5], 5, 21], GG[d, a, b, c, M[10], 9, 22], GG[c, d, a, b, M[15], 14, 23], GG[b, c, d, a, M[4], 20, 24], GG[a, b, c, d, M[9], 5, 25], GG[d, a, b, c, M[14], 9, 26], GG[c, d, a, b, M[3], 14, 27], GG[b, c, d, a, M[8], 20, 28], GG[a, b, c, d, M[13], 5, 29], GG[d, a, b, c, M[2], 9, 30], GG[c, d, a, b, M[7], 14, 31], GG[b, c, d, a, M[12], 20, 32],

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

f) Tính toán 4 vòng (64 bước)

Vòng 3, HH[a,b,c,d,M(k),s,i]

HH[a, b, c, d, M[5], 4, 33], HH[d, a, b, c, M[8], 11, 34], HH[c, d, a, b, M[11], 16, 35], HH[b, c, d, a, M[14], 23, 36], HH[a, b, c, d, M[1], 4, 37], HH[d, a, b, c, M[4], 11, 38], HH[c, d, a, b, M[7], 16, 39], HH[b, c, d, a, M[10], 23, 40], HH[a, b, c, d, M[13], 4, 41], HH[d, a, b, c, M[0], 11, 42], HH[c, d, a, b, M[3], 16, 43], HH[b, c, d, a, M[6], 23, 44], HH[a, b, c, d, M[9], 4, 45], HH[d, a, b, c, M[12], 11, 46], HH[c, d, a, b, M[15], 16, 47], HH[b, c, d, a, M[2], 23, 48],

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

f) Tính toán 4 vòng (64 bước)

Vòng 4, II[a,b,c,d,M(k),s,i]

II[a, b, c, d, M[0], 6, 49], II[d, a, b, c, M[7], 10, 50], II[c, d, a, b, M[14], 15, 51], II[b, c, d, a, M[5], 21, 52], II[a, b, c, d, M[12], 6, 53], II[d, a, b, c, M[3], 10, 54], II[c, d, a, b, M[10], 15, 55], II[b, c, d, a, M[1], 21, 56], II[a, b, c, d, M[8], 6, 57], II[d, a, b, c, M[15], 10, 58], II[c, d, a, b, M[6], 15, 59], II[b, c, d, a, M[13], 21, 60], II[a, b, c, d, M[4], 6, 61], II[d, a, b, c, M[11], 10, 62], II[c, d, a, b, M[2], 15, 63], II[b, c, d, a, M[9], 21, 64],

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

f) Tính toán 4 vòng (64 bước)

A = A + AA

B = B + BB

C = C + CC

D = D + DD

Digest = ABCD

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm MD5

e) Các phép biến đổi FF,GG, HH, II cho vòng lặp 1,2,3,4 (tt)

T[1] = d76aa478	T[17] = f61e2562	T[33] = fffa3942	T[49] = f4292244
T[2] = e8c7b756	T[18] = c050b340	T[34] = 8771f681	T[50] = 432aff97
T[3] = 242070db	T[19] = 265e5a51	T[35] = 69d96122	T[51] = ab9423a7
T[4] = c1bdceee	T[20] = e9b6c7aa	T[36] = fde5380c	T[52] = fc93a039
T[5] = f57c0faf	T[21] = d62f105d	T[37] = a4beea44	T[53] = 655b59c3
T[6] = 4787c62a	T[22] = 02441453	T[38] = 4bdecfa9	T[54] = 8f0ccc92
T[7] = a8304613	T[23] = d8a1e681	T[39] = f6bb4b60	T[55] = ffeff47d
T[8] = fd469501	T[24] = e7d3fbc8	T[40] = bebfbc70	T[56] = 85845dd1
T[9] = 698098d8	T[25] = 21e1cde6	T[41] = 289b7ec6	T[57] = 6fa87e4f
T[10] = 8b44f7af	T[26] = c33707d6	T[42] = eaa127fa	T[58] = fe2ce6e0
T[11] = ffff5bb1	T[27] = f4d50d87	T[43] = d4ef3085	T[59] = a3014314
T[12] = 895cd7be	T[28] = 455a14ed	T[44] = 04881d05	T[60] = 4e0811a1
T[13] = 6b901122	T[29] = a9e3e905	T[45] = d9d4d039	T[61] = f7537e82
T[14] = fd987193	T[30] = fcefa3f8	T[46] = e6db99e5	T[62] = bd3af235
T[15] = a679438e	T[31] = 676f02d9	T[47] = 1fa27cf8	T[63] = 2ad7d2bb
T[16] = 49b40821	T[32] = 8d2a4c8a	T[48] = c4ac5665	T[64] = eb86d391

4.4. Ứng dụng hàm băm
4.4.3. Hàm băm SHA-512

Thuật toán băm an toàn (SHA) là một nhóm kỹ thuật mã hóa, chuyển đổi dữ liệu thành một chuỗi có độ dài cố định bằng các phép toán như bitwise, cộng mô-đun, và nén. Chuỗi này không thể đảo ngược để khôi phục dữ liệu gốc, tạo ra tính bảo mật cao. SHA-1 tạo ra băm 160 bit, còn SHA-2 có các phiên bản 256, 384, và 512 bit. SHA-3 là bổ sung cho SHA-2.

SHA thường được dùng để mã hóa mật khẩu, giúp bảo vệ dữ liệu. Nó có hiệu ứng tuyết lở: thay đổi nhỏ trong đầu vào gây thay đổi lớn trong đầu ra. SHA còn cung cấp ba tính năng bảo mật chính: chống ảnh trước (khó tìm thông điệp gốc từ giá trị băm), chống ảnh trước thứ hai (khó tìm hai thông điệp khác nhau tạo cùng một băm), và chống va chạm (khó có hai thông điệp tạo ra băm trùng).

4.4. Ứng dụng hàm băm
4.4.3. Hàm băm SHA-512

SHA – 512

Message Size: MS < 2^{128}

Block Size: BS = 1024

Word Size: WS = 64

Digest Size: DS = 512

a) Đệm thông điệp với số 1 và các số 0

- Thông điệp M: |M| = L < MS
- L' = L + (1 + pad) + 128 = 1024N
- MOD = L mod 1024
- Nếu 895 ≥ MOD: Pad = 895 – MOD
- Nếu 895 < MOD: Pad = 895 + (1024 – MOD)
- M' = $M_1M_2...M_N$

4.4. Ứng dụng hàm băm
4.4.3. Hàm băm SHA-512

b) Khởi tạo 8 thanh ghi (tổng 512 bit)

Mỗi thanh ghi 64 bit với giá trị Hexadecimal

$$r_1 = \texttt{6a09e667f3bcc908}, \quad r_5 = \texttt{510e527fade682d1},$$
$$r_2 = \texttt{bb67ae8584caa73b}, \quad r_6 = \texttt{9b05688c2b3e6c1f},$$
$$r_3 = \texttt{3c6ef372fe94f82b}, \quad r_7 = \texttt{1f83d9abfb41bd6b},$$
$$r_4 = \texttt{a54ff53a5f1d36f1}, \quad r_8 = \texttt{5be0cd19137e2179}.$$

4.4. Ứng dụng hàm băm
4.4.3. Hàm băm SHA-512

c) Hàm nén SHA-512

Input: Mi với |Mi| = 1024 bit

H_{i-1} ($1 \le i \le N$) là nội dung hiện tại trong 8 thanh ghi

$M_i = W_0, W_1, \ldots W_{15}$ (Mỗi khối W dài 64 bit)

$W_i = M[64i, 64i+64]$, $i = 0,1,\ldots 15$

Tạo 64 chuỗi nhị phân 64 bit: W16,W17,...W79

$Wt = [lamda_1(W_{t-2}) + W_{t-7} + lamda_0(W_{t-15}) + W_{t-16}] \bmod 2^{64}$, $t = 16,\ldots,79$

$lamda_0(W) = (W >>1) \oplus (W >>8) \oplus (W>>7)$;

$lamda_1 = (W>>19) \oplus (W>>61) \oplus (W>>6)$

W >> n dịch chuyển W theo vòng tròn sang phải n lần

4.4. Ứng dụng hàm băm
4.4.3. Hàm băm SHA-512

c) Hàm nén SHA-512 (tt)

$X \wedge Y = (x_1 \wedge y_1)(x_2 \wedge y_2)...(x_l \wedge y_l)$, Với $0 \wedge 0 = 0, 1 \wedge 1 = 1$

$X \vee Y = (x_1 \vee y_1)(x_2 \vee y_2)...(x_l \vee y_l)$, Với $1 \vee 1 = 1, 0 \vee 0 = 0$

$\overline{X} = \overline{x}_1\overline{x}_2...\overline{x}_l$, Với $\overline{0} = 1, \overline{1} = 0$

$ch(X,Y,Z) = (X \wedge Y) \vee (\overline{X} \wedge Z)$

$maj(X,Y,Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$

$Delta_0(r) = (r >> 28) \oplus (r >> 34) \oplus (r >> 39)$

$Delta_1(r) = (r >> 14) \oplus (r >> 18) \oplus (r >> 41)$

4.4. Ứng dụng hàm băm
4.4.3. Hàm băm SHA-512

c) Hàm nén SHA-512 (tt)

$T_1 \leftarrow [r_8 + ch(r_5,r_6,r_7) + Delta_1(r_5) + W_t + K_t] \bmod 2^{64}$,

$T_2 \leftarrow [Delta_0(r_1) + maj(r_1,r_2,r_3)] \bmod 2^{64}$,

$r_8 \leftarrow r_7$, $r_7 \leftarrow r_6$, $r_6 \leftarrow r_5$,

$r_5 \leftarrow (r_7 + T_1) \bmod 2^{64}$,

$r_4 \leftarrow r_3$, $r_3 \leftarrow r_2$, $r_2 \leftarrow r_1$,

$r_1 \leftarrow (T_1 + T_2) \bmod 2^{64}$.

Sau khi lặp 80 vòng $t = 0,..79$; $F(M_i,H_{i-1}) = r_1r_2r_3r_4r_5r_6r_7r_8$

4.4. Ứng dụng hàm băm
4.4.3. Hàm băm SHA-512

d) Thuật toán SHA-512

$X \oplus_l Y = [(X_1+Y_1) \bmod 2^l][(X_2+Y_2) \bmod 2^l]\cdots[(X_k+Y_k) \bmod 2^l].$

$H(M) = H_N$

$H_0 = r_0r_1r_2r_3r_4r_5r_6r_7r_8$ (các thanh ghi ban đầu)

$H_i = H_{i-1} \oplus_{64} F(M_i,H_{i-1})$, $I = 1,2\ldots,N.$

4.4. Ứng dụng hàm băm
4.4.2. Hàm băm SHA-512

$K_0, K_1, ... K_{79}$ là hằng số 64 bit

i	K_i	i	K_i	i	K_i
0	428a2f98d728ae22	1	7137449123ef65cd	2	b5c0fbcfec4d3b2f
3	e9b5dba58189dbbc	4	3956c25bf348b538	5	59f111f1b605d019
6	923f82a4af194f9b	7	ab1c5ed5da6d8118	8	d807aa98a3030242
9	12835b0145706fbe	10	243185be4ee4b28c	11	550c7dc3d5ffb4e2
12	72be5d74f27b896f	13	80deb1fe3b1696b1	14	9bdc06a725c71235
15	c19bf174cf692694	16	e49b69c19ef14ad2	17	efbe4786384f25e3
18	0fc19dc68b8cd5b5	19	240ca1cc77ac9c65	20	2de92c6f592b0275
21	4a7484aa6ea6e483	22	5cb0a9dcbd41fbd4	23	76f988da831153b5
24	983e5152ee66dfab	25	a831c66d2db43210	26	b00327c898fb213f
27	bf597fc7beef0ee4	28	c6e00bf33da88fc2	29	d5a79147930aa725
30	06ca6351e003826f	31	142929670a0e6e70	32	27b70a8546d22ffc
33	2e1b21385c26c926	34	4d2c6dfc5ac42aed	35	53380d139d95b3df
36	650a73548baf63de	37	766a0abb3c77b2a8	38	81c2c92e47edaee6
39	92722c851482353b	40	a2bfe8a14cf10364	41	a81a664bbc423001
42	c24b8b70d0f89791	43	c76c51a30654be30	44	d192e819d6ef5218
45	d69906245565a910	46	f40e35855771202a	47	106aa07032bbd1b8
48	19a4c116b8d2d0c8	49	1e376c085141ab53	50	2748774cdf8eeb99
51	34b0bcb5e19b48a8	52	391c0cb3c5c95a63	53	4ed8aa4ae3418acb
54	5b9cca4f7763e373	55	682e6ff3d6b2b8a3	56	748f82ee5defb2fc
57	78a5636f43172f60	58	84c87814a1f0ab72	59	8cc702081a6439ec
60	90befffa23631e28	61	a4506cebde82bde9	62	bef9a3f7b2c67915
63	c67178f2e372532b	64	ca273eceea26619c	65	d186b8c721c0c207
66	eada7dd6cde0eb1e	67	f57d4f7fee6ed178	68	06f067aa72176fba
69	0a637dc5a2c898a6	70	113f9804bef90dae	71	1b710b35131c471b
72	28db77f523047d84	73	32caab7b40c72493	74	3c9ebe0a15c9bebc
75	431d67c49c100d4c	76	4cc5d4becb3e42b6	77	597f299cfc657e2a
78	5fcb6fab3ad6faec	79	6c44198c4a475817		

4.4. Ứng dụng hàm băm
4.4.4. Các ứng dụng cuả hàm băm

- Lưu trữ mật khẩu
- Xác thực tính toàn vẹn
- Tham gia vào quá trình tạo chữ ký số

Cảm ơn các bạn,

Chúc các bạn thành công!