HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

NHẬP MÔN MẬT MÃ HỌC

HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

NỘI DUNG

HỌC VIỆN KỸ THUẬT MẬT MÃ
ACADEMY OF CRYPTOGRAPHY TECHNIQUES

CHƯƠNG 04

HÀM BĂM, XÁC THỰC VÀ CHỮ KÍ SỐ

CHƯƠNG 4. HÀM BĂM XÁC THỰC VÀ CHỮ KÍ SỐ

Nội dung các bài học trong chương 04

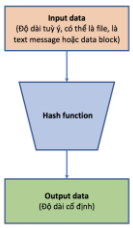
Bài 01. Vấn đề xác thực, hàm băm, chữ kí số

- Bài toán xác thực liên quan tới bảo vệ tính toàn vẹn, kiểm chứng danh tính, nguồn gốc, chống chối từ bản gốc?
- Hàm băm, mã xác thực, chữ kí số?
- Các ứng dụng trong việc xác thực và đảm bảo tính toàn vẹn dữ liệu?

Vấn đề xác thực

- **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.

Hàm băm

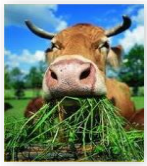


- **Giá trị băm "đại diện" cho một thông báo (văn bản) rất dài**
  - Có thể gọi là "bản tóm lược" của thông báo (*message digest*)
- **Một bản tóm lược thông báo như là một `` dấu vân tay số - digital fingerprint'' của tài liệu gốc**

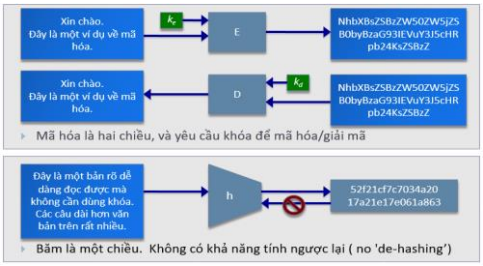
Tóm lược thông báo M có độ dài tùy ý thành bản tóm lược có độ dài cố định
$h = H(M)$

"Hàm nghiền"

- **Hàm băm như hàm "nghiền" hay "tóm lược"**



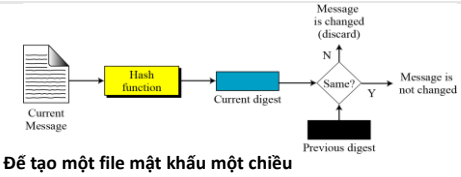
Băm và mã hóa



Các ứng dụng của hàm băm

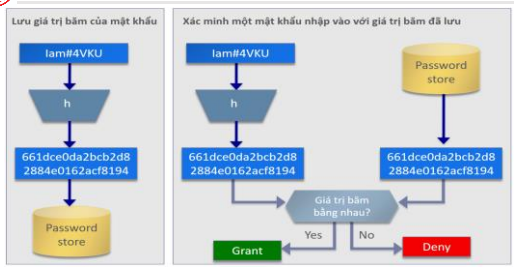
- **Ứng dụng đơn**
  - "Dấu vân tay" – xác minh tính toàn vẹn của file, "dấu vân tay" cho khóa công khai
  - Lưu trữ mật khẩu (mã hóa một chiều)
- **Kết hợp với các hàm mã hóa**
  - Mã xác thực thông điệp (Message Authentication Code - MAC)
    - Bảo vệ cả tính toàn vẹn cũng như tính xác thực của thông báo
  - Chữ ký số
    - Mã hóa giá trị băm với khóa riêng (khóa ký) và xác minh bằng khóa công khai (khóa xác minh - verification)

Tính toàn vẹn

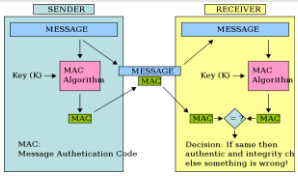


- **Để tạo một file mật khẩu một chiều**
  - Lưu giá trị băm của mật khẩu, không phải là mật khẩu thực
- **Dùng cho phát hiện tấn công và phát hiện virus**
  - Duy trì và kiểm tra giá trị băm của các file trên hệ thống

Xác minh mật khẩu

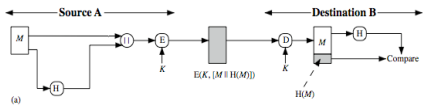


Xác thực

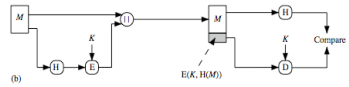


- **Bảo đảm cả tính toàn vẹn và xác thực của thông báo bằng cách kiểm tra (ai là người sở hữu khóa mật) để phát hiện bất kỳ thay đổi nào trong nội dung của thông báo**

Sử dụng hàm băm

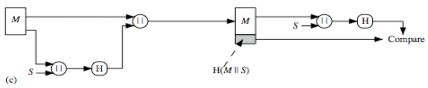


Thông điệp được mã hóa: Bí mật và Xác thực

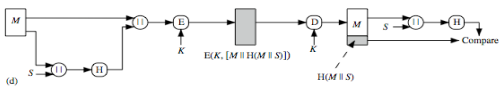


Thông điệp không được mã hóa: Xác thực

Sử dụng hàm băm

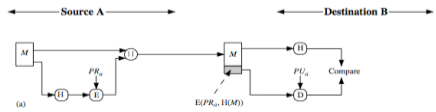


Thông điệp không được mã hóa: Xác thực (Không cần mã hóa!)



Thông điệp được mã hóa: Xác thực, Bí mật

Sử dụng hàm băm



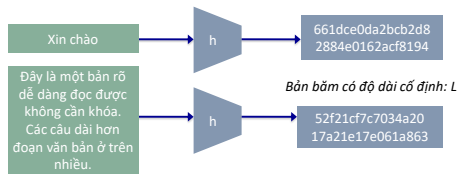
Xác thực, chữ ký số

Xác thực, chữ ký số, bí mật

Các tính chất của hàm băm

- Thông điệp có độ dài tùy ý thành bản tóm lược có độ dài cố định
- Kháng tiền ảnh (tính một chiều) {Preimage resistant (One-way property)}
  - Đầu ra được xác định trước không có khả năng tính toán để tìm 1 đầu vào bất kì mà khi băm sẽ cho ra đầu ra tương ứng (tìm x': h(x') = y, với y cho trước và không biết đầu vào tương ứng)
- Kháng tiền ảnh thứ 2 (kháng va chạm yếu) {Second preimage resistant (Weak collision resistant) }
  - Không có khả năng tính toán để tìm một đầu vào đã cho trước (tức là với x cho trước phải tìm x' ≠ x sao cho h(x) = h(x'))
- Kháng va chạm mạnh (Strong collision resistance)
  - Không có khả năng về mặt tính toán để tìm 2 đầu vào khác nhau bất kì x và x' để h(x) = h(x')

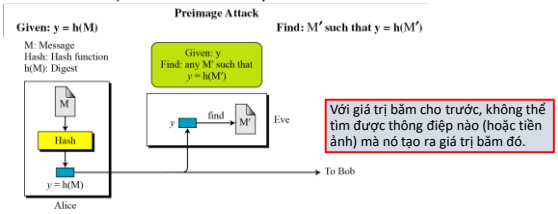
Sử dụng hàm băm



- **Thông điệp có độ dài tùy ý, bản băm có độ dài cố định**

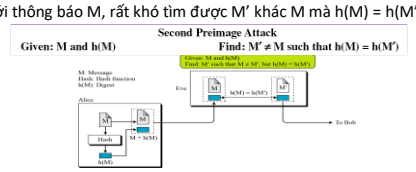
Kháng tiền ảnh (tính chất một chiều)

- Nghĩa là cho M tính y = H(M) là dễ, nhưng ngược lại, biết y tính ra M là việc cực kỳ khó
- Nói cách khác, hàm băm là hàm một chiều.



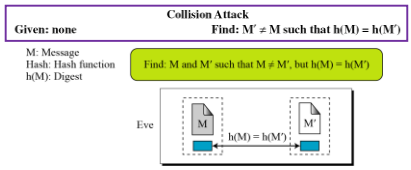
Kháng tiền ảnh thứ hai (kháng va chạm yếu)

- Đối với thông báo M, rất khó tìm được M' khác M mà h(M) = h(M')



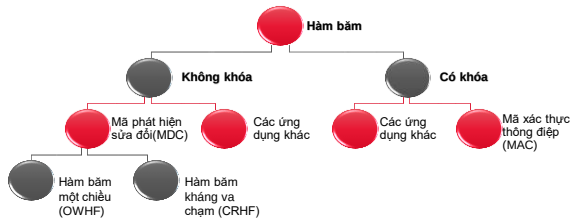
- Cho trước một thông báo, không thể tìm được thông báo khác mà có giá trị băm giống nhau. Tấn công tìm một thông báo thứ 2 có cùng giá trị băm được gọi là tấn công tiền ảnh thứ 2 (*second pre-image* attack).
  - Sẽ dễ dàng để giả mạo chữ ký mới từ chữ ký cũ nếu hàm băm được dùng không có tính chất kháng tiền ảnh thứ 2

Kháng va chạm (kháng va chạm mạnh)



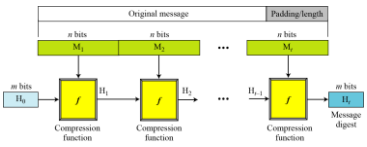
- Không thể tìm được 2 thông điệp khác nhau mà có giá trị băm giống nhau
  - Kháng va chạm hàm ý đến kháng kháng tiền ảnh thứ 2
  - Nếu tìm thấy các va chạm, thì các bên ký kết dễ dàng phủ nhận chữ ký của mình.

Sơ đồ phân loại hàm băm mật mã và ứng dụng



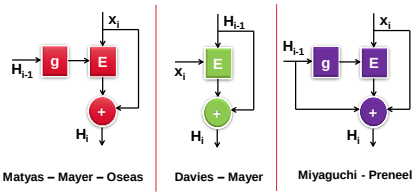
Cấu trúc hàm băm

- **Lược đồ Merkle - Damgard**

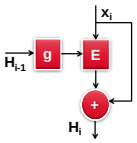


- Một thông điệp có độ dài bất kỳ được chia thành các khối
  - Độ dài phụ thuộc vào hàm nén *f*
  - Đệm vào để kích thước thông điệp là bội số của kích thước khối.
  - Xử lý tuần tự các khối, dùng kết quả băm của mỗi khối và khối hiện tại như là đầu vào của quá trình băm tiếp theo, khối cuối cùng là đầu ra có độ dài cố định

Cấu trúc hàm băm



Thuật toán Matyas – Mayer – Oseas



Cấu trúc thuật toán

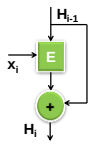
- **Input: Xâu bit x**
- **Output: Mã băm n bit của x**

(1) Đầu vào *x* được phân chia thành các khối n bit và được độn nếu cần thiết nhằm tạo khối cuối cùng hoàn chỉnh. Ta được ***t*** khối ***n*** bit: $x_1 x_2 \dots x_t$. Xác định trước một giá trị ban đầu n bit (***kí hiệu IV***)

(2) Đầu ra là H_t được xác định như sau:

$H_0 = IV, H_i = E_{g(Hi-1)}(x_i) \oplus x_i, 1 \le i \le t$

Thuật toán băm Davies - Mayer



Cấu trúc thuật toán

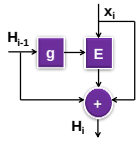
- **Input: Xâu bit x**
- **Output: Mã băm n bit của x**

(1) Đầu vào x được phân chia thành các khối *n* bit và được độn nếu cần thiết nhằm tạo khối cuối cùng hoàn chỉnh. Ta được ***t* khối *n* bit:** $x_1 x_2 \dots x_t$. Xác định trước một giá trị ban đầu *n* bit (kí hiệu **IV**)

(2) Đầu ra là H_t được xác định như sau:

$$H_0 = IV, Hi = E_{x_i}(H_{i-1}) \oplus H_{i-1}, 1 \le i \le t$$

Thuật toán băm Miyaguchi - Preneel



Cấu trúc thuật toán

- Sơ đồ này tương tự như ở thuật toán M-M-O ngoại trừ H_{i-1} (đầu ra ở giai đoạn trước) được cộng mod 2 với tín hiệu ra ở giai đoạn hiện thời. Như vậy:

$H_0 = IV, H_i = E_{g(Hi-1)}(x_i) \oplus x_i \oplus H_{i-1}; 1 \le i \le t$

Họ hàm băm

- **MD (Message Digest)**
  - Designed by Ron Rivest
  - Family: MD2, MD4, MD5
- **SHA (Secure Hash Algorithm)**
  - Designed by NIST
  - Family: SHA-0, SHA-1, and SHA-2
    - SHA-2: SHA-224, SHA-256, SHA-384, SHA-512
    - SHA-3: New standard in competition
- **...**

Các tấn công lên hàm băm

- **Tấn công kiểu vét cạn**
- **Tấn công vào tính chất kháng tiền ảnh, kháng tiền ảnh thứ 2**
  - Tìm m sao cho H(m) bằng một giá trị băm y đã cho
- **Kháng va chạm**
  - Tìm hai thông điệp **$x \neq y$ mà H(x) = H(y)**

Tấn công ngày sinh nhật

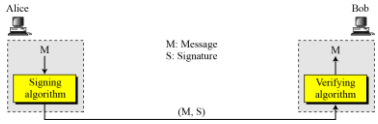
- Cần có bao nhiêu người để xác suất 2 người trong số đó trùng ngày sinh > 50% ?
- Trong 23 người được chọn 1 cách ngẫu nhiên thì ít nhất có 2 người trùng ngày sinh (tức có va chạm mạnh)
- Người ta chứng minh được rằng: Nếu có tất cả *n* bản tóm lược, và

$k \approx \sqrt{2ln\frac{1}{1-\varepsilon}}$ thì trong *k* văn bản được chọn ngẫu nhiên có ít nhất một va chạm mạnh (tức là có $x \neq y$ mà $h(x) = h(y)$) với xác suất là ε

- Khi $\varepsilon = 0.5$ thì $k \approx 1.17\sqrt{n}$, trong trường hợp ngày sinh n = 365, nên k ≈23
- Với vấn đề chọn độ dài cho đầu ra của hàm băm. Nếu là 40 bít, thì $n = 2^{40}$, do đó $k \approx 2^{20}$ (khoảng 1 triệu văn bản) sẽ có một va chạm mạnh, như vậy là không an toàn!

Xác thực và chữ kí số

- **Chữ kí số:**
  - Chữ kí thông thường được bao gồm trong tài liệu, là một phần không tách rời của tài liệu
  - Nhưng khi ký tài liệu số, chữ ký số là phần tách riêng, được gửi kèm cùng tài liệu
  - Chữ ký tay thường "giống nhau" trên nhiều văn bản
  - Chữ ký số: Mỗi văn bản là một chữ ký số duy nhất (1-1)



Xác thực và chữ kí số

- **Phương pháp kiểm tra chữ kí:**
  - Đối với một chữ ký thông thường, khi người nhận nhận được một tài liệu, họ so sánh chữ ký trên văn bản với chữ ký trong hồ sơ.
  - Đối với một chữ ký số, người nhận nhận được tài liệu số và chữ ký. Người nhận cần phải áp dụng một kỹ thuật **kiểm tra** sự kết hợp của thông điệp và chữ ký để **xác minh tính xác thực.**
  - Chữ ký viết tay thường rất ngắn. Một chữ ký số phải mang được chút gắn bó nào đó với từng bít của thông tin
    - ⇒ theo hình dung ban đầu, độ dài chữ ký số cũng phải theo độ dài của văn bản
    - Cần có được chữ ký ngắn ⇒ Phải dùng thêm một kỹ thuật riêng

Xác thực và chữ kí số

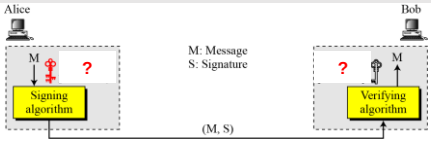
- **Định nghĩa:**
  - Một sơ đồ hệ thống chữ ký số là bộ 5 (*P*, *A*, *K*, *S*, *V*), trong đó
    - ***P*** là một tập hữu hạn các thông báo có thể.
    - ***A*** là một tập hữu hạn các chữ ký có thể.
    - ***K*** là một tập hữu hạn các khóa, mỗi khóa $k \in K$ gồm có 2 thành phần $k = (k_s, k_v)$, k_s là khóa bí mật dùng để ký, k_v là khóa công khai dùng để kiểm tra chữ ký.
    - Với mỗi $k = (k_s, k_v)$ trong ***S*** có một thuật toán ký $sig_k: P \rightarrow A$, và trong ***V*** có một thuật toán kiểm tra chữ ký.

$$ver_k: P \times A \rightarrow \{\text{đúng, sai}\}$$

thỏa mãn điều kiện sau với mọi thông báo $x \in P$ và chữ ký $y \in A$

$$ver_{k_v}(x, y) = \text{đúng} \Leftrightarrow y = sig_{k_s}(x)$$

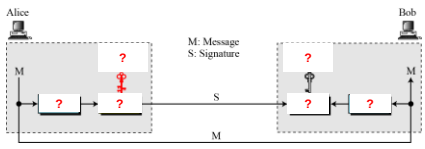
Xác thực và chữ kí số



- **Chú ý:**
  - Một hệ mật sử dụng khóa riêng và khóa công khai của **người nhận**
  - Hệ thống chữ ký số sử dụng khóa riêng và khóa công khai của **người gửi**

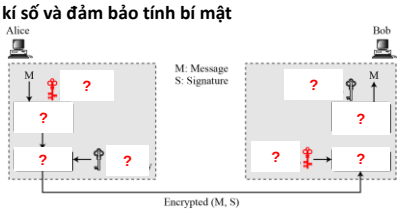
Xác thực và chữ kí số

- **Chữ kí số và hàm băm**



Xác thực và chữ kí số

- **Chữ kí số và đảm bảo tính bí mật**



- Chữ kí số không đảm bảo tính bí mật, nếu cần đảm bảo tính bí mật, kĩ thuật mã hóa/giải mã phải được áp dụng

CHƯƠNG 4. HÀM BĂM XÁC THỰC VÀ CHỮ KÍ SỐ

Nội dung các bài học trong chương 04

BÀI 01. VẤN ĐỀ XÁC THỰC, HÀM BĂM, CHỮ KÍ SỐ

BÀI 02. LƯỢC ĐỒ KÍ SỐ RSA, ELGAMAL VÀ VẤN ĐỀ XÁC THỰC KCK

Bài 02. Vấn đề xác thực, hàm băm, chữ kí số (tiếp)

- Lược đồ kí RSA?
- Các tấn công đối với chữ kí RSA, và chữ kí RSA trong thực tế?
- Chữ kí số ElGamal cơ bản, hệ chữ kí ElGamal tổng quát sử dụng các đường cong elliptic?
- Vấn đề xác thực khóa công khai?

Xác thực và chữ kí số

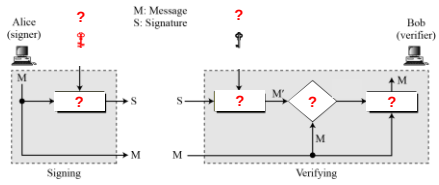
- **Chữ kí số RSA:**
  - Sơ đồ hệ thống chữ ký số RSA là bộ 5 **(*P, A, K, S, V*)**, trong đó
    - ***P = A = Z_n*** với ***n = p. q*** là tích của 2 số nguyên tố lớn ***p*** và ***q***
    - ***K*** = {(k_s, k_v), k_s = *d*, k_v = (*n*, *e*): và *e.d* ≡1 *mod* $\phi(n)$}
    - Hàm ký ***sig_k: P→ A*** và hàm kiểm tra chữ kí ***ver_k: P x A → {đúng, sai}***

    được định nghĩa như sau:

$$s = sig_{k_s}(m) = m^d \bmod n$$
$$ver_{k_v}(m, s) = \text{đúng} \Leftrightarrow m = s^e \bmod n$$

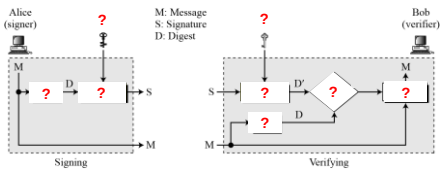
Xác thực và chữ kí số

- **Sơ đồ hệ thống chữ kí số RSA:**



Xác thực và chữ kí số

- **Chữ kí số RSA và hàm băm**



Xác thực và chữ kí số

- **Ví dụ:**
  - Mô phỏng lược đồ kí số RSA với p = 31, q = 23; khóa riêng d = 223 và thông điệp m = 439.

Xác thực và chữ kí số

- **Ví dụ**
  - p = 31, q = 23
  - n = 31 * 23 = 713
  - Φ(n) = 30 * 22 = 660
    - → d = 223 với gdc(223,660) = 1
    - → e = 223^{-1} mod 660 = 367
  - Thông điệp cần ký: 439
  - **Ký:** s = 439^{223} mod 713 = 284
  - **Kiểm tra chữ ký:** 439 = 284^{367} mod 713 ⇔ đúng

Công khai: (713, 367)
Bí mật : (223)

Xác thực và chữ kí số

- **Sơ đồ chữ kí ElGamal (1985)**
  - Được thiết kế với mục đích dành riêng cho chữ kí số, khác với RSA được dùng cho cả hệ thống mã khóa công khai lẫn chữ kí số.
  - Sơ đồ E là không tất định giống như hệ thống mã KCK Elgamal. Điều này có nghĩa là **có nhiều chữ kí hợp lệ** trên bức điện cho trước bất kì
  - Thuật toán xác minh phải có khả năng chấp nhận bất kì chữ kí hợp lệ khi xác thực.

Xác thực và chữ kí số

- **Mô tả sơ đồ E:**
  - Cho số nguyên tố p: bài toán logarit rời rạc trên Z_p là khó và giả sử $\alpha \in Z_p$ là phần tử nguyên thủy
  - Chọn số $a \in Z_p$ và tính $\beta = \alpha^a \bmod p$
  - Giá trị p, α, β là công khai, còn a là mật
  - Chọn số ngẫu nhiên (mật) $k \in Z_{p-1}$. Định nghĩa:

    $sig_k(x) = (\gamma, \delta)$
  - Trong đó: $\gamma = \alpha^k \bmod p$; $\delta = (x - a.\gamma).k^{-1} \bmod (p-1)$, với x, $\gamma \in Z_p$ và $\delta \in Z_{p-1}$, ta định nghĩa: **$Ver(x, \gamma, \delta) = true \Leftrightarrow \beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p$**

Xác thực và chữ kí số

- **Ví dụ:**
  - Cho p = 467, α = 2, a = 127.
  - Hãy kí lên bức điện x = 100, với số ngẫu nhiên k = 213 và xác minh chữ kí thu được

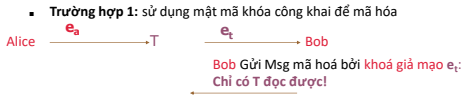
Xác thực và chữ kí số

- **Giải:**
  - Ta có:
    - β = 2^{127} mod 467 = 132
    - Vì Vì 213^{-1} mod 466 = 431. Khi đó:
      - γ = 2^{213} mod 467 = 29
      - δ = (100 – 127.29) 431mod 466 = 51

    $Sig_k(x) = (29, 51)$
  - Xác minh chữ kí bằng cách kiểm tra:
    - $132^{29}\ 29^{51} \equiv$ **189** mod 467
    - $2^{100} \equiv$ **189** mod 467
    - Vậy chữ kí là hợp lệ

Xác thực và chữ kí số

- **Vấn đề chứng thực khóa công khai**
  - Trước hết, ta hãy xem xét một số vấn đề trong sử dụng mật mã khóa công khai:
    - **Trường hợp 1**: sử dụng mật mã khóa công khai để mã hóa



→ Khoá công khai e_a của Alice cần được chứng thực, Vì có thể Bob đã nhận khoá giả mạo e_t

Xác thực và chữ kí số

- **Vấn đề chứng thực khóa công khai:**
  - Trước hết, ta hãy xem xét một số vấn đề trong sử dụng Khóa công khai:
    - **Trường hợp 2:** sử dụng chữ ký số
      - Alice nhận m và chữ ký $s = SigB(m)$ từ Bob.
      - Alice sử dụng khoá công khai của Bob e_B để kiểm tra chữ ký.
      - Nếu $Ver_{e_B}(s, m) = TRUE,$ thì Alice có thể tin Bob đã ký m.
      - Nhưng Bob không công nhận e_B là khoá công khai của mình thì sao ?

        → **Khoá công khai e_B của Bob cần được chứng thực !**

Xác thực và chữ kí số

- **Vấn đề chứng thực khóa công khai:**
  - Qua 2 trường hợp ta thấy: Trong môi trường sử dụng Khóa công khai đã nẩy sinh vấn đề **CHỨNG THỰC KHÓA CÔNG KHAI**
  - Đây là vấn đề cơ bản cần phải giải quyết trong ứng dụng mật mã khóa công khai.

Xác thực và chữ kí số

- **Vấn đề chứng thực khóa công khai: Giải pháp?**
  - Cần có một Trung tâm chứng thực tin cậy:

    Trusted Certification Authority – CA
  - **CA** phát hành các Chứng thư số

    gắn **Khoá công khai** với **Thực thể xác định**

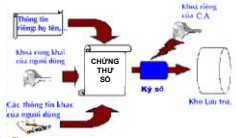
    (Con người, Cơ quan,...).
  - **Thực thể** đăng ký **khóa công khai** với **CA**
  - **CA** tạo chứng thư số gắn **thực thể** với **khóa công khai**
  - **CA** ký vào chứng thư số

Xác thực và chữ kí số

- **Quá trình tạo chứng thư số**
  - **Thực thể** đăng ký **khóa công khai** với **CA**
  - **CA** tạo chứng thư số gắn **thực thể** với **khóa công khai**
  - **CA** ký vào chứng thư số

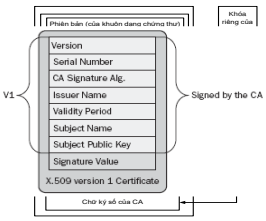
Xác thực và chữ kí số

- **Sử dụng chứng thư số**
  - Sử dụng khoá công khai của CA để kiểm tra chứng thư số (cần xác thực)
  - Nếu đúng thì có thể tin chứng thư đó do CA phát hành và có thể sử dụng khoá công khai lấy ra từ chứng thư số (của đối tác).
- **Một số nội dung của chứng thư số**



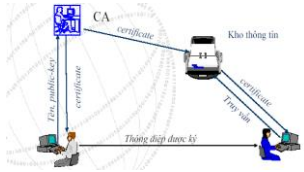
Xác thực và chữ kí số

- **Một số nội dung của chứng thư số**
  - Tên của CA phát hành chứng thư
  - Tên của chủ thể chứng thư
  - Thời gian hợp lệ
  - Khoá công khai của chủ thể
  - ….
  - Chữ ký số của CA cho chứng thư
  - …



Xác thực và chữ kí số

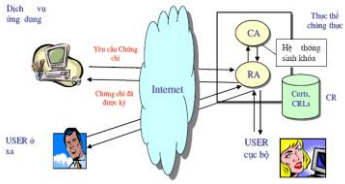
- **Quy trình cấp phát và sử dụng chứng thư**



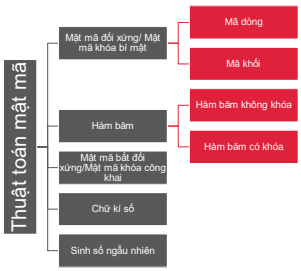
- Người sử dụng gửi yêu cầu tới nhà cung cấp chứng thư
- Nhà cung cấp chứng thư tạo chứng thư và gửi lại cho người dùng
- Chứng thư đã được ký bằng khoá riêng của nhà cung cấp chứng thư

Xác thực và chữ kí số

- **Mô hình hệ thống chứng thực đơn giản**
- **Một số giải pháp**
  - EJBCA, Window CA
  - OpenCA,….



TỔNG KẾT VỀ PHÂN LOẠI MẬT MÃ



CẢM ƠN.