



TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY



Mật mã và độ phức tạp thuật toán

Chữ ký số



Nội dung



- Giới thiệu về Chữ ký số
- Ký số RSA
- Hàm băm
- Ký số ElGamal
- Certificate Authority

1/ Giới thiệu



Giới thiệu



- Chữ ký và con dấu truyền thống
 - Tính xác thực nguồn gốc/chối giả mạo
 - Tính toàn vẹn
 - Chối chối bỏ
- Đ彰显
 - Thực sự chữ ký tay không gắn trực tiếp với nội dung

Giới thiệu



- **Dữ liệu điện tử**
 - Dễ dàng chia sẻ
 - Dễ dàng sao chép, sửa đổi
 - Giao dịch điện tử - cần đảm bảo pháp lý
- **Chữ ký điện tử và chữ ký số**
 - Chữ ký điện tử: có các dấu hiệu nhận biết điện tử
 - Chữ ký số: sử dụng thuật toán mật mã

Giới thiệu



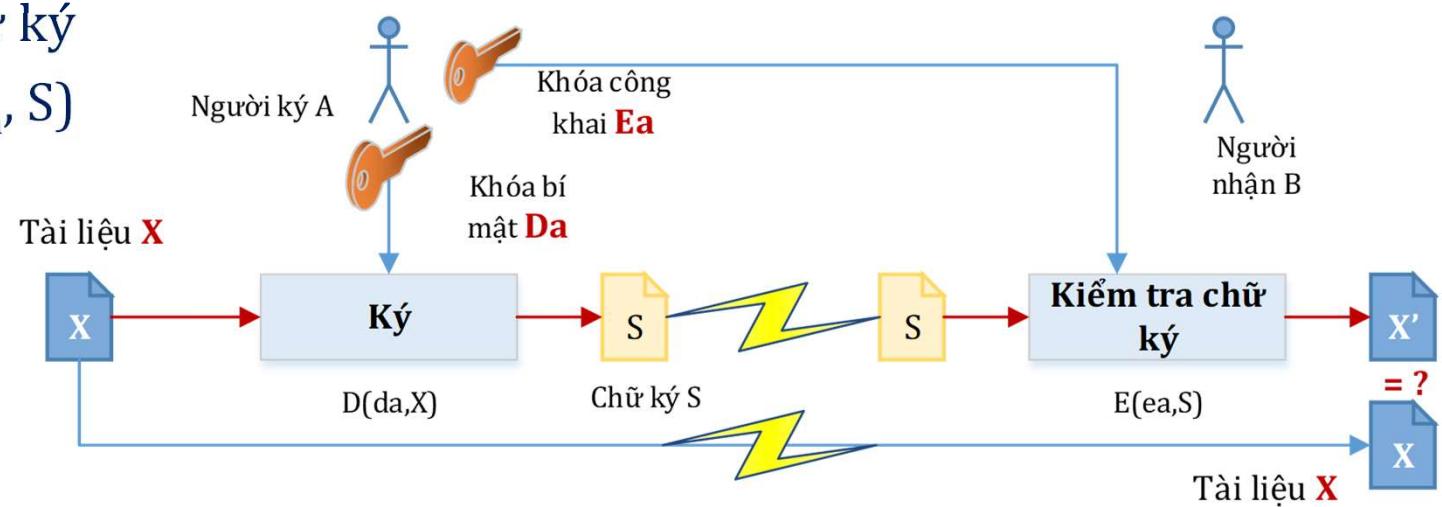
- Khái niệm chữ ký số - được đề xuất bởi Diffie và Hellman 1976 (New directions in cryptography)
- Nguyên tắc
 - Văn bản X => chữ ký S - $S=f(X)$
 - Yếu tố bảo mật: chỉ người ký tạo được (tham số - khóa mật), người khác không thể tạo/làm giả được
 - Khả năng kiểm tra: mọi người có thể kiểm tra, không cần biết tham số mật
- Mật mã khóa công khai được sử dụng - thỏa mãn yêu cầu chữ ký số
 - Hàm ký ~ hàm mã hóa sử dụng khóa bí mật
 - Hàm kiểm tra chữ ký ~ hàm giải mã sử dụng khóa công khai

2/ Chữ ký số



Sơ đồ vận hành

- Bên A: gửi văn bản X và chữ ký
 - chữ ký $S = D(d_a, X)$
- Gửi: văn bản X cùng chữ ký S
- Bên B: kiểm tra chữ ký
 - so sánh X với $E(e_a, S)$



Chú ý

- ký và mã hóa là 2 tác vụ

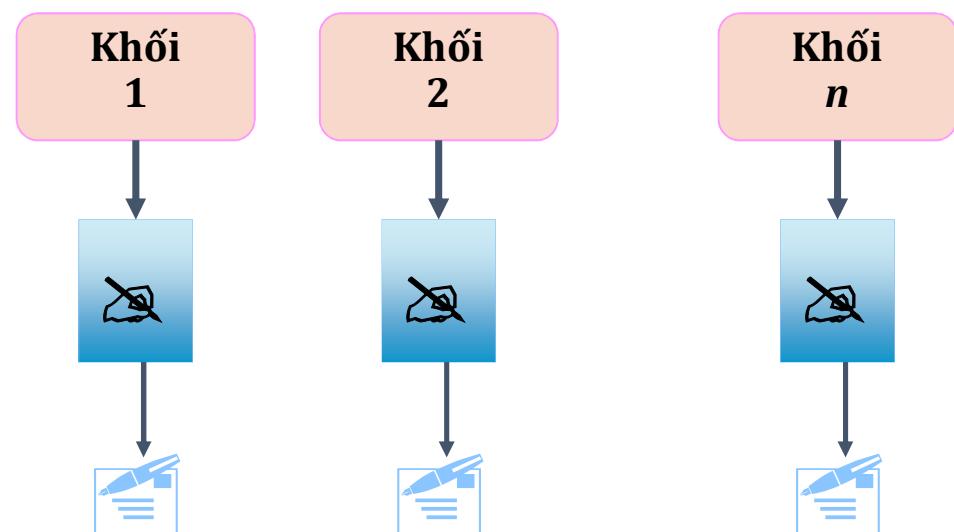
- **Ứng dụng chữ ký số**
 - Chống chối bỏ & nguồn gốc
 - B nhận đc X + S => kiểm tra thành công => A kh thể phủ nhận việc ký (tạo chữ ký) - do chỉ có A biết khóa bí mật dA
 - Công chứng: bên thứ 3 C được tin cậy
 - C ký trên $(X+S_A)=S_C$, gửi tới B: $X+S_A+S_C$
 - Chứng thực nhận
 - Bên nhận B chứng thực đã nhận văn bản: X
B gửi lại A : chữ ký của B trên X: $S_B = D_B(X)$

■ Vấn đề

- Kích cỡ chữ ký S tương đương văn bản X, Văn bản X có thể dài
Dẫn đến
 - thời gian, chi phí thực hiện ký - có thể rất lâu
 - chi phí lưu trữ, chi phí truyền tin
 - thời gian kiểm tra chữ ký

■ Vấn đề

- Nếu kích cỡ văn bản dài hơn block của thuật toán mã/ký ?
 - Văn bản => cắt thành các block
 - Chữ ký => ký từng block
 - Kiểm tra chữ ký ?
- Chữ ký sẽ thế nào nếu
 - Bên thứ 3 tấn công
 - Thay đổi thứ tự (data & signature block)
 - Lắp lại/bỏ bớt block



3/ Hàm băm





- Hàm băm & Hàm băm mật mã
 - Hàm băm - chỉ mục tìm kiếm: đồng dữ

Về Hàm băm



- Hàm băm mật mã h - tính giá trị đặc trưng (digest) cho thông điệp X
 - $h=h(X)$
 - Dữ liệu vào X - độ dài tùy ý => dữ liệu h - độ dài ngắn & cố định
 - tính $h(X)$ - dễ
 - hàm ngược: biết $h=h(X)$, tìm X - khó
 - Chống đụng độ:
 - $X \neq X'$ thì $h(X) \neq h(X')$
 - rất khó để tìm $X \neq X'$ mà $h(X) = h(X')$
 - Ngẫu nhiên
 - Bit đầu vào bất kỳ: xác suất bit đầu ra =1 là 0.5

Về Hàm băm



- Tính chống đụng độ
 - Rõ ràng nếu Không gian giá trị băm < không gian bản rõ => sẽ xảy ra đụng độ

Bài toán ngày sinh nhật



- Bài toán ngày sinh nhật
 - Cần nhóm bao nhiêu người để xác suất có 2 người trùng ngày sinh > 50% ?
 - Lấy ngẫu nhiên n giá trị ngày sinh từ k=365 khả năng
 - Số khả năng (bộ n ngày sinh) là k^n
 - Số bộ k giá trị không trùng là $(k)_n = k(k-1)\dots(k-n+1)$
 - Xác suất để bộ n ngày không trùng:
 - $p = (k)_n/k^n \approx 1 - n(n-1)/2k$
 - Với k=366, n >= 23
- Với $n(n-1)/2$ cặp, mỗi cặp có xác suất trùng là $1/k$
- Để $n(n-1)/2k > 50\%$ thì $n > k^{1/2}$

Giá trị băm tối thiểu ? Bit



- Theo kết quả trên:
 - với m bits, với $2^{m/2}$ xâu thì xác suất $>50\%$ có 2 xâu trùng giá trị băm
 - Với 64 bits, cứ 2^{32} thông điệp thì xác suất $>50\%$ có 2 trùng giá trị băm (khả thi để thử 2^{32})
 - Từ đó, đề xuất giá trị băm tối thiểu dài 128 bits

Xây dựng hàm băm



- Một số kỹ thuật xây dựng
 - Dựa trên mã khối và mật mã khóa bí mật
 - Dựa trên phép toán số học đồng dư
 - Các hàm đặc biệt

Xây dựng hàm băm

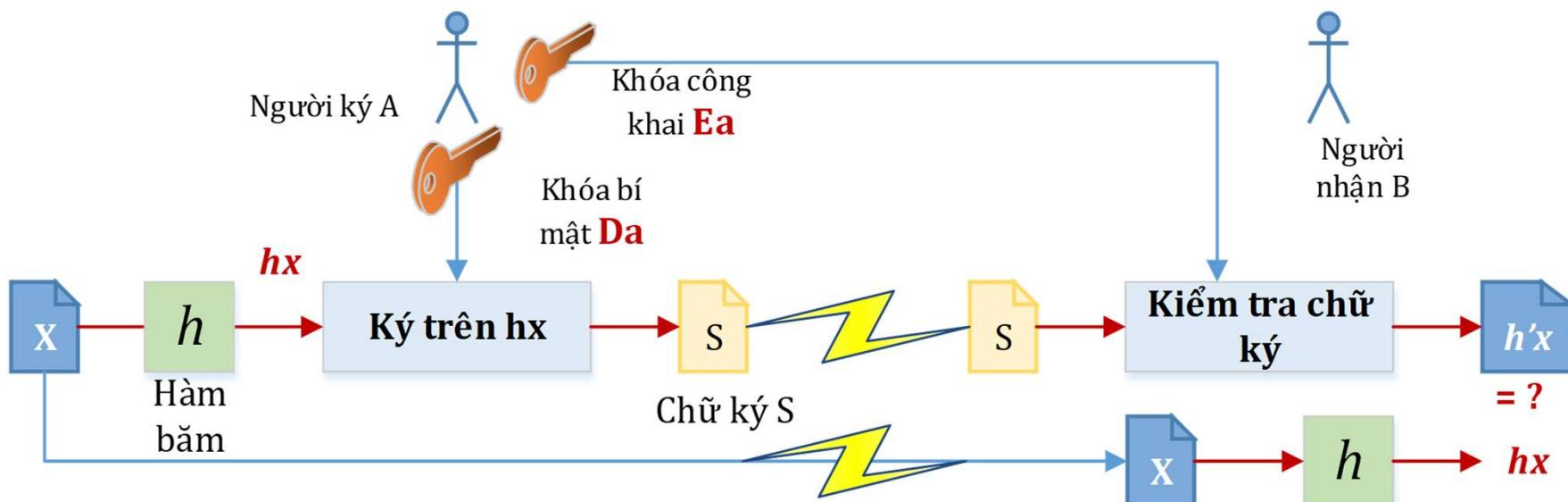


- Một số hàm băm thông dụng
 - MD5 (Rivest 1992)
 - Một trong các hàm băm đã được sử dụng phổ biến
 - Giá trị băm: 128bit
 - Có lỗ hổng => hiện nay ít được sử dụng trong chữ ký số
 - SHA: Secure Hash
 - SHA1: 2002, 160bit
 - họ SHA2: SHA-224, 256, 384, 512

Chữ ký số và hàm băm mật mã



- Ứng dụng hàm băm trong chữ ký số
 - Ký trên giá trị băm của thông điệp => kích thước nhỏ, chi phí tính toán, lưu trữ và truyền tin



4/ Chữ ký El-Gamal



- Bài toán logarit rời rạc
 - p là một số nguyên tố. Xét nhóm nhân các số nguyên modulo p : $Z_p^* = \{1, 2, \dots, p\}$ với phép nhân modulo p .
Lũy thừa bậc k modulo p : $a^k \text{ mod } p$
Logarit rời rạc: phép tính ngược lại
 - Ví dụ:
 $p=11, a=2, k=4 \Rightarrow a^k = 2^4 = 16 \text{ mod } 11 = 5$
logarit: $2^k = 5 \text{ mod } 11$, tìm k



■ Bài toán logarit rời rạc

- Tổng quát:

G - nhóm cyclic hữu hạn có n phần tử - bậc n, có phép toán nhân
a là phần tử sinh, b là phần tử của G

Logarit rời rạc của b theo cơ số a, $\log_a b$ là số nguyên x, $0 \leq x \leq n - 1$ thỏa
 $b = a^x$

- Bài toán logarit rời rạc là bài toán khó với số nguyên tố p đủ lớn
 - ($p-1$ không phải là tích các số nguyên tố nhỏ)

▪ Sơ đồ chữ ký ElGamal

- Được xây dựng trên *tính khó* của bài toán logarit trên không gian Z_p khi p là số nguyên tố (lớn)
- A chọn số nguyên tố p lớn sao cho $p-1$ có ước số nguyên tố lớn a là phần tử nguyên thủy của Z_p
chọn $x: 0 \leq x \leq p - 2$, tính $y = a^x$
khóa công khai = (p, a, y) , khóa bí mật= x
- Ký thông điệp M:
 - chọn ngẫu nhiên số nguyên bí mật k $1 \leq k \leq p - 1$, $\gcd(k, p-1) = 1$
 - chữ ký của M là cặp (r, s) :
 - $r = a^k \bmod p$, $s = (M - x \cdot r)k^{-1} \bmod (p - 1)$
 - Kiểm tra chữ ký: kiểm tra hệ thức $a^M \equiv y^r \cdot r^s \bmod p$

■ Ví dụ

- $p=11$, $a=2$, khóa bí mật $x=3 \Rightarrow y = 2^3 = 8 \text{ mod } 11 \Rightarrow$ khóa công khai $(11, 2, 8)$
- Thông điệp $M=9$
- Ký:
 - chọn $k=7 \Rightarrow k^{-1} = 3$
 - $r = 2^7 \text{ mod } 11 = 7, s = (9 - 3 \cdot 7) \cdot 3 \text{ mod } (11 - 1) = 4$
 - chữ ký là cặp $(7, 4)$
- Kiểm tra chữ ký: nhận $M=9$, sig $(7, 4)$
 - $a^M = 2^9 \equiv? y^r \cdot r^s = 8^7 \cdot 7^4 \text{ mod } 11$

Một số hình thức chữ ký



- Chữ ký mù - blind signature
 - Người ký không biết nội dung ký
- Ký tập thể - group signature
 - Chữ ký chỉ có thể tạo bởi 1 nhóm người - kiểm tra được do thành viên trong nhóm tạo
- Chữ ký kh thể từ chối - undeniable signature
 - Kiểm tra chữ ký cần sự tham gia của người ký => không chuyển giao được => dùng như giấy cấp phép sử dụng sản phẩm
- Đồng ký - multi signature
 - Chữ ký của nhóm người - muốn ký thì tất cả phải tham gia ký. Ai cũng có thể kiểm tra

- Chữ ký
 - người ký biết ký trên nội dung nào
- Chữ ký mù
 - Người ký B không biết thực sự ký trên nội dung gì. B có thể kiểm tra tính hợp lệ của chữ ký, người A kh thể tự tạo nội dung bất kỳ với chữ ký của B
 - Đặc điểm
 - Tính ẩn danh/mù: người ký không biết nội dung văn bản
 - Tính không truy vết: người ký kh lần vết đc mối liên hệ chữ ký với nội dung
 - Ứng dụng:
 - Tiền điện tử
 - Bầu cử điện tử

- Chữ ký mù sử dụng hệ mật RSA

- A - người A cần B ký trên nội dung m
- A làm mù nội dung m : chọn r ngẫu nhiên $r \in Z_n^*$
 - tính $z = m \cdot r^b$
 - Gửi z cho B để ký
- B - người ký
 - Ký trên z: $y = z^a \pmod{n} = (m \cdot r^b)^a = m^a \cdot r^{a \cdot b} = m^a \cdot r \pmod{n}$
- Người nhận chữ ký
 - xóa mù => lấy lại chữ ký đúng trên $m : \frac{y}{r} = m^a \cdot r \frac{1}{r \pmod{n}} = m^a \pmod{n}$

5/ Certification Authority

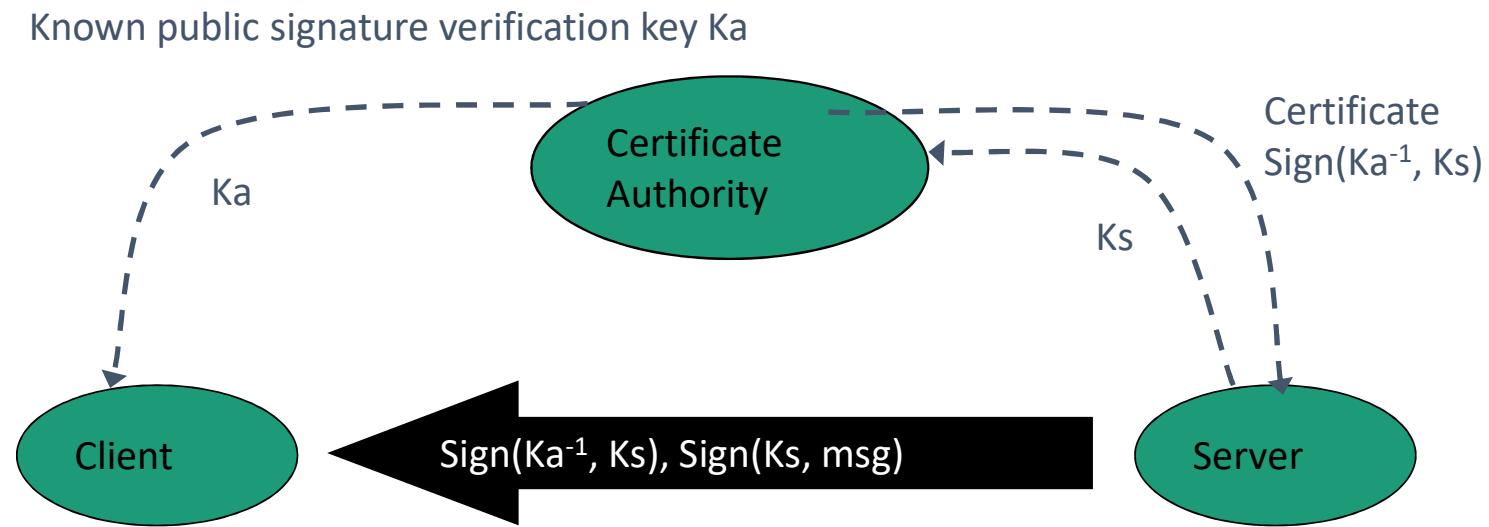


Public-Key Infrastructure (PKI)



- Ai cũng gửi được thông tin tới Bob
 - Biết khóa công khai của Bob
- Vấn đề MIM - làm sao biết khóa đó đúng là của Bob?
 - Nếu kẻ xấu giả khóa => có thể đọc thông tin
- Phương án: PKI
 - Tin cậy vào bên thứ 3

Public-Key Infrastructure



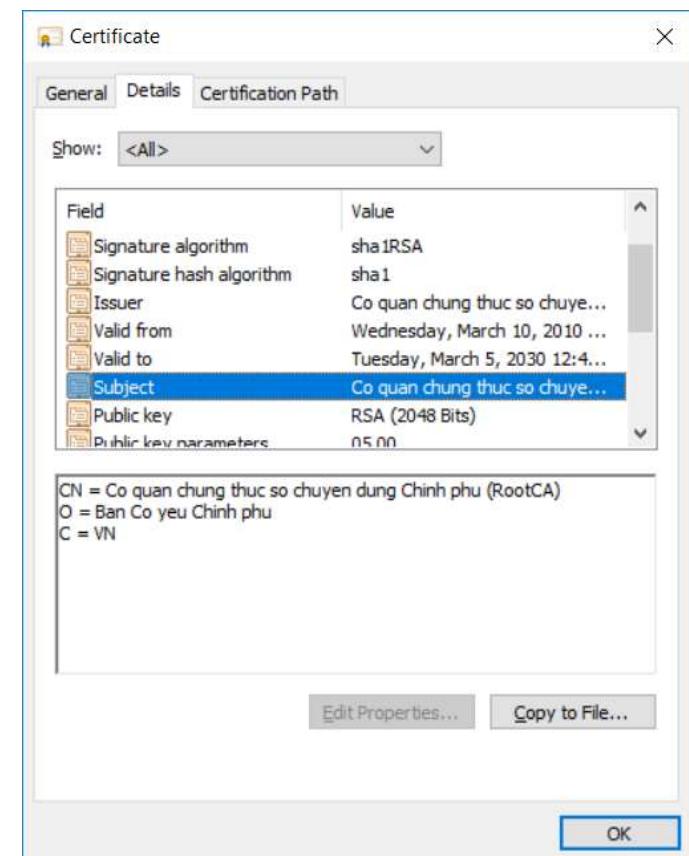
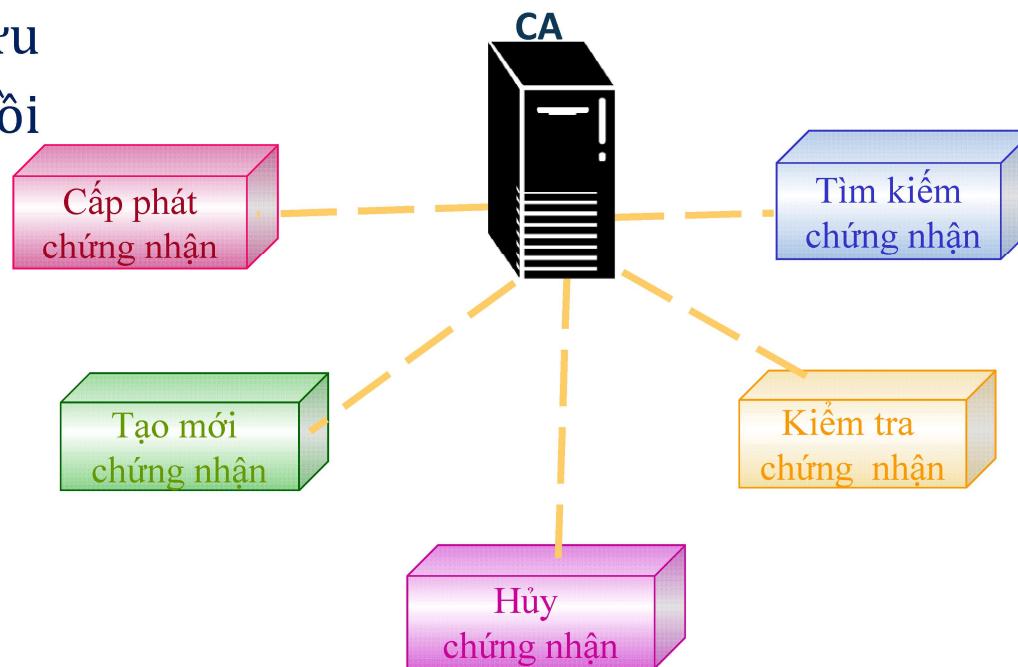
Server certificate can be verified by any client that has CA key K_a

Certificate authority is "off line"

Certificate Authority System



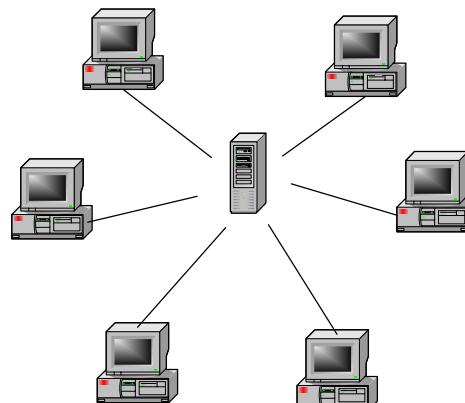
- Một tổ chức thứ ba đáng tin cậy
- Quản lý chứng nhận số: các quy trình
 - Cấp phát
 - Tra cứu
 - Thu hồi



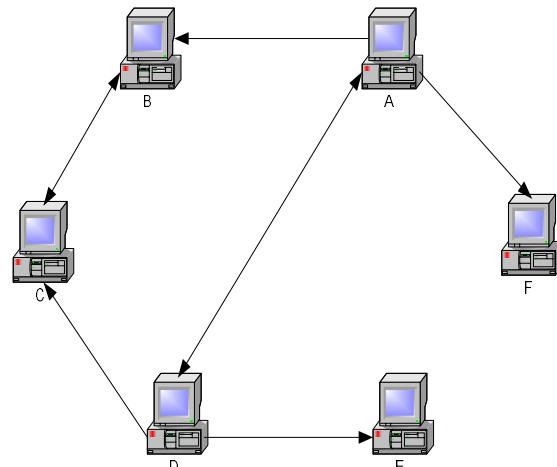
Certificate Authority System CA(S)



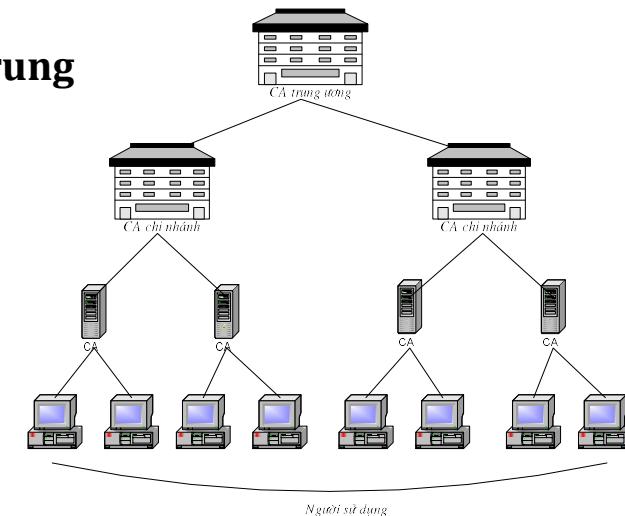
- Hệ thống CA
 - Quốc gia: 1, nhiều root



Mô hình phân cấp



Mô hình tập trung



Web of Trust

Digital Certificate

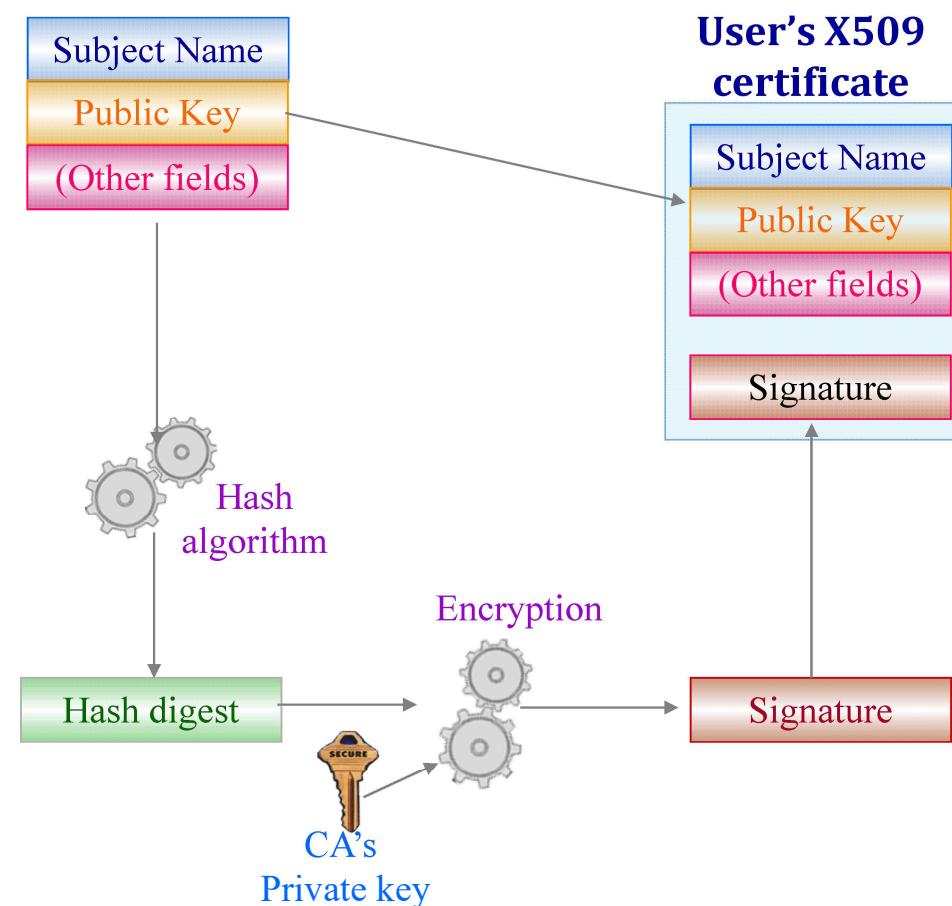


- Chứng nhận điện tử là chứng thực sự sở hữu khóa công khai

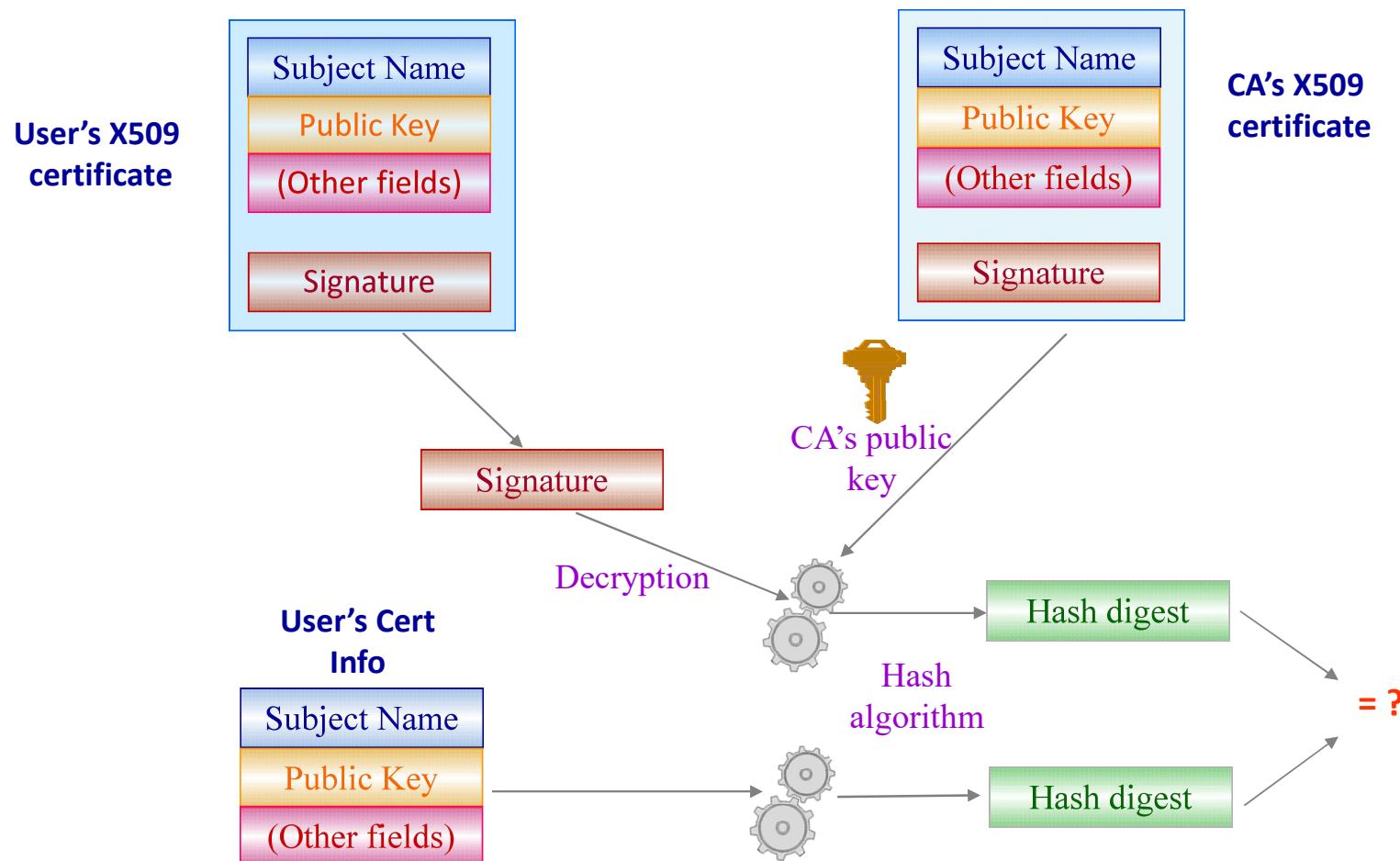


Chứng nhận điện tử giải quyết được vấn đề MIM

Tạo chứng thực số



Kiểm tra chứng thực số



Chuẩn X.509 (ver. 3.0)



- *Version*: Chỉ định phiên bản của chứng nhận X.509.
- *Serial Number*: Số ID phát hành được gán bởi CA. Mỗi CA gán một mã serial duy nhất cho mỗi giấy chứng nhận mà nó phát hành.
- *Signature Algorithm*: Thuật toán chữ ký chỉ rõ thuật toán mã hóa được CA sử dụng để ký giấy chứng nhận. Trong chứng nhận X.509 thường là sự kết hợp giữa thuật toán băm (chẳng hạn như MD5) và thuật toán khóa công cộng (chẳng hạn như RSA).

Version
Serial Number
Signature
Issuer Name
Validity Period
Subject Name
Public Key
Issuer Unique ID
Subject Unique ID
Extensions
Signature

Chuẩn X.509 (ver. 3.0)

- *Issuer Name*: Tên tổ chức CA phát hành giấy chứng nhận, đây là một tên phân biệt theo chuẩn X.500 (X.500 Distinguished Name – X.500 DN). Hai CA không được sử dụng cùng một tên phát hành.
- *Validity Period*: Trường này bao gồm hai giá trị chỉ định khoảng thời gian mà giấy chứng nhận có hiệu lực. Hai phần của trường này là not-before và not-after. Not-before chỉ định thời gian mà chứng nhận này bắt đầu có hiệu lực, Not-after chỉ định thời gian mà chứng nhận hết hiệu lực. Các giá trị thời gian này được đo theo chuẩn thời gian Quốc tế, chính xác đến từng giây.

Version
Serial Number
Signature
Issuer Name
Validity Period
Subject Name
Public Key
Issuer Unique ID
Subject Unique ID
Extensions
Signature

Chuẩn X.509 (ver. 3.0)



- *Issuer Unique ID* và *Subject Unique ID*: Hai trường này được giới thiệu trong X.509 phiên bản 2, được dùng để xác định hai tổ chức CA hoặc hai chủ thể khi chúng có cùng DN. RFC 2459 đề nghị không nên sử dụng hai trường này.
- *Extensions*: Chứa các thông tin bổ sung cần thiết mà người thao tác CA muốn đặt vào chứng nhận. Trường này được giới thiệu trong X.509 phiên bản 3.

Version
Serial Number
Signature
Issuer Name
Validity Period
Subject Name
Public Key
Issuer Unique ID
Subject Unique ID
Extensions
Signature

Chuẩn X.509 (ver. 3.0)



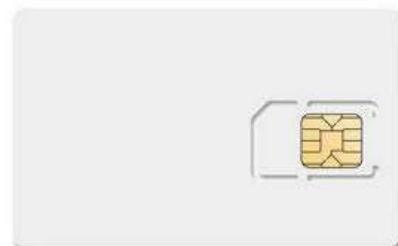
- *Signature*: Đây là chữ ký điện tử được tổ chức CA áp dụng. Tổ chức CA sử dụng khóa bí mật có kiểu quy định trong trường thuật toán chữ ký. Chữ ký bao gồm tất cả các phần khác trong giấy chứng nhận. Do đó, tổ chức CA chứng nhận cho tất cả các thông tin khác trong giấy chứng nhận chứ không chỉ cho tên chủ thể và khóa công cộng.

Version
Serial Number
Signature
Issuer Name
Validity Period
Subject Name
Public Key
Issuer Unique ID
Subject Unique ID
Extensions
Signature

Lưu trữ cắp khóa



- Cắp khóa - khóa bí mật - lưu an toàn
 - Thiết bị USB token
 - Thiết bị HSM (Hardware Secure Module)
 - SIM PKI
 - File (pfx, key, pem, p12,...)



vtnam1.pfx	3/5/2019 9:19 AM
vtnam2.pfx	3/5/2019 9:20 AM
chu ky chuan.png	8/5/2019 2:44 PM
chu ky vtn.png	3/5/2020 6:05 PM
chu ky.png	4/5/2019 2:19 PM
chu ky1.png	4/9/2019 2:04 PM
con dau 120.png	4/5/2019 2:19 PM
con dau chuan.png	8/5/2019 2:45 PM