Chủ đề 7:
Chữ ký điện tử

PGS.TS. Trần Minh Triết

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Nội dung

- Mở đầu
- Phương pháp RSA
- Phương pháp DSA (đọc thêm)
- Phương pháp ElGamal (đọc thêm)

Mở đầu

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Mở đầu

Mục tiêu của chữ ký điện tử (Digital Signature) :

- Xác nhận người dùng (Authentication)
- Tính toàn vẹn thông tin (Data Integrity)
- Không thể từ chối trách nhiệm (Non-Repudiation)

Mở đầu

- Một số khái niệm cơ bản:
  - **Chữ ký điện tử**: chuỗi dữ liệu cho phép xác định nguồn gốc/xuất xứ/thực thể đã tạo ra 1 thông điệp.
  - **Thuật toán phát sinh chữ ký điện tử**: phương pháp tạo ra chữ ký điện tử
  - **Chiến lược chữ ký điện tử**: bao gồm ***thuật toán phát sinh chữ ký điện tử*** và ***thuật toán tương ứng để kiểm chứng chữ ký điện tử***.

    Digital Signature Scheme =

    Digital Signature Generation Algorithm +

    Digital Signature Verification Algorithm

Mở đầu

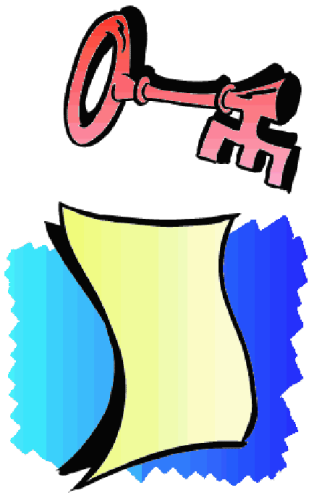
- Các mức độ "Phá vỡ" chiến lược chữ ký điện tử:
  - ***Total Break***: tìm được phương pháp hiệu quả để "giả mạo" chữ ký hợp lệ.
    - Biết được private key?
    - Không biết private key nhưng tìm được phương pháp hiệu quả để giả tạo chữ ký hợp lệ.
  - ***Selective forgery***: cho trước một thông điệp, người tấn công *có khả năng* tạo ra được chữ ký hợp lệ trên thông điệp này.
  - ***Existential forgery***: có thể tìm và chỉ ra được một thông điệp (có thể vô nghĩa) nhưng dễ dàng để người tấn công có thể tạo ra được chữ ký hợp lệ trên thông điệp này.

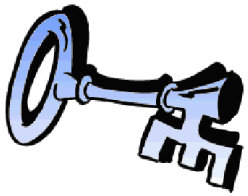
Mở đầu

- Phân loại cách tấn công
  - ***Key-only***: người tấn công **chỉ biết public key**
  - Message attack
    - ***Known-message attack***: người tấn công **có các chữ ký của một tập các thông điệp**. Người tấn công **biết nội dung của các thông điệp này** nhưng **không được phép chọn sẵn** các thông điệp.
    - ***Chosen-message attack***: người tấn công **có được các chữ ký hợp lệ** của một **tập các thông điệp có chọn lọc**. (non-adaptive)
    - ***Adaptive chosen-message attack***: người tấn công có thể sử dụng người ký/module ký như một "**oracle**"

Mã hóa khóa công khai

Public key: Mọi người đều có thể sử dụng được

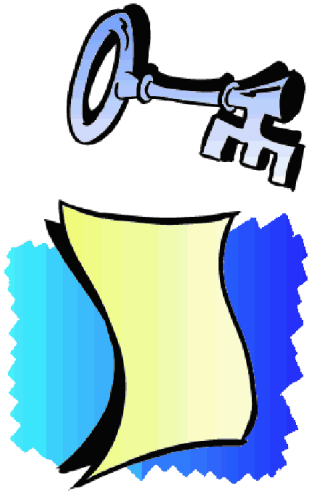


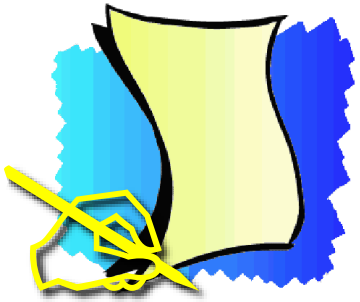


Private key: Chỉ người chủ sở hữu cặp khóa mới có để sử dụng → Bảo mật thông tin

Ý tưởng: chữ ký điện tử

Private key: Chỉ người chủ sở hữu cặp khóa mới có để ký





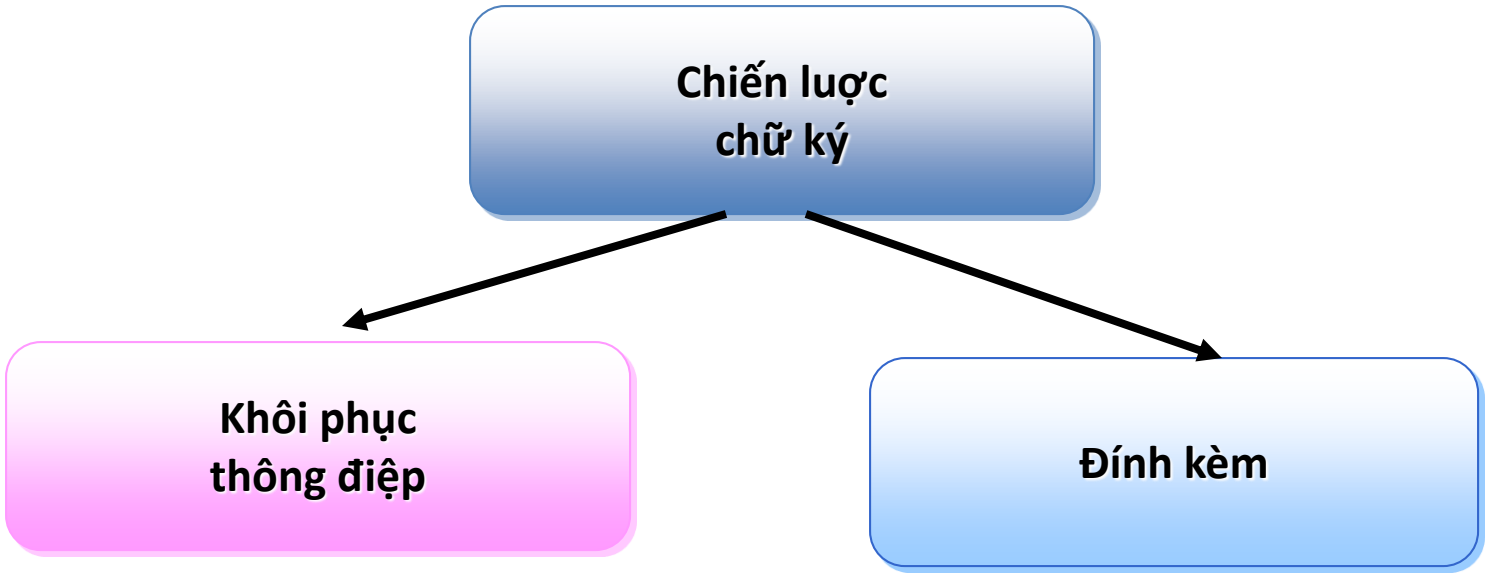
Public key: Mọi người đều có thể kiểm tra chữ ký

Mở đầu

- Một số ký hiệu:
  - M Không gian thông điệp
  - M_S Không gian thông điệp được ký
  - S Không gian chữ ký
  - R Ánh xạ 1-1 từ M vào M_S (redundancy function)
  - M_R Ảnh của R
  - R^{-1} Hàm ngược của R
  - h Hàm một chiều với tập nguồn M
  - M_h Không gian giá trị *hash* (h: $M \rightarrow M_h$)

Mở đầu

- Phân loại chiến lược chữ ký điện tử

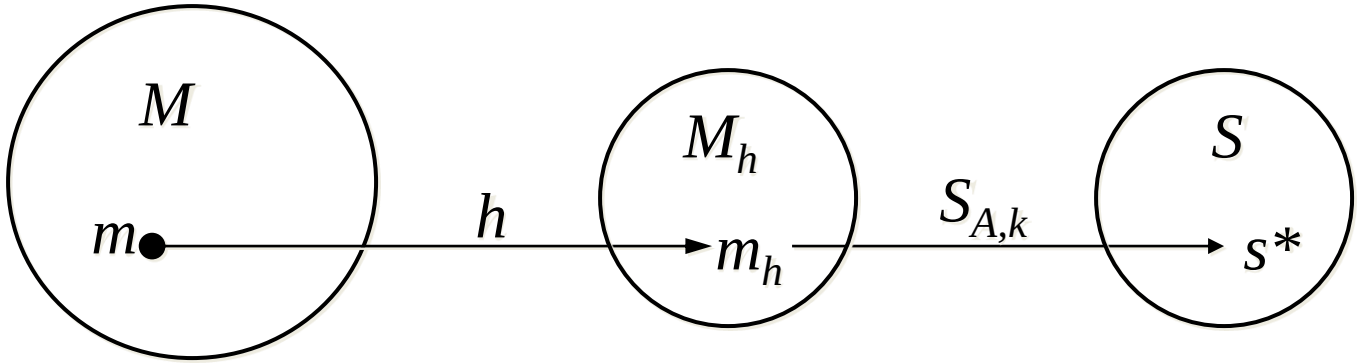


Mở đầu

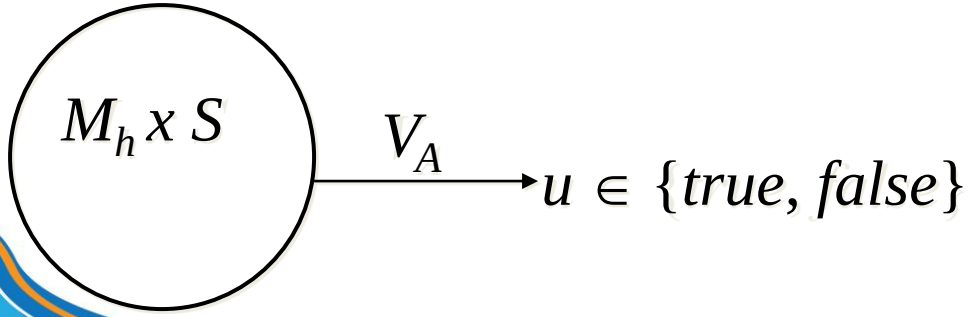
- Các chiến lược chữ ký với phần đính kèm (appendix)
  - Chữ ký điện tử đi kèm với thông điệp gốc
  - Cần có thông điệp (gốc) cho quá trình kiểm tra chữ ký điện tử
  - Sử dụng hàm băm mật mã
  - Ví dụ: RSA, DSA, ElGamal, Schnorr…

Mở đầu

- Chữ ký điện tử với phần đính kèm



$$s^* = S_{A,k}(m_h)$$
$$u = V_A(m_h, s^*)$$

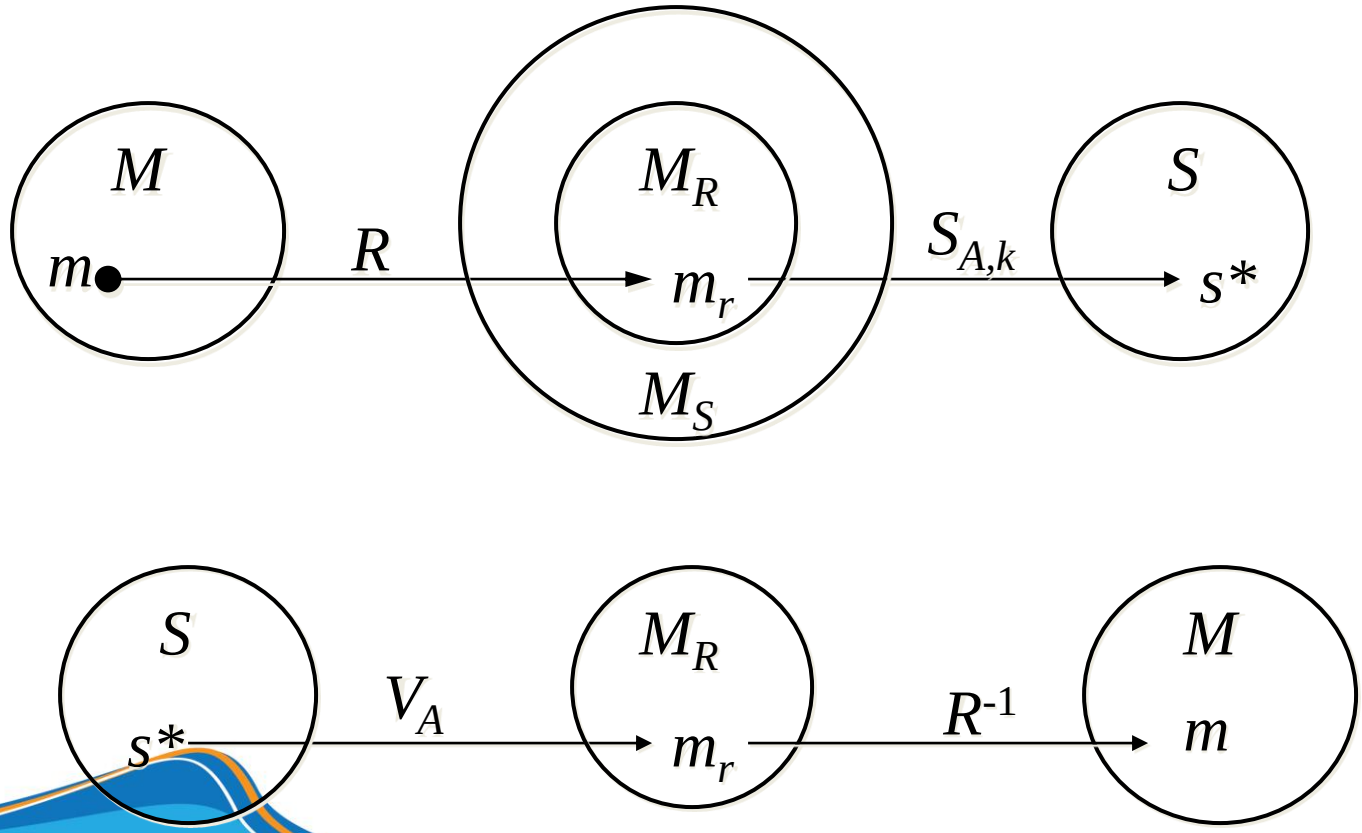


Mở đầu

- Yêu cầu:
  - Với mỗi $k \in R$, có thể dễ dàng tính $S_{A,k}$
  - Phải dễ dàng tính được V_A
  - Rất khó để một người không phải là *signer* có thể tìm ra $m \in M$ và $s^* \in S$ sao cho $V_A(m', s^*) = true$, với $m' = h(m)$

Mở đầu

- Chữ ký điện tử có khả năng cho phép khôi phục lại thông điệp



Mở đầu

- Yêu cầu:
  - Với mỗi $k \in R$, có thể dễ dàng tính $S_{A,k}$
  - Có thể dễ dàng tính V_A
  - Rất khó (computationally infeasible) để một người không phải là A có thể tìm ra $s^* \in S$ sao cho $V_A(s^*) \in M_R$

Phương pháp RSA

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Phương pháp RSA

- Phát sinh khóa n, p, q, e, d
- Tạo chữ ký
  - Tính $m_r = R(m)$
  - Tính $s = m_r^d \bmod n$
  - Chữ ký tương ứng với m là s
- Kiểm tra chữ ký
  - Nhận được public key (n, e)
  - Tính $m_r = s^e \bmod n$
  - Kiểm tra $m_r \in M_r$
  - Khôi phục $m = R^{-1}(m_r)$

Phương pháp RSA

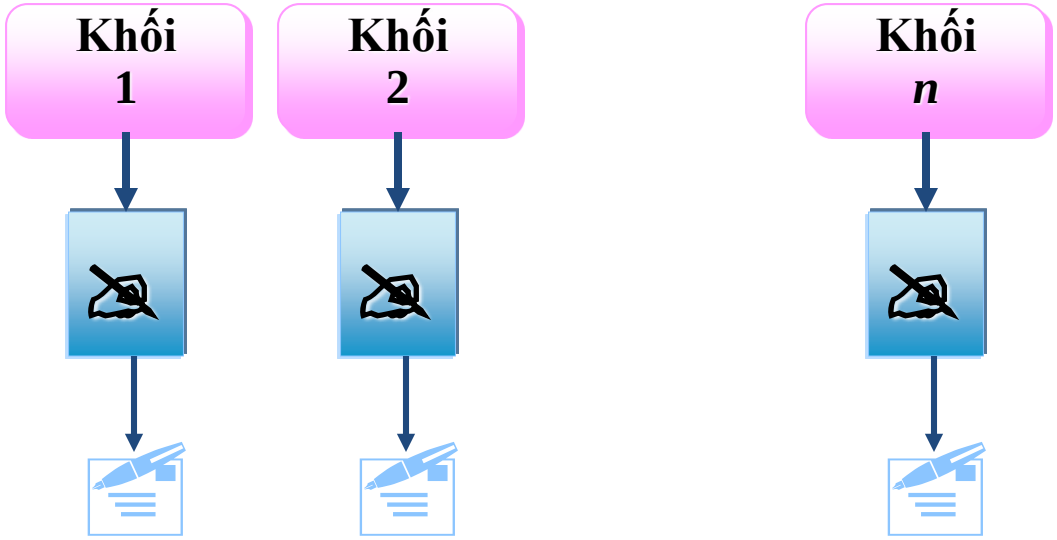
- Tấn công
  - Phân tích ra thừa số nguyên tố một số nguyên lớn
  - Khả năng nhiều cặp khóa cho ra cùng chữ ký
  - Tính chất homomorphic:

$$E(x_1).E(x_2)$$
$$= x_1^e x_2^e \bmod n$$
$$= (x_1.x_2)^e \bmod n$$
$$= E(x_1.x_2 \bmod n)$$

- Vấn đề tái cấu trúc nội dung (Reblocking problem)

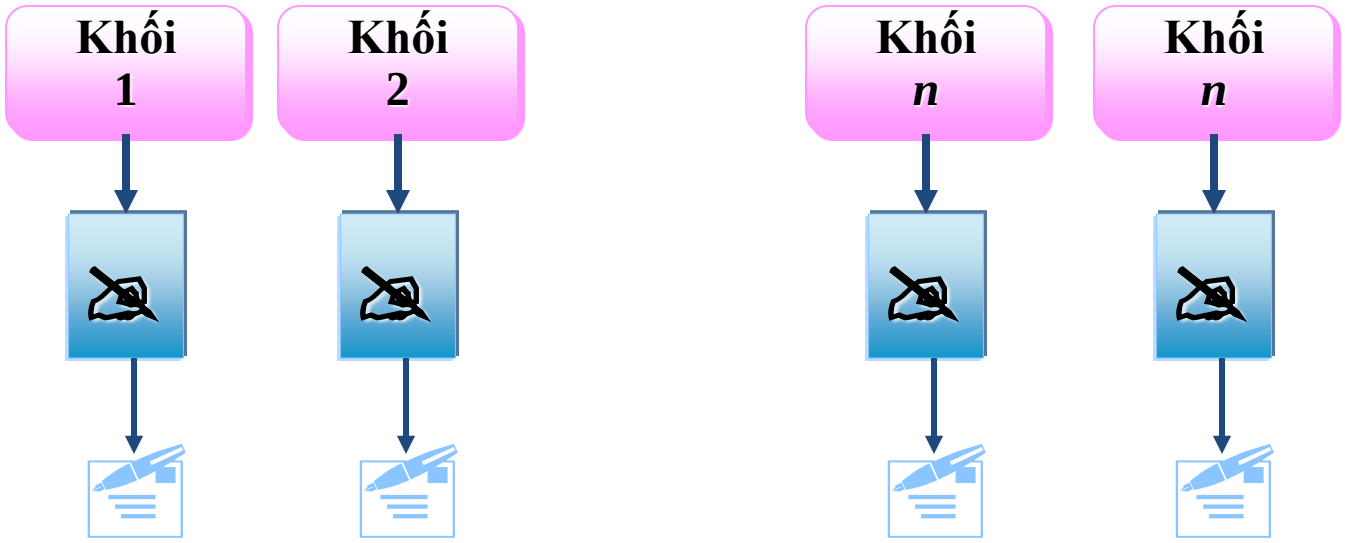
Một số lưu ý

- Khi tạo chữ ký trên văn bản cần ký, văn bản có thể dài hơn kích thước khối dữ liệu của thuật toán tạo chữ ký. Giải pháp?
  - Ký từng khối?



Một số lưu ý

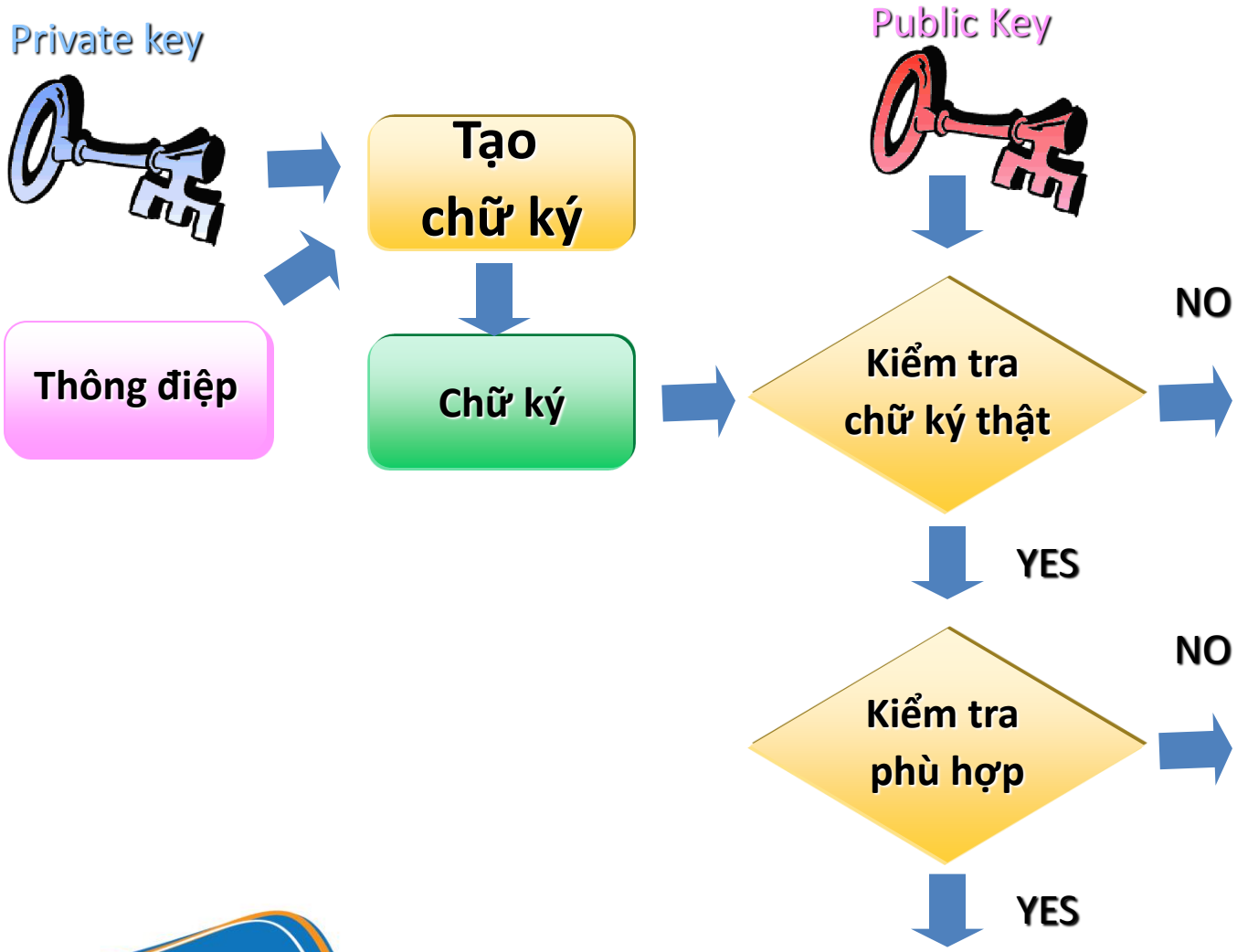
- Điều gì xảy ra:
  - Khi thay đổi thứ tự khối (và chữ ký tương ứng?)
  - Khi bỏ bớt/lặp lại nhiều lần 1 khối (và chữ ký tương ứng?)



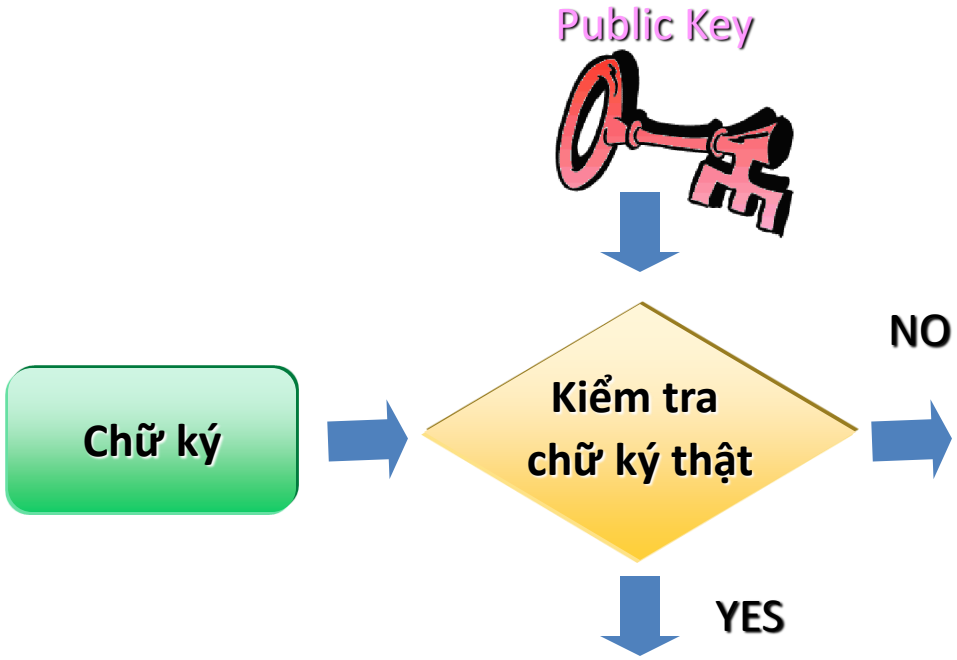
Một số lưu ý

- Trong chiến lược chữ ký đính kèm (appendix), quá trình kiểm tra chữ ký thực chất gồm 2 công đoạn:
  - Kiểm tra chữ ký “thật”?
  - Kiểm tra chữ ký có phù hợp với văn bản?

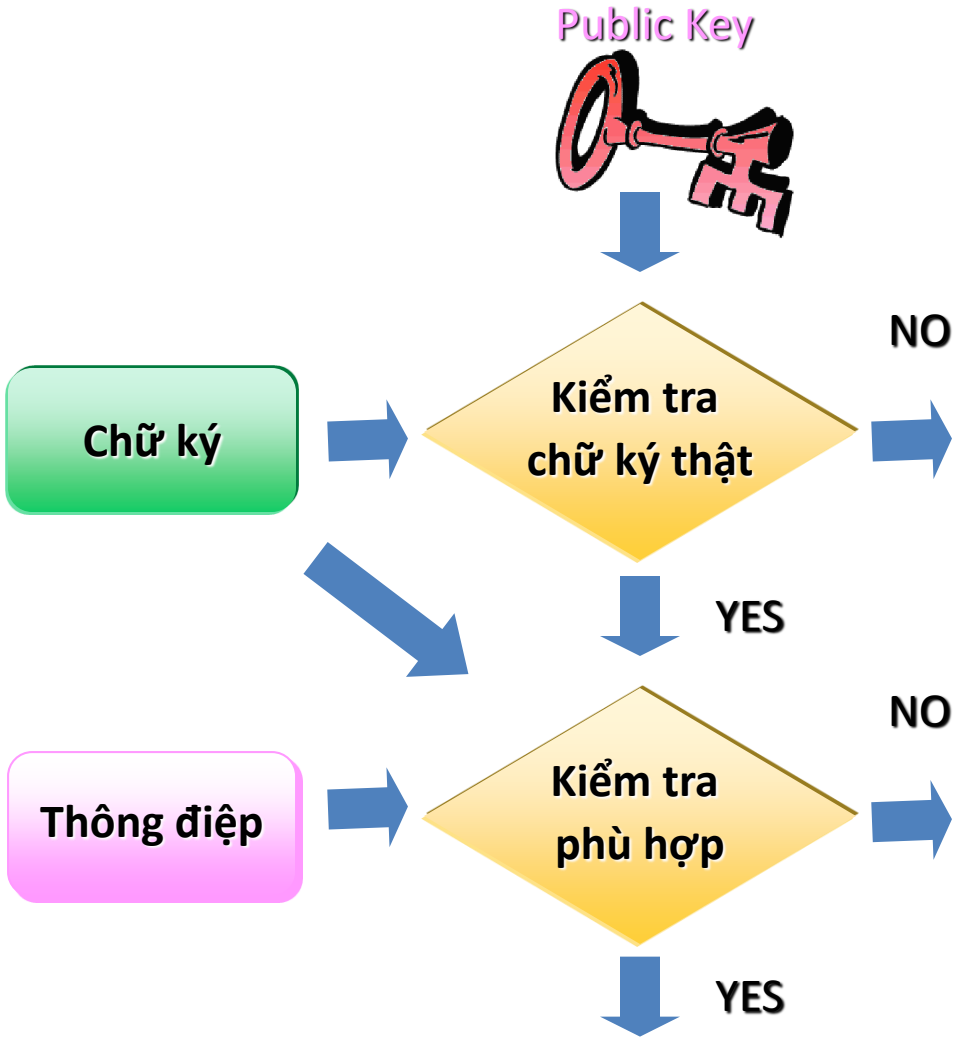
Một số lưu ý


Private key
Public Key
Tạo chữ ký
Thông điệp
Chữ ký
Kiểm tra chữ ký thật
NO
YES
Kiểm tra phù hợp
NO
YES

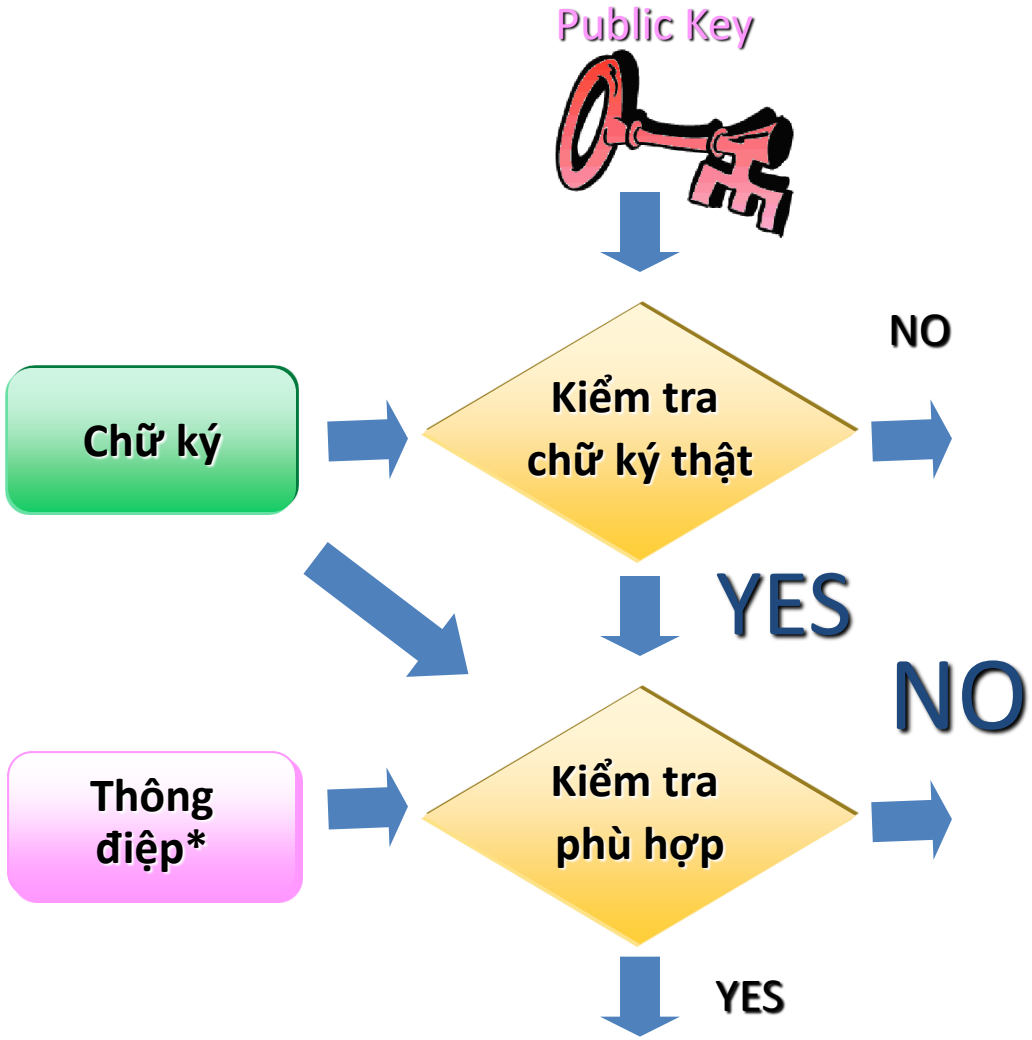
Một số lưu ý



Một số lưu ý


Public Key
Chữ ký
Kiểm tra
chữ ký thật
NO
YES
Thông điệp
Kiểm tra
phù hợp
NO
YES

Một số lưu ý


Public Key
Chữ ký
Kiểm tra chữ ký thật
NO
YES
Thông điệp*
Kiểm tra phù hợp
NO
YES

Phụ lục

Phương pháp DSA

Digital Signature Algorithm

Digital Signature Standard (DSS)

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Phương pháp DSA

- Phát sinh khóa:
  1. Chọn 1 số nguyên tố q 160 bit
  2. Chọn $0 \le t \le 8$, chọn $2^{511+64t} < p < 2^{512+64t}$ với $q|p-1$
  3. Chọn g trong Z_p^*, và $\alpha = g^{(p-1)/q} \bmod p$, $\alpha \neq 1$ (α là phần tử sinh của nhóm con bậc q của Z_p^*)
  4. Chọn $1 \le a \le q-1$, tính $y = \alpha^a \bmod p$
  5. public key (p, q, α, y), private key a

Phương pháp DSA

- Tạo chữ ký:
  - Chọn ngẫu nhiên số nguyên k, $0 < k < q$
  - Tính $r=(\alpha^k \bmod p) \bmod q$
  - Tính $k^{-1} \bmod q$
  - Tính $s=k^{-1} * (h(m) + ar) \bmod q$
  - Chữ ký = (r, s)

Phương pháp DSA

- Kiểm tra chữ ký
  - Kiểm tra $0<r<q$ và $0<s<q$, nếu không thỏa thì kết luận là không chữ ký hợp lệ
  - Tính $w= s^{-1} \bmod q$ và $h(m)$
  - Tính $u_1=w*h(m) \bmod q$, $u_2=r*w \bmod q$
  - Tính $v = (\alpha^{u_1} y^{u_2} \bmod p) \bmod q$
  - Chữ ký hợp lệ $\Leftrightarrow v = r$

$$h(m) \equiv -ar + ks \pmod{q}$$

$$wh(m) + arw \equiv k \pmod{q}$$

$$u_1 + au_2 \equiv k \pmod{q}$$

$$\alpha^{u_1} y^{u_2} \bmod p \pmod{q} = \alpha^{k} \bmod p \pmod{q}$$

Phương pháp DSA

- Vấn đề an toàn của DSA: bài toán logarithm rời rạc trên Z_P^* và trên nhóm con cyclic bậc q
- Các tham số:
  - q~160bit, p 768~1Kb
- Xác suất thất bại: trong quá trình kiểm tra, ta cần tính nghịch đảo của s. Nếu s=0 thì không tồn tại nghịch đảo

$$Pr[s=0]= (1/2)^{160}$$

Phương pháp DSA

- Tính hiệu quả
  - Tạo chữ ký
    - Một thao tác tính lũy thừa modulo
    - Một số thao tác 160-bit (nếu p ~ 768 bit)
    - Việc tính lũy thừa có thể được tính sẵn trước
    - ***Nhanh hơn phương pháp RSA***
  - Kiểm tra chữ ký
    - Hai thao tác tính lũy thừa modulo
    - ***Châm hơn phương pháp RSA***

Phương pháp ElGamal

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Phương pháp ElGamal

- Phát sinh khóa : p, q, α, a, $y=\alpha^a \bmod p$
  - α là phần tử sinh của Z^*_p
  - Public key (p, α), private key (a)
- Tạo chữ ký
  - Chọn ngẫu nhiên k, $1 \le k \le p-1$, $\gcd(k, p-1)=1$
  - Tính $r = \alpha^k \bmod p$
  - Tính $k^{-1} \bmod (p-1)$
  - Tính $s = k^{-1} * (h(m) - ar) \bmod (p-1)$
  - Chữ ký là (r,s)

Phương pháp ElGamal

- Kiểm tra chữ ký
  - Kiểm tra $1 \le r \le p\text{-}1$
  - Tính $v_1 = y^r r^s \bmod p$
  - *Tính* $h(m)$ và $v_2 = \alpha^{h(m)} \bmod p$
  - Chữ ký hợp lệ $\Leftrightarrow v_1 = v_2$

$$s \equiv k^{-1}\{h(m) - ar\} \pmod{p-1}$$

$$ks \equiv h(m) - ar \pmod{p-1}$$

$$\alpha^{h(m)} \equiv \alpha^{ar+ks} \equiv (\alpha^a)^r r^s \pmod{p}$$

Phương pháp ElGamal

- Một số vấn đề
  - Giá trị *k* phải phân biệt cho mỗi thông điệp được ký
    - $(s_1-s_2)k=(h(m_1)-h(m_2))\mod (p-1)$
    - Nếu $\gcd((s_1-s_2),p-1)=1$ thì có thể dễ dàng xác đinh giá trị *k*, từ đó có được private key *a*
  - Nếu không dùng hàm băm thì có thể bị tình trạng existential forgery

Phương pháp ElGamal

- Tính hiệu quả
  - Tạo chữ ký
    - Một thao tác tính lũy thừa modulo
    - Một thao tác sử dụng thuật toán Euclide để tính nghịch đảo
    - Hai thao tác nhân modulo
  - Kiểm tra chữ ký
    - Ba thao tác lũy thừa modulo
- Đọc thêm: Generalized ElGamal Signature