Chương IX

4

CHỮ KÝ ĐIỆN TỬ - CHỮ KÝ SỐ

(ELECTRONIC SIGNATURE - DIGITAL SIGNATURES)

Nội dung chính

1. Khái niệm về chữ ký số (Digital Signature)
2. Các dịch vụ bảo mật cung cấp bởi chữ ký số
3. Một vài chữ ký số thông dụng
4. Mô tả vài ứng dụng của chữ ký số

(*Cryptography & Network Security*. McGraw-Hill, Inc., 2007., Chapter 13)

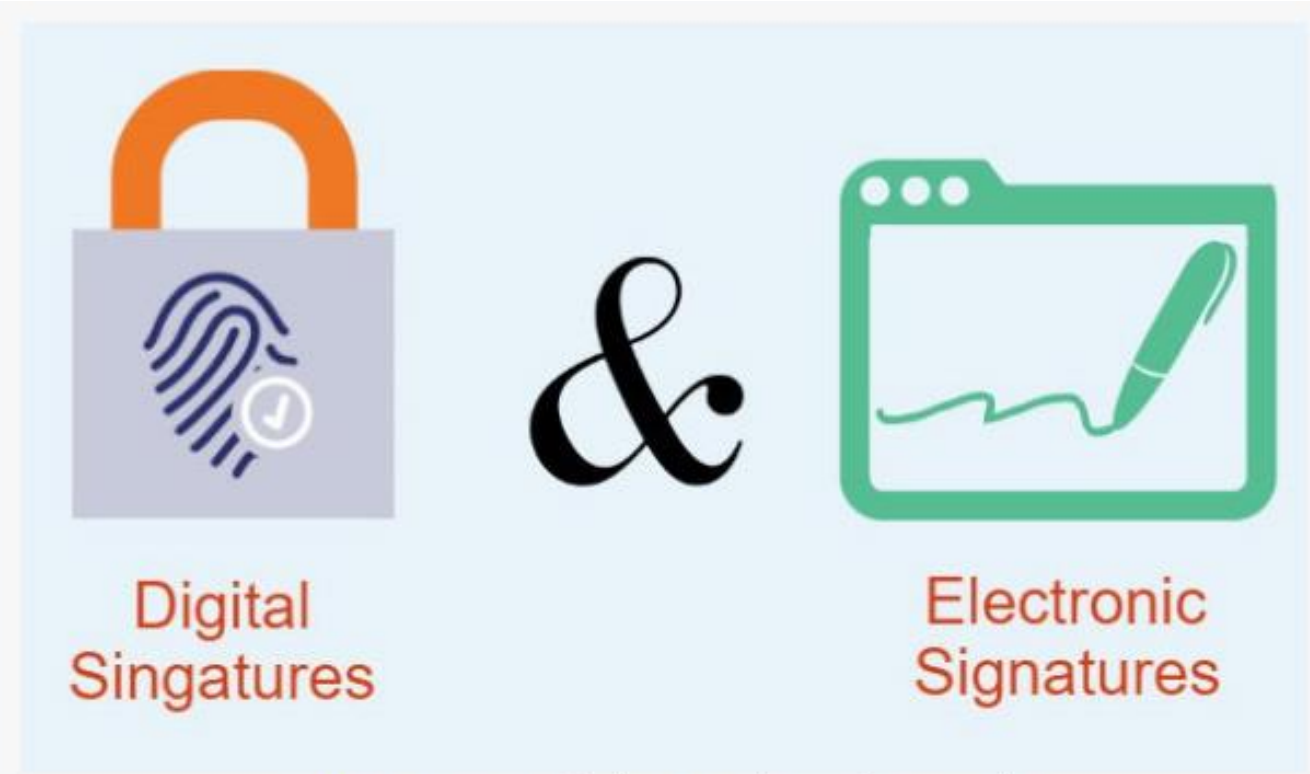
Khái niệm về chữ ký điện tử và chữ ký số (Electronic Signature and Digital Signature)

- **Chữ ký điện tử (electronic signature)** được đề cập tại khoản 1 Điều 21 Luật Giao dịch điện tử năm 2005.
- Chữ ký điện tử là dạng thông tin đi kèm dữ liệu (văn bản, hình ảnh, video…) nhằm mục đích xác định người ký của dữ liệu đó và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký.
- **Chữ ký điện tử** là một thay thế cho chữ ký viết tay của cá nhân hay doanh nghiệp.

Khái niệm về chữ ký điện tử và chữ ký số (Electronic Signature and Digital Signature)

- **Chữ ký số** là một dạng của chữ ký điện tử. Chữ ký số là thông tin đi kèm theo các tài liệu điện tử như Word, Excel, PDF,…; hình ảnh; video…) nhằm đảm bảo tính xác thực của người ký. Nó mã hóa tài liệu và nhúng vĩnh viễn thông tin vào đó. Bất kỳ thay đổi nào trong các tài liệu sau khi nó đã được ký là vô hiệu, do đó nó bảo vệ, chống lại sự giả mạo chữ ký và thông tin giả mạo.
- **Chữ ký số** giúp các tổ chức duy trì ký xác thực, trách nhiệm giải trình, tính toàn vẹn dữ liệu và không thoái thác tài liệu điện tử và các hình thức ký kết.
- Nó có vai trò như chữ ký đối với cá nhân hay con dấu đối với tổ chức, doanh nghiệp và dùng để xác nhận lời cam kết của tổ chức, cá nhân đó trong văn bản mình đã ký trên môi trường điện tử số. Chữ ký số được được thừa nhận về mặt pháp lý.

Khái niệm về chữ ký điện tử và chữ ký số (Electronic Signature and Digital Signature)



Chữ ký điện tử và chữ ký số giống nhau là đều thay thế cho chữ viết tay

Ứng dụng của chữ ký điện tử và chữ ký số (Electronic Signature and Digital Signature)

- Giúp các doanh nghiệp có thể ký hợp đồng làm ăn với các đối tác qua online. Đơn giản chỉ cần ký vào file tài liệu văn bản (Word, Excel, PDF,…) rồi gửi qua mail. Chữ ký điện tử dùng nhiều trong các trường hợp kê khai, nộp thuế trực tuyến, khai báo hải quan,…
- Chữ ký số tương đương với chữ ký tay nên có giá trị sử dụng trong các ứng dụng giao dịch điện tử với máy tính và mạng Internet. Nó có thể giúp bạn bảo đảm an toàn, nhất là các giao dịch chứa các thông tin liên quan đến tài chính.

Lợi ích của chữ ký điện tử và chữ ký số (Electronic Signature and Digital Signature)

Việc sử dụng chữ ký điện tử và chữ ký số giúp doanh nghiệp tối ưu hóa các thủ tục và quy trình giao dịch trực tuyến, cụ thể như:

- Tiết kiệm được thời gian và chi phí trong quá trình hoạt động giao dịch điện tử.
- Linh hoạt trong cách thức ký kết các văn bản hợp đồng, buôn bán,… có thể diễn ra ở bất kỳ nơi đâu, ở bất kỳ thời gian nào.
- Đơn giản hóa quy trình chuyển, gửi tài liệu, hồ sơ cho đối tác khách hàng, cơ quan tổ chức.
- Bảo mật danh tính của cá nhân, doanh nghiệp an toàn.
- Thuận lợi trong việc nộp hồ sơ thuế, kê khai thuế cho doanh nghiệp khi chỉ cần sử dụng chữ ký điện tử thực hiện các giao dịch điện tử là có thể hoàn thành xong các quá trình đó.
- Bảo mật danh tính của cá nhân, doanh nghiệp một cách an toàn.

Giá trị pháp lý của chữ ký điện tử (Electronic Signature and Digital Signature)

Trong trường hợp pháp luật quy định văn bản cần có chữ ký thì yêu cầu đó đối với một thông điệp dữ liệu được xem là đáp ứng nếu chữ ký điện tử được sử dụng để ký thông điệp dữ liệu đó đáp ứng các điều kiện sau đây:

- Phương pháp tạo chữ ký điện tử cho phép xác minh được người ký và chứng tỏ được sự chấp thuận của người ký đối với nội dung thông điệp dữ liệu.
- Phương pháp tạo chữ ký phải đủ tin cậy và phù hợp với mục đích mà theo đó thông điệp dữ liệu được tạo ra và gửi đi.
- Trong trường hợp pháp luật quy định văn bản cần được đóng dấu của cơ quan, tổ chức thì yêu cầu đó đối với một thông điệp dữ liệu được xem là đáp ứng nếu thông điệp dữ liệu đó được ký bởi chữ ký điện tử của cơ quan, tổ chức đáp ứng các điều kiện quy định tại khoản 1 Điều 22 của Luật Giao dịch Điện tử và chữ ký điện tử đó có chứng thực.

Giá trị pháp lý của chữ ký số (Electronic Signature and Digital Signature)

Để đảm bảo giá trị pháp lý, chữ ký số phải đáp ứng các điều kiện như sau:

- Chữ ký số được tạo ra khi chứng thư số có hiệu lực và có thể kiểm tra được bằng khoá công khai ghi trên chứng thư số có hiệu lực đó.
- Chữ ký số được tạo ra bằng khoá bí mật tương ứng với khoá công khai ghi trên chứng thư số do tổ chức có thẩm quyền cấp.
- Khóa bí mật chỉ thuộc sự kiểm soát của người ký tại thời điểm ký.
- Khóa bí mật và nội dung thông điệp dữ liệu chỉ gắn duy nhất với người ký khi người đó ký số thông điệp dữ liệu.

Sự khác biệt giữa chữ ký điện tử và chữ ký số (Electronic Signature and Digital Signature)

CHỮ KÝ ĐIỆN TỬ	CHỮ KÝ SỐ
Tính chất: Chữ ký điện tử có thể là bất kỳ biểu tượng, hình ảnh, quy trình nào được đính kèm với tin nhắn hoặc tài liệu biểu thị danh tính của người ký và hành động đồng ý với nó.	Chữ ký số có thể được hình dung như một "dấu vân tay" điện tử, được mã hóa và xác định danh tính người thực sự ký nó.
Tiêu chuẩn: Chữ ký điện tử Không phụ thuộc vào các tiêu chuẩn.Không sử dụng mã hóa	Sử dụng các phương thức mã hóa mật mã.
Cơ chế xác thực: Chữ ký điện tử Xác minh danh tính người ký thông qua email, mã PIN điện thoại, v.v.	ID kỹ thuật số dựa trên chứng chỉ.

Sự khác biệt giữa chữ ký điện tử và chữ ký số (Electronic Signature and Digital Signature)

CHỮ KÝ ĐIỆN TỬ	CHỮ KÝ SỐ
Tính năng - Chữ ký điện tử Xác minh một tài liệu.	- Bảo mật một tài liệu.
Xác nhận - Chữ ký điện tử Không có quá trình xác nhận cụ thể.	- Được thực hiện bởi các cơ quan chứng nhận tin cậy hoặc nhà cung cấp dịch vụ ủy thác.
Bảo mật - Chữ ký điện tử Dễ bị giả mạo.	- Độ an toàn cao.

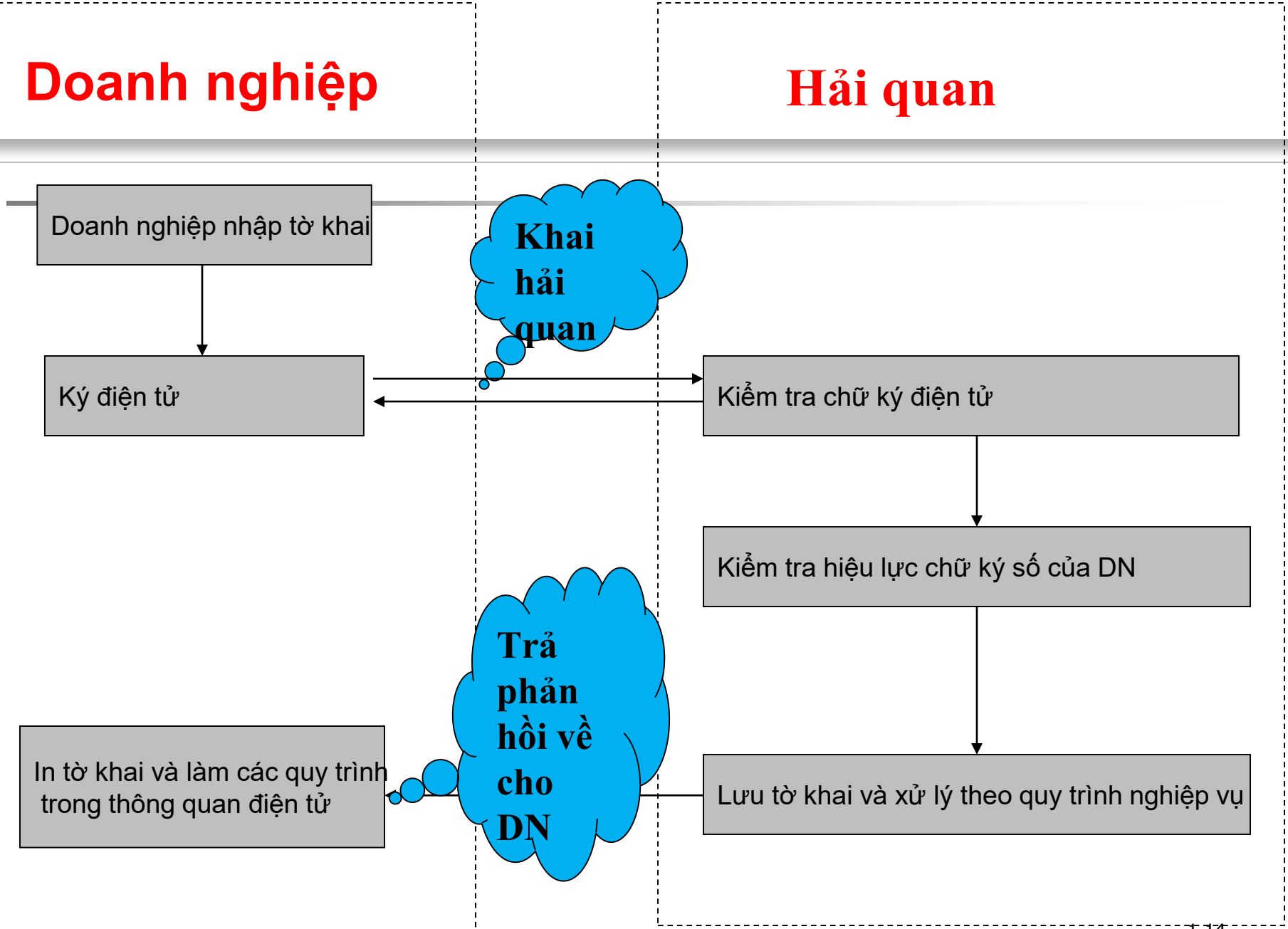
Khái niệm về chữ ký số

- Khái niệm về Digital Signature được để xuất bởi Diffie & Hellman (1976).
- 1989, phiên bản thương mại Chữ ký số đầu tiên trong Lotus Notes, dựa trên RSA
- Có nhiều loại chữ ký khác nhay như: chữ ký RSA, chữ ký ECC, chữ ký ElGamal
- “Chữ ký số là thông tin được mã hoá bằng Khoá riêng của người gửi, được gửi kèm theo văn bản nhằm đảm bảo cho người nhận định danh, xác thực đúng nguồn gốc và tính toàn vẹn của tài liệu nhận.
- Chữ ký số và chữ ký tay đều có chung đặc điểm là rất khó có thể tìm được hai người có cùng một chữ ký.

Khái niệm về chữ ký số

- Chữ ký số là một trong ứng dụng quan trọng nhất của mã hóa khóa công khai.
- Message Authentication chỉ bảo vệ thông điệp trao đổi giữa hai bên tham gia không bị hiệu chỉnh hay giả mạo từ bên thứ 3, nhưng nó không bảo vệ thông điệp bị hiệu chỉnh hay giả mạo từ một trong 2 bên tham gia, nghĩa là:
  - Bên nhận giả mạo thông điệp của bên gửi
  - Bên gửi chối là đã gửi thông điệp đến bên nhận
- Chữ ký số không những giúp xác thực thông điệp mà còn bảo vệ quyền lợi mỗi bên tham gia.

VÍ DỤ CHỮ KÝ SỐ TRONG THỦ TỤC HQĐT



Mục tiêu của chữ ký số

Mục tiêu an toàn

- Xác thực (Authentication)
- Chống phủ nhận (Non-repudiation)

Đặc điểm chữ ký số

1. Đảm bảo tính xác thực

- Chứng minh tính hợp pháp của người gửi
- Chứng minh tính toàn vẹn của dữ liệu

2. Chữ ký số là hàm của các tham số

- Thông báo giao dịch (văn bản gốc)
- Thông tin bí mật của người gửi (Khóa riêng của sender)
- Thông tin công khai trên mạng (Khóa công khai)
- Mã xác thực : Đảm bảo tính toàn vẹn của thông điệp

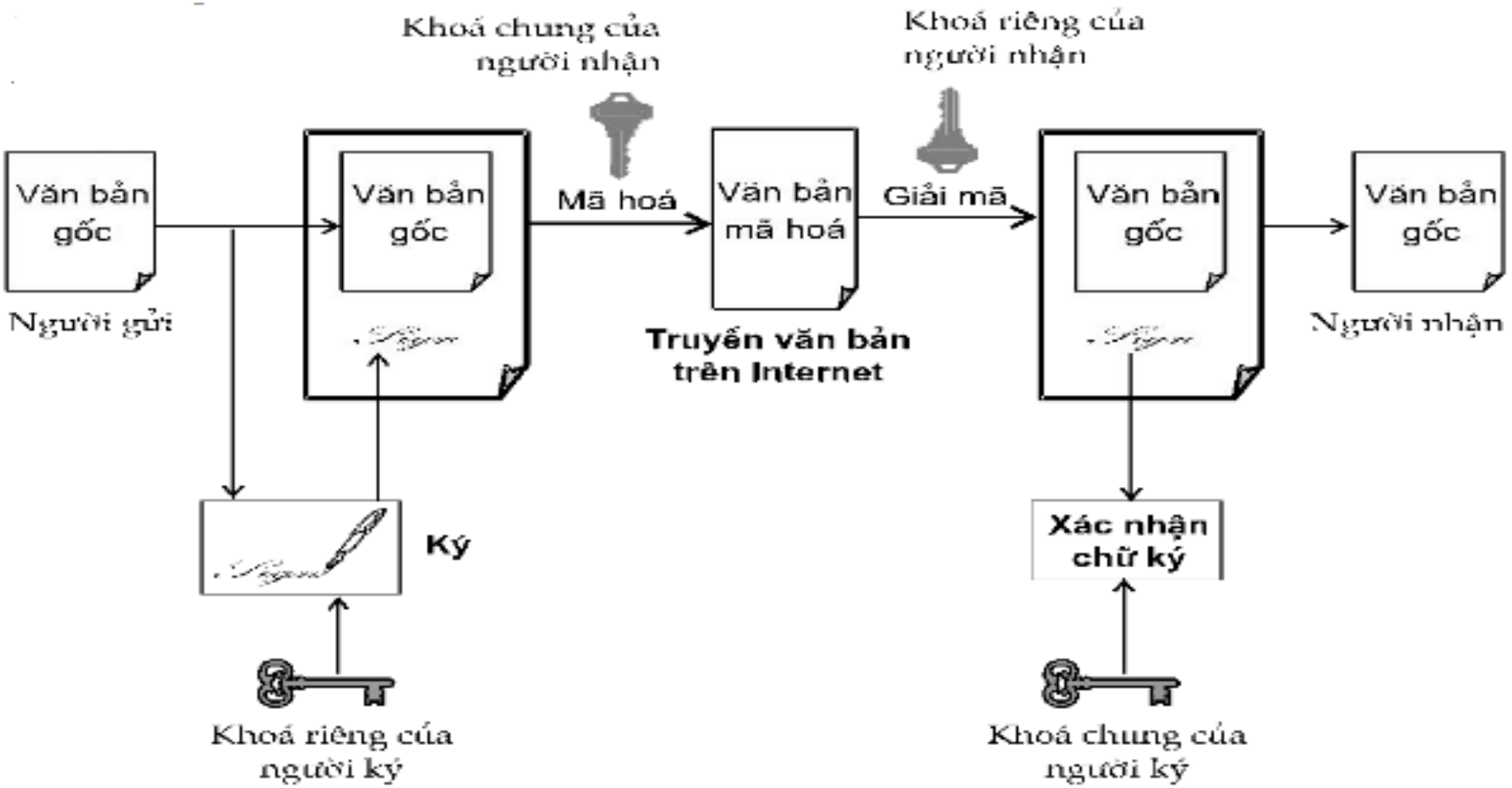
Đặc điểm chữ ký số

Khóa bí mật	**Tính bí mật của Khóa bí mật**	Chỉ có người chủ mới biết
Khóa công khai	**Tính sẵn sàng truy cập của khóa công khai**	Có thể truy cập thông qua phương tiện thông dụng vào bất cứ thời điểm: Chứa trong một thư mục công cộng Đảm bảo tính chính xác và không giả mạo
Chứng thư số	**Công bố khóa công khai**	Được cấp phát bởi tổ chức có thẩm quyền
Độ dài khóa	**Tương ứng tính an toàn của khóa**	Khóa có thể có độ dài (thông dụng là) 512, 1024, 2048, 4096 Khóa càng dài mã càng chậm
Tính pháp lý	**Với công nghệ đảm bảo sẽ tương đương chữ ký tay**	Được cấp phát theo quy trình an toàn với các thông số kỹ thuật đảm bảo Được lưu trữ an toàn
Tính khả dụng	**Ngày càng dễ sử dụng**	Được lưu trong các thiết bị cá nhân như USB-token, smart card

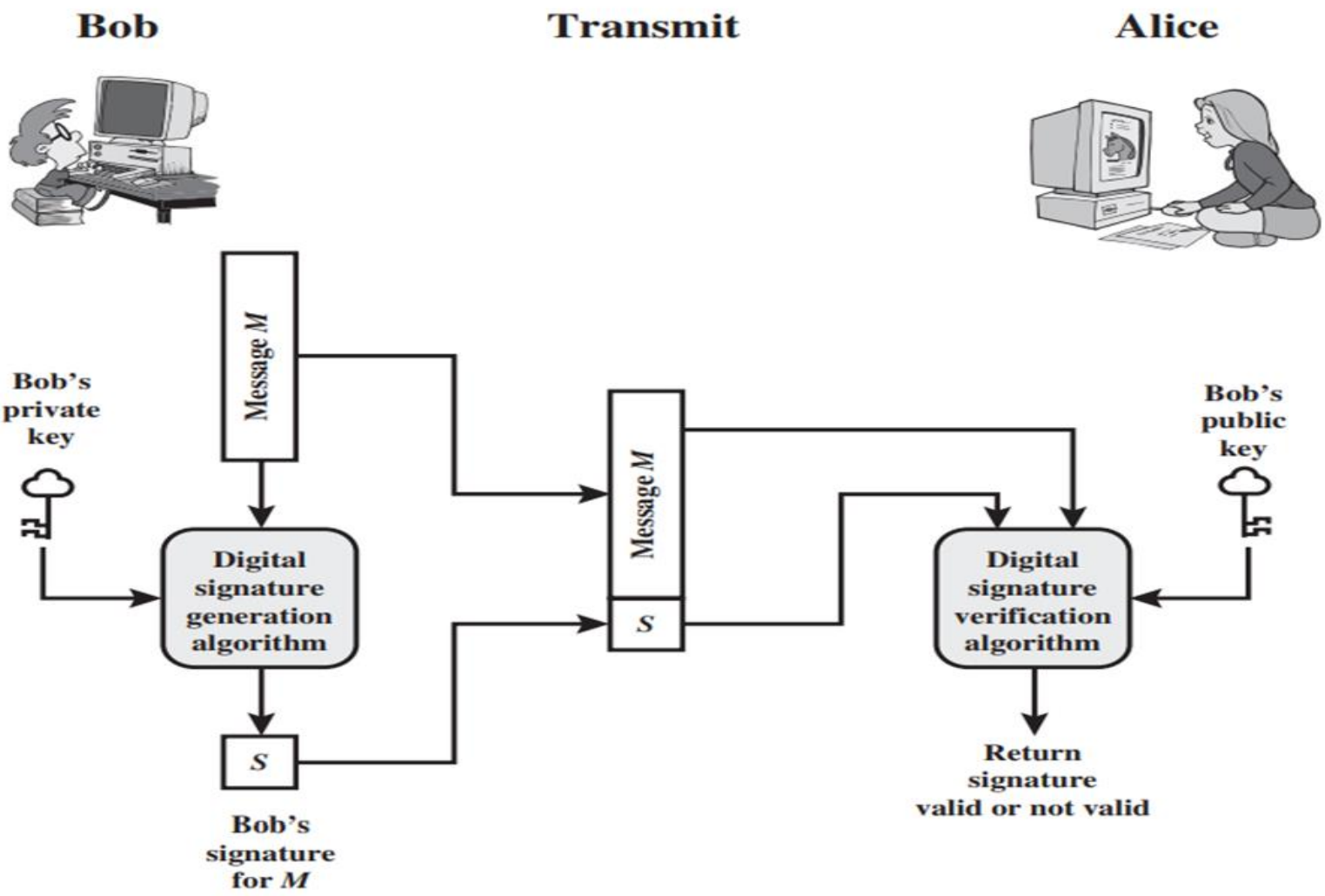
Nguyên lý ký điện tử trong hệ mật mã công khai

- Tạo chữ ký và gửi chữ ký & thông điệp
  - Người gửi sẽ dùng một thuật toán tạo chữ ký (signing algorithm) để tạo chữ ký của mình thông điệp bằng khóa Private Key của mình
  - Gửi chữ ký kèm thông điệp cho người nhận
- Thẩm tra chữ ký
  - Người nhận sẽ dùng một thuật toàn thẩm tra chữ ký (Verifying algorithm) để thẩm tra chữ ký có phải của người gửi không.
  - Nếu đúng, thông điệp được chấp nhận, ngược lại sẽ từ chối thông điệp

Sơ đồ sử dụng chữ ký số

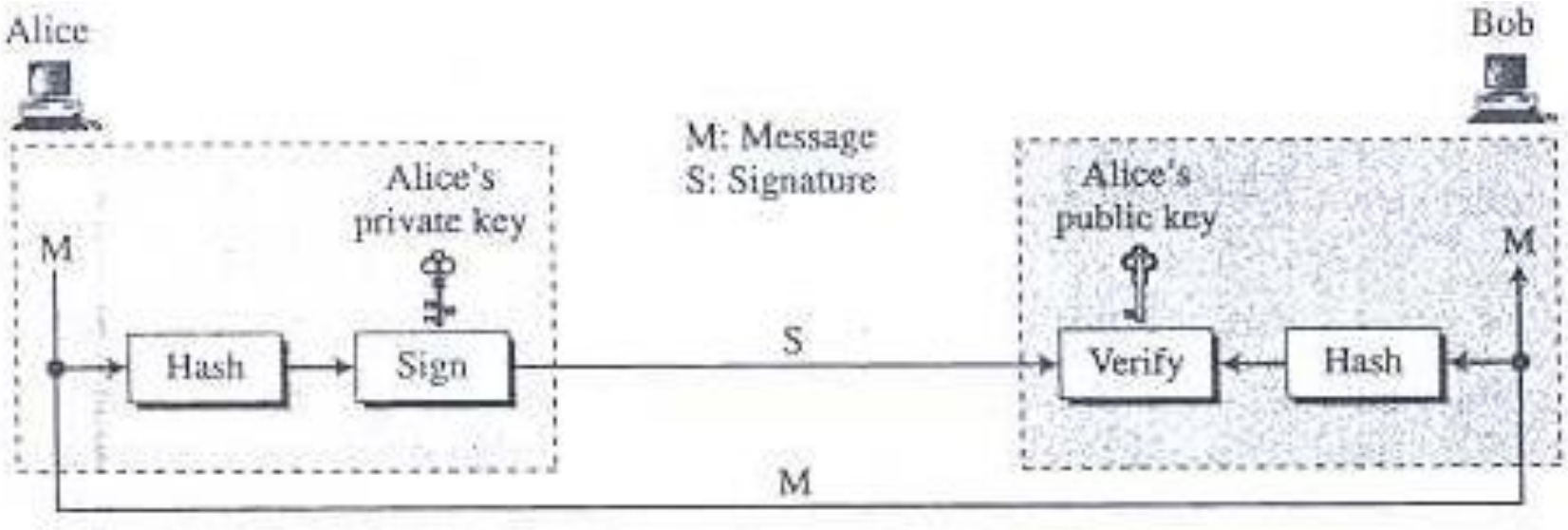


Sơ đồ sử dụng chữ ký số



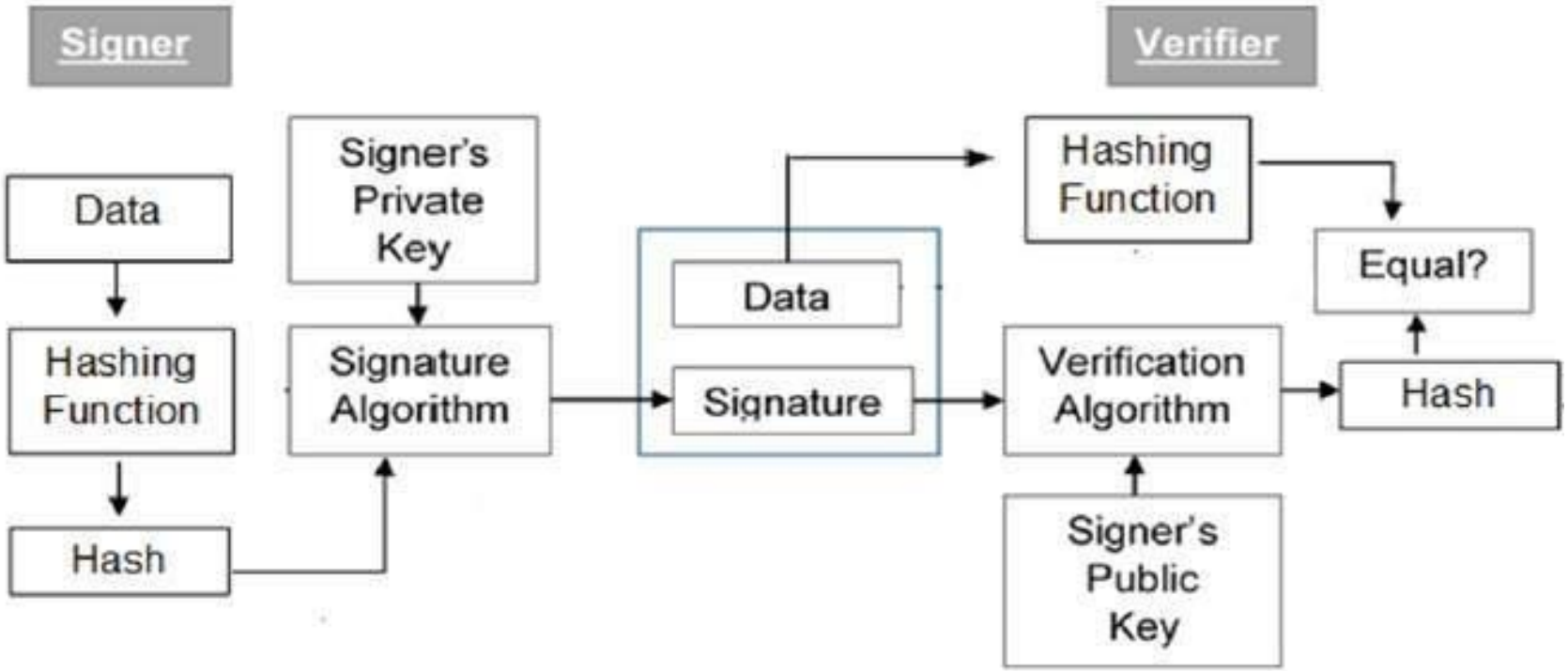
Hàm băm mật mã
Signing the Digest

- Ký trên digest của thông điệp sẽ ngắn hơn ký trên thông điệp
- Người gửi có thể ký trên cốt thông điệp và người nhận có thể kiểm tra trên cốt thông điệp

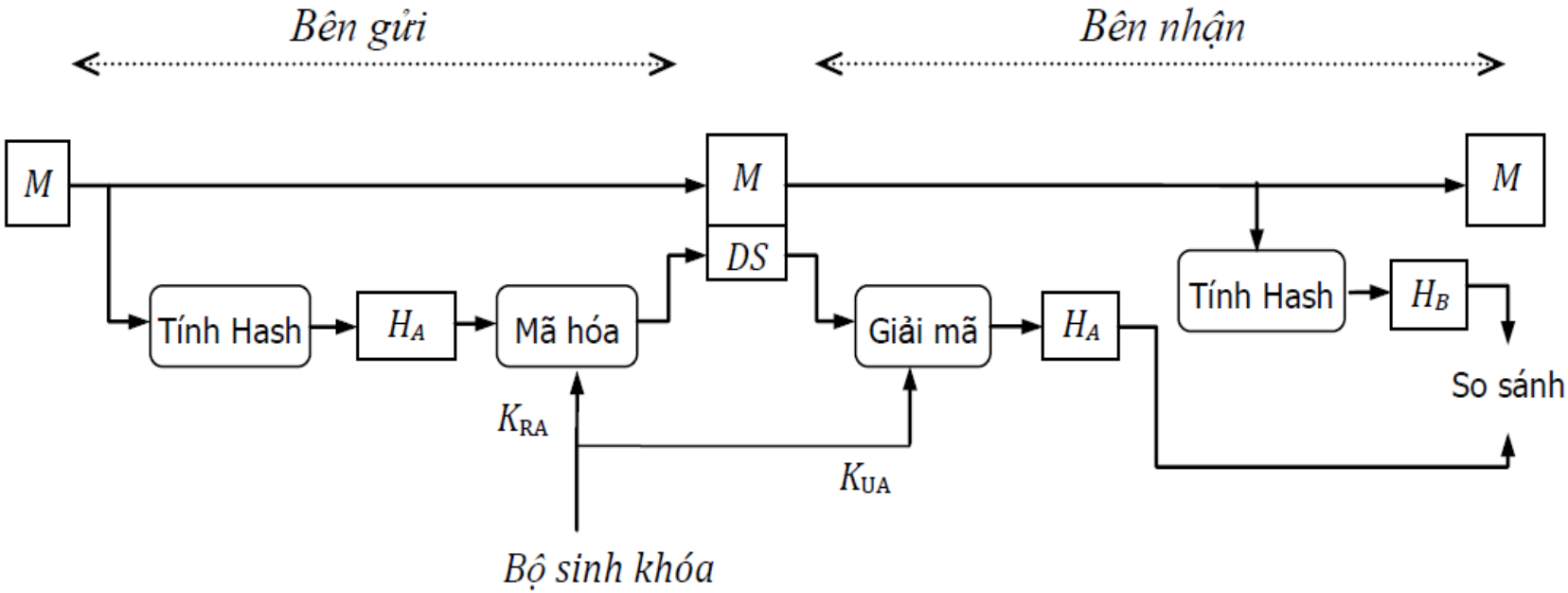


Digital Signature Process
Tạo và Kiểm tra chữ ký số

- Chữ ký với hàm băm
  - Chữ ký sẽ ngắn (nhẹ) → tăng hiệu năng cho hệ thống



Digital Signature Process
Tạo và Kiểm tra chữ ký số



DS: Data signature – chữ ký điện tử

Nhận xét

- Chữ ký không phải là nét vẽ ngoằn ngoèo khó bắt chước mà là một dãy số trích từ đặc trưng văn bản đã được mã hóa.
- So với chữ ký thông thường, chữ ký số có ưu thế vượt trội hơn chữ ký tay.
  - Chính xác tuyệt đối
  - Kiểm định dễ dàng và chính xác

"Chữ ký điện tử mở đường cho các dịch vụ có độ tin cậy cao"

Nhược điểm mô hình chữ ký số

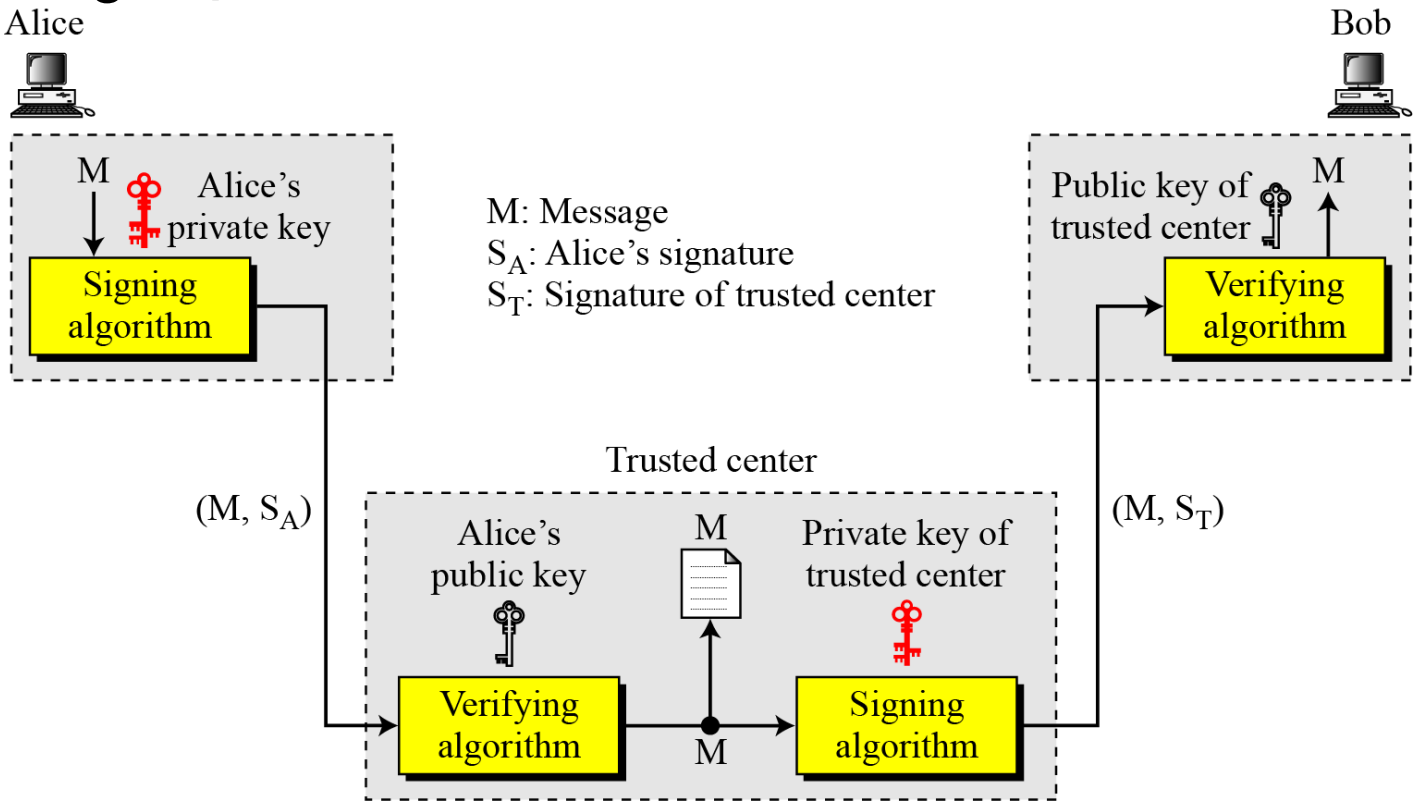
- Mô hình CKS ở trên chỉ đạt được nếu như mỗi người sở hữu đúng cặp chìa khóa của chính mình.
- Có thể xẩy ra hiện tượng "*mạo danh*" người gởi. Do đó, ta cần có cơ chế để xác định *"ai là ai"* trên toàn hệ thống.
- Giải pháp: chứng minh thư số

Ứng dụng của chữ ký số

1. Xác thực thông điệp (Message Authentication): Người ký được xác nhận là chủ chữ ký.
2. Toàn vẹn thông điệp (Message Integrity): Nội dung chưa bị thay đổi hoặc xáo trộn kể từ khi nó được ký điện tử.
3. Chống từ chối (Non-repudiation): Chứng minh với tất cả các bên về nguồn gốc của nội dung đã ký. Từ "thoái thác" dùng để chỉ hành động của một người ký từ chối bất kỳ mối liên kết nào với nội dung đã ký.
4. Bảo mật (Confidentiality)

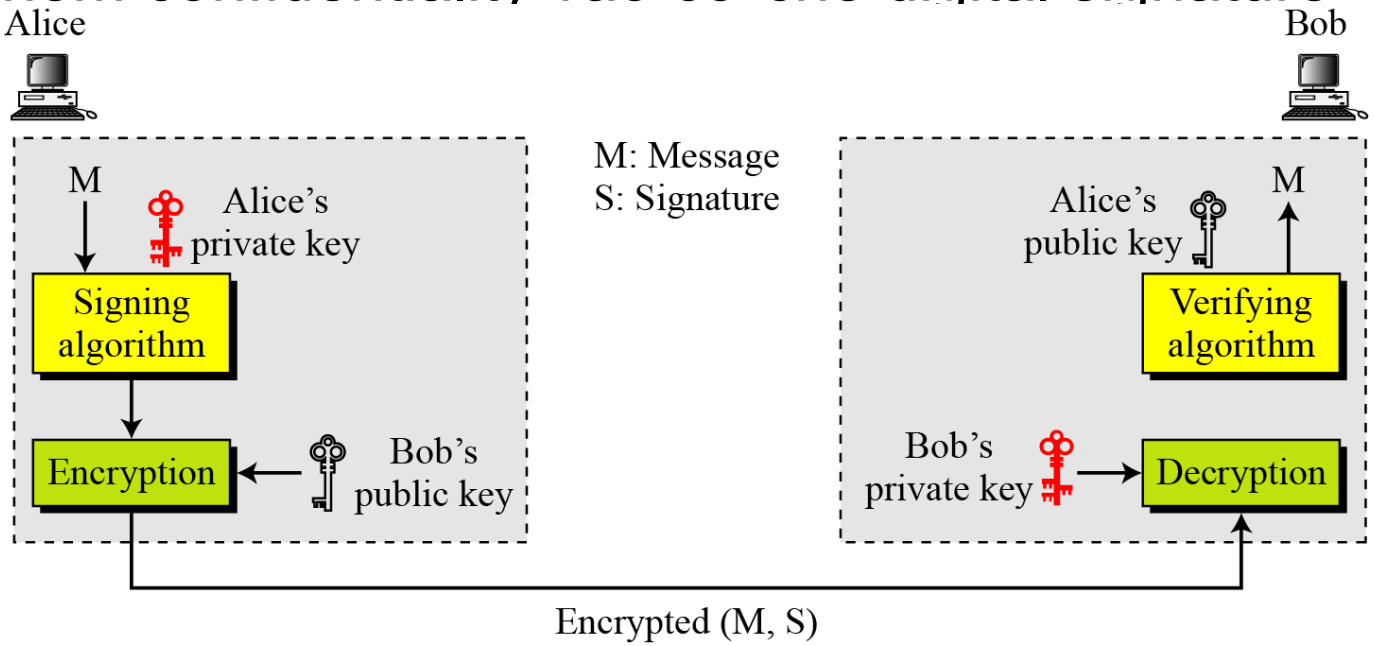
Nonrepudiation

- Nonrepudiation có thể được cung cấp bằng cách dùng một trusted Center



Confidentiality

- Thêm confidentiality vào cơ chế digital signature



Một Digital Signature không cung cấp tính bí mật. Nếu cần bảo mật, encryption/decryption được áp dụng

Public Notary (công chứng)

- Trong trường hợp bên Alice cố cãi rằng cô ta chẳng may làm thất lạc hay vô tình đánh lộ zA và bị một kẻ thứ ba lợi dụng chứ không có ý định tạo ra văn bản có chữ ký như thế→ khi đó có thể thêm trọng tài vào hệ thống.
- Người trọng tài này cũng còn gọi là công chứng viên (public notary) sẽ ký đè lên chữ ký của Alice để chứng thực, Alice không thể nào chối cãi.

Proof of delivery (xác nhận giao hàng - hoá đơn)

- Ngược lại, bên gửi cũng cần được bảo vệ để chống lại hiện tượng người nhận có nhận được thông báo nhưng chối là chưa nhận được.
- Điều này có thể thực hiện được qua những giao thức có phân xử (adjudicated protocol), tức là những giao thức mà sau đó cho phép người thứ ba có thể kiểm định lại được.

Tấn công trên Digital Signature

- Các loại tấn công trên Digital Signature (Attack Types)
- Giả mạo chữ ký (Forgery)

Attack Types

- Key-Only Attack
- Known-Message Attack
- Chosen-Message Attack

Forgery Types

- Existential Forgery
- Selective Forgery

Vài chữ ký số thông dụng

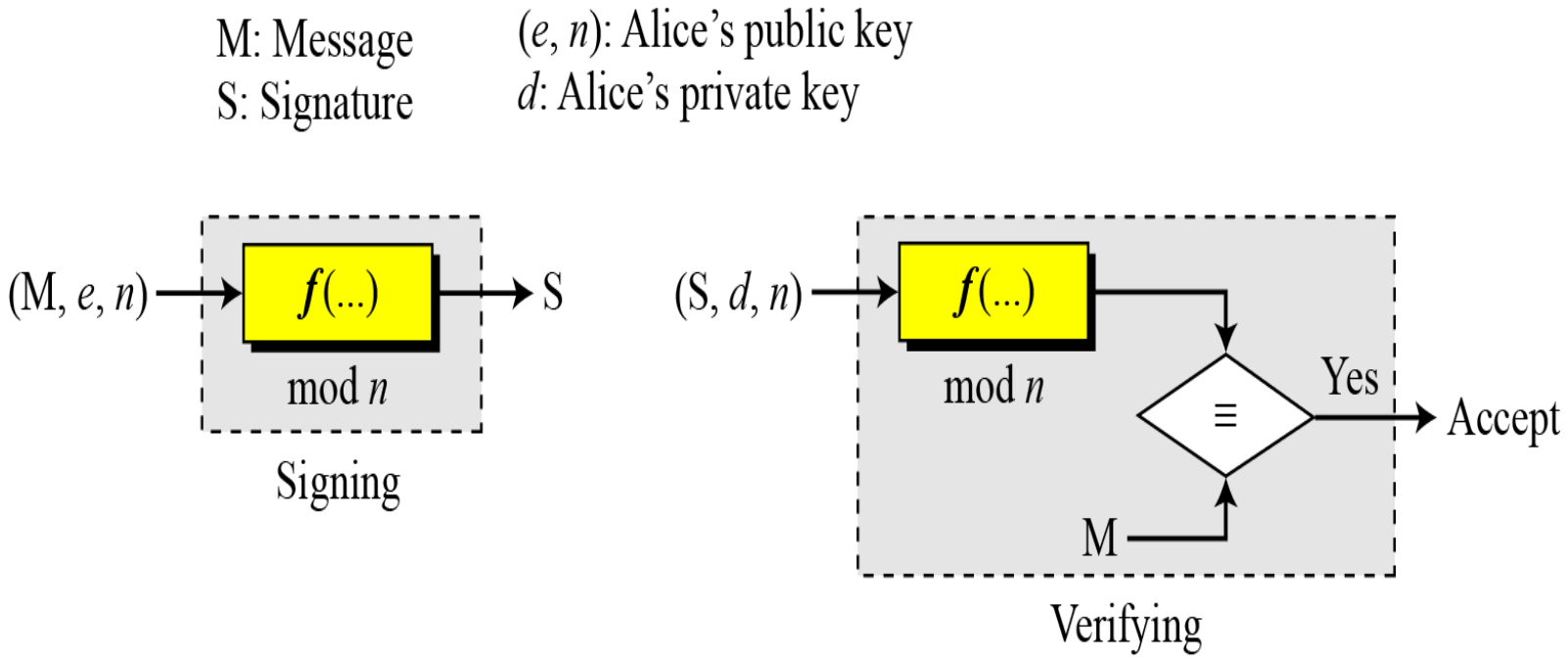
- RSA Digital Signature Scheme
- ElGamal Digital Signature Scheme
- Schnorr Digital Signature Scheme
- Digital Signature Standard (DSS)
- Elliptic Curve Digital Signature Scheme

RSA Digital Signature Scheme

- Ý tưởng mật mã RSA được dùng cho việc ký và kiểm tra chữ ký, nó được gọi là cơ chế chữ ký số RSA
- Người gửi dùng private key của chính mình để ký vào tài liệu; người nhận dùng public key của người gửi để kiểm tra chữ ký
- So với chữ ký truyền thống, private key đóng vai trò là chữ ký của chính người gửi, public key của người gửi đóng vài trò là bản sao của chữ ký mà có thể được công khai

RSA Digital Signature Scheme

- Ý tưởng tổng quát của cơ chế chữ ký RSA



RSA Digital Signature Scheme

Phát sinh khóa (Key Generation)

- Phát sinh khóa trong cơ chế chữ ký RSA là hoàn toàn giống như phát sinh khóa RSA
- Trong đó **d** là bí mật, **e** và **n** là công khai

RSA Digital Signature Scheme

1) Tạo cặp khóa (***bí mật, công khai***) (**a**, **b**):

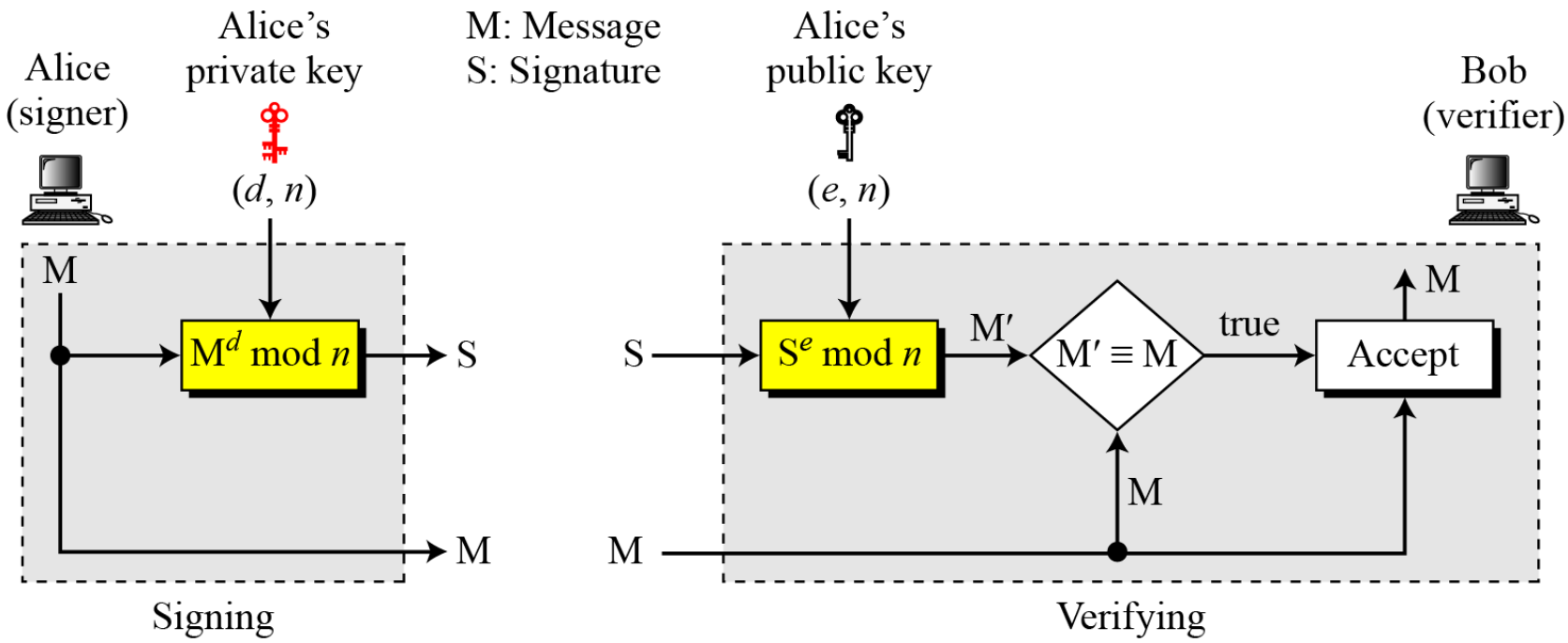
- Chọn 2 số nguyên tố **p**, **q**, xác định **n** = **p** * **q**, n là công khai, đặt P = A = Zn và định nghĩa:
- Tính $\phi(\mathbf{n}) = (\mathbf{p-1}).(\mathbf{q-1})$.
- Chọn khóa công khai **e** < $\phi(\mathbf{n})$, nguyên tố cùng nhau với $\phi(\mathbf{n})$.
- Khóa bí mật **d** là phần tử nghịch đảo của e theo mod ϕ(n): $\mathbf{e}*d \equiv \mathbf{1} \pmod{\phi(n)}$.
- Tập cặp khóa (bí mật, công khai) **K** = $\{(\mathbf{e}, d)/\ e, d \in Zn\ ,\ e*\mathbf{d} \equiv 1 \pmod{\phi(n)}\}$.

2) ***Ký số***: Chữ ký trên $\mathbf{M} \in \mathbf{P}$ là $\mathbf{S} = \mathbf{sig_k}(\mathbf{M}) = \mathbf{M^d} \pmod{\mathbf{n}}$, $S \in \mathbf{A}$

3) ***.Kiểm tra chữ ký***: $\mathbf{ver_k}(\mathbf{M}, S) = \text{TRUE} \Leftrightarrow \mathbf{M} \equiv \mathbf{S^e} \pmod{\mathbf{n}}$ với $M,S \in Z_n$.

RSA Digital Signature Scheme

Tạo và Thẩm tra chữ ký



RSA Digital Signature Scheme

Ví dụ:

Phát sinh khóa:

- Alice chọn $p = 823$ và $q = 953$, và tính $n = 784319$.
- Giá trị $\phi(n)$ là 782544
- Alice chọn $e = 313$ và tính $d = 160009$

Alice muốn ký và gửi thông điệp M=19070 cho Bob

- Tạo chữ ký:

$$S=(19070^{160009}) \bmod 784319 = 210625 \bmod 784319$$

- Gửi (M, S) cho Bob

- Bob nhận (M, S) và tính M'

$$M'=210625^{313} \bmod 784319 = 19070 \bmod 784319$$

- → $M \equiv M' \bmod n$

EXAMPLE

Chữ ký trên m = 2

******Tạo cặp khóa (bí mật, công khai)* :

Chọn 2 số nguyên tố: **p**=3, **q**=5 → **n** = **p*****q** = 3*5 = 15(công khai)

Đặt **P** = **A** = $\mathbf{Z_n}$. Tính $\phi(\mathbf{n}) = (\mathbf{p-1}).(\mathbf{q-1}) = 2 * 4 = 8$.

Chọn khóa công khai **e** = **3** < $\phi(\mathbf{n})$, nguyên tố với $\phi(\mathbf{n}) = \mathbf{8}$.

=>Tìm d: là phần tử nghịch đảo của **e** theo mod ϕ(n): e***d**≡**1** (mod ϕ(n)).

Bước i	N	b	R_{i+1}	Q_{i+1}	X_i	X_{i+1}	X_{i+2}
0	8	3	2	2	0	1	-2
1	3	2	1	1	1	-2	3
2	2	1	0	1	-2	3	-5

Vậy khóa bí mật **d** = **3**

EXAMPLE

* ***Ký số***: Chữ ký trên $\mathbf{M = 2 \in P}$ là:

$$\mathbf{S} = \mathbf{sig_k}\,(\mathrm{M}) = \mathrm{M}^{\mathbf{d}}\ (\mathrm{mod}\ \mathbf{n})$$

$$= \mathbf{2^3}\ (\mathrm{mod}\ \mathbf{15})$$

$$= \mathbf{8}, \mathbf{S \in A}.$$

* ***Kiểm tra chữ ký***:

$$\mathbf{ver_k}(\mathbf{M}, \mathrm{S}) = \mathrm{TRUE} \Leftrightarrow \mathbf{M \equiv S^e}\ (\mathrm{mod}\ \mathbf{n})$$

$$\Leftrightarrow \mathbf{2 \equiv 8^3}\ (\mathrm{mod}\ \mathbf{15}).$$

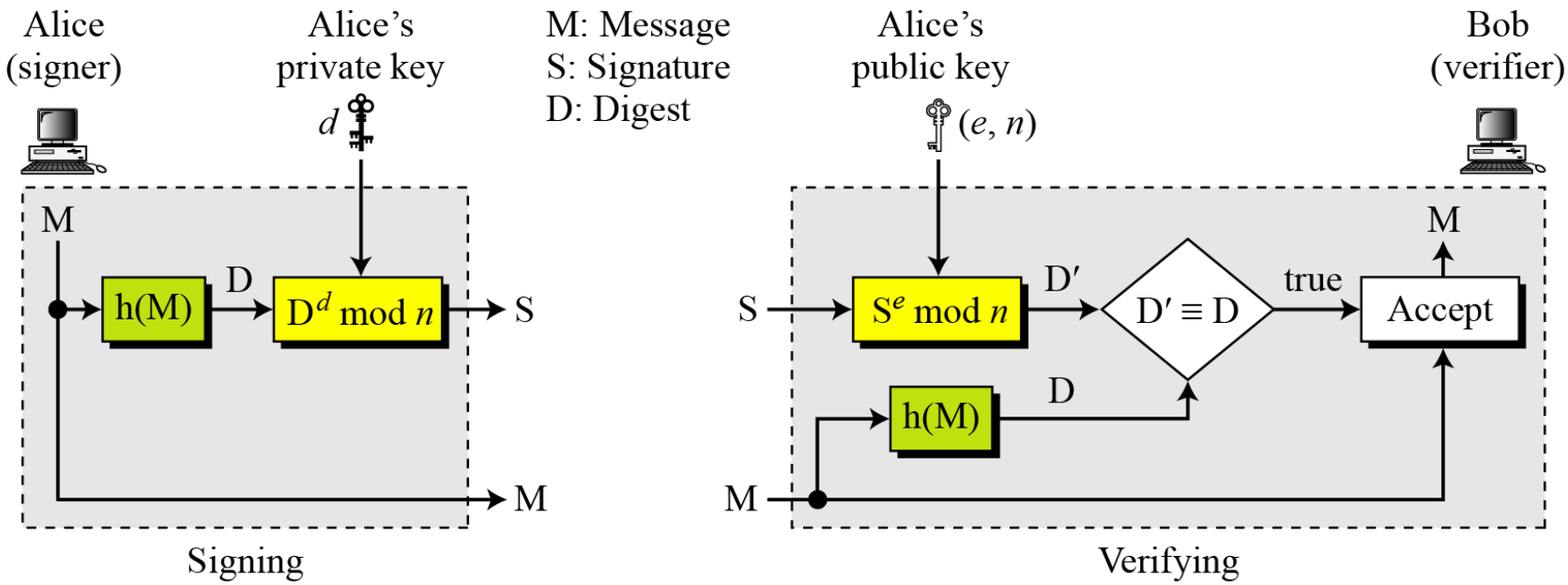
BÀI TẬP

Sử dụng cơ chế chữ ký RSA cho các bài toán sau:

1) Cho p=5, q=11, e=7. Tạo và kiểm tra chữ ký điện tử với bản tin M=5

2) Cho p=7, q=11, e=17. Tạo và kiểm tra chữ ký điện tử với bản tin M=3

Chữ ký RSA trên Message Digest



Chữ ký RSA trên Message Digest

Lưu ý:

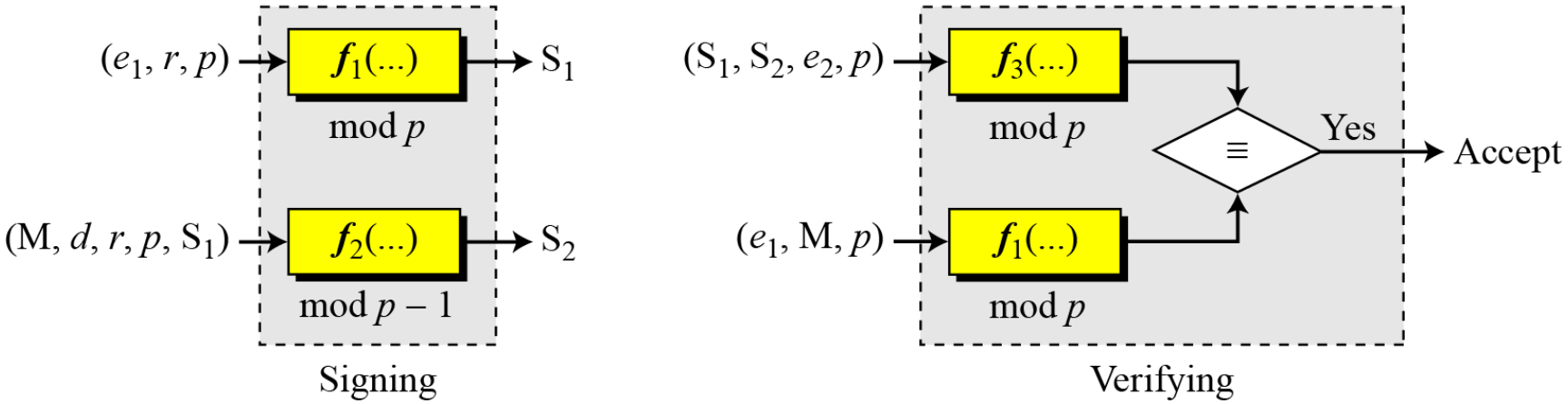
- Khi cốt thông điệp được ký thay cho thông điệp của nó, thì độ nhạy cảm của chữ ký số RSA tùy thuộc vào sức mạnh của hàm băm

ElGamal Digital Signature Scheme

- Ý tưởng tổng quát của chữ ký ElGamal

S_1, S_2: Signatures
M: Message
(e_1, e_2, p): Alice's public key

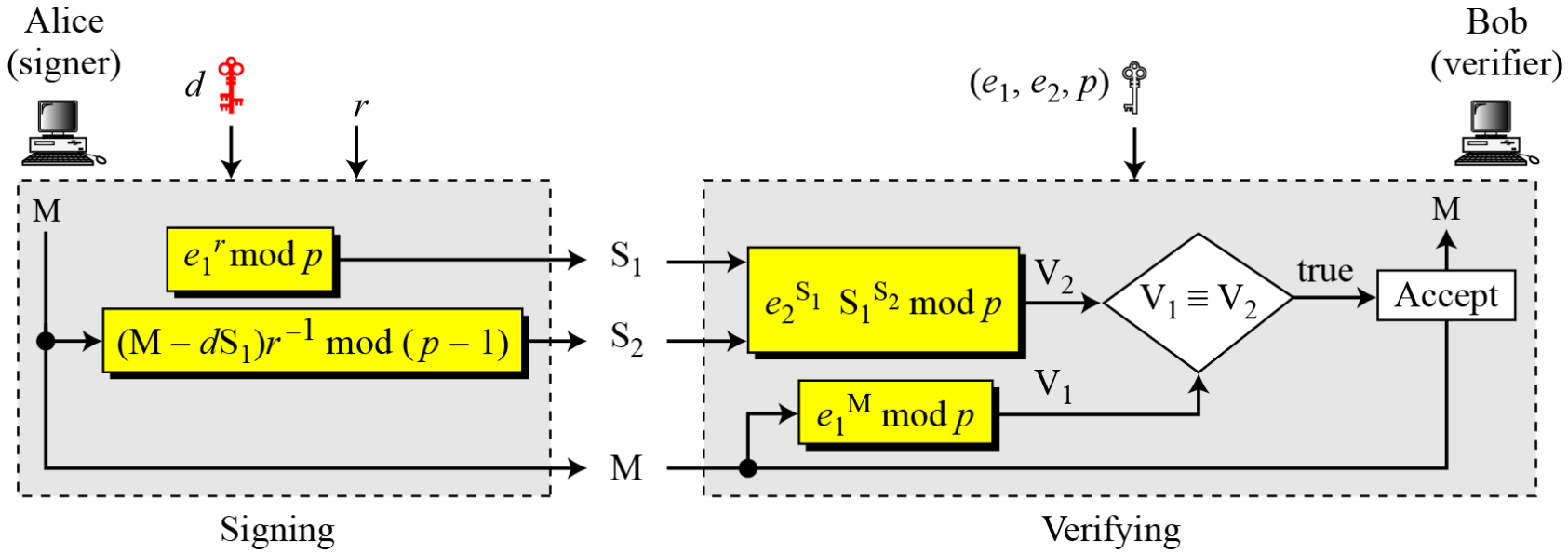
d: Alice's private key
r: Random secret



ElGamal Digital Signature Scheme

Tạo và Thẩm tra chữ ký

M: Message
S_1, S_2: Signatures
V_1, V_2: Verifications
r: Random secret
d: Alice's private key
(e_1, e_2, p): Alice's public key



ElGamal Digital Signature Scheme

Phát sinh khóa (Key Generation)

- Phát sinh khóa trong cơ chế chữ ký ElGamal là hoàn toàn giống như phát sinh khóa mật mã ElGamal
- Trong đó (e_1,e_2,p) là public key; d là private key

ElGamal Digital Signature Scheme

Tạo chữ ký

- Chọn ngẫu nhiên r, $1 \le r \le p\text{-}1$, $\gcd(r, p\text{-}1)=1$
- Tính $S_1 = e_1{}^k \bmod p$
- Tính $S_2 = (\text{M-d x } S_1) \text{ x } r^{-1} \bmod (p\text{-}1)$, với r^{-1} là nghịch đảo nhân của r modulo n
- Chữ ký là (S_1, S_2)

Thẩm tra chữ ký

- Kiểm tra $1 \le S_1 \le p$; $1 \le S_2 \le p\text{-}1$;
- Tính $v_1 = e_1{}^M \bmod p$
- Tính $v_2 = e_2{}^{S1} x\ S_1{}^{S2} \bmod p$
- Chữ ký hợp lệ $\Leftrightarrow v_1 = v_2$

ElGamal Digital Signature Scheme

Một số vấn đề

- Giá trị r phải phân biệt cho mỗi thông điệp được ký
  - $(S_1-S_2)r = (h(m_1)-h(m_2)) \bmod (p-1)$
  - Nếu $\gcd((S_1-S_2),p-1)=1$ thì có thể dễ dàng xác đinh giá trị r, từ đó có được private key a
- Nếu không dùng hàm băm thì có thể bị tình trạng existential forgery

Schnorr Digital Signature Scheme

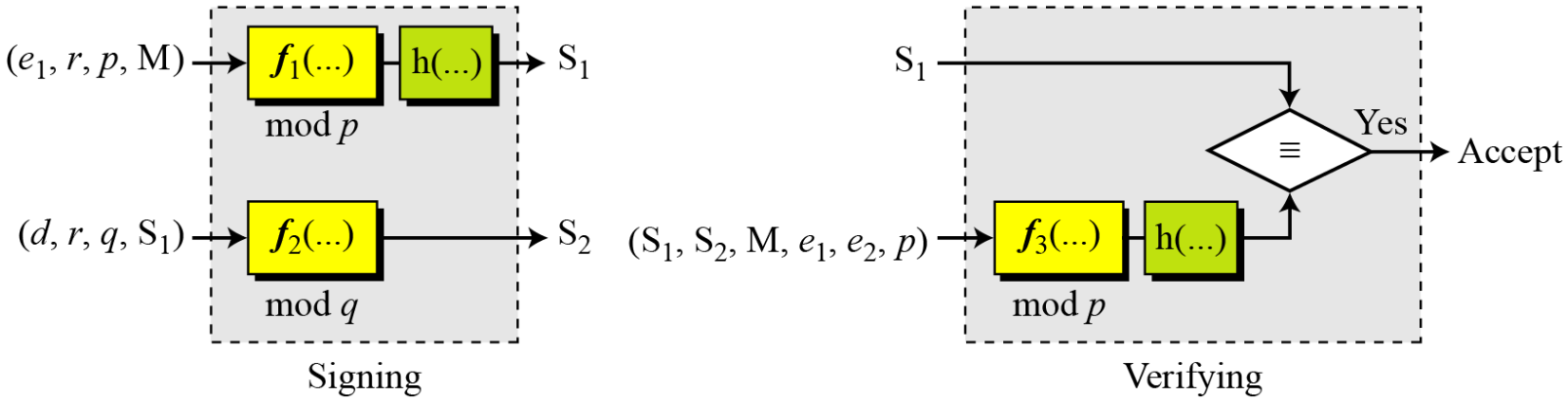
- Với chữ ký ElGamal thì p cần phải rất lớn thì mới đảm bảo bài toán logaric rời rạc là khó thực hiện trong Z^*_p. Theo khuyến cáo p phải ít nhất 1024-bit → chữ ký là 2048-bit.

- Để giảm kích cỡ của chữ ký, Schnorr đề xuất một cơ chế chữ ký mới dựa trên ElGamal nhưng với một kích cỡ chữ ký được giảm.

Schnorr Digital Signature Scheme

Ý tưởng tổng quát của chữ ký Schnorr

S_1, S_2: Signatures
M: Message
(e_1, e_2, p, q): Alice's public key
(d): Alice's private key
r: Random secret



Schnorr Digital Signature Scheme

Phát sinh khóa

1. Chọn một số nguyên tố p, thường chọn p có độ lớn 1024-bit
2. Chọn số nguyên tố q
3. Alice chọn e_1 sao cho $e_1^p = 1 \bmod p$.
4. Chọn 1 số nguyên d, làm private key
5. Tính $e_2 = e_1^d \bmod p$.
6. Public key là (e_1, e_2, p, q); private key là d

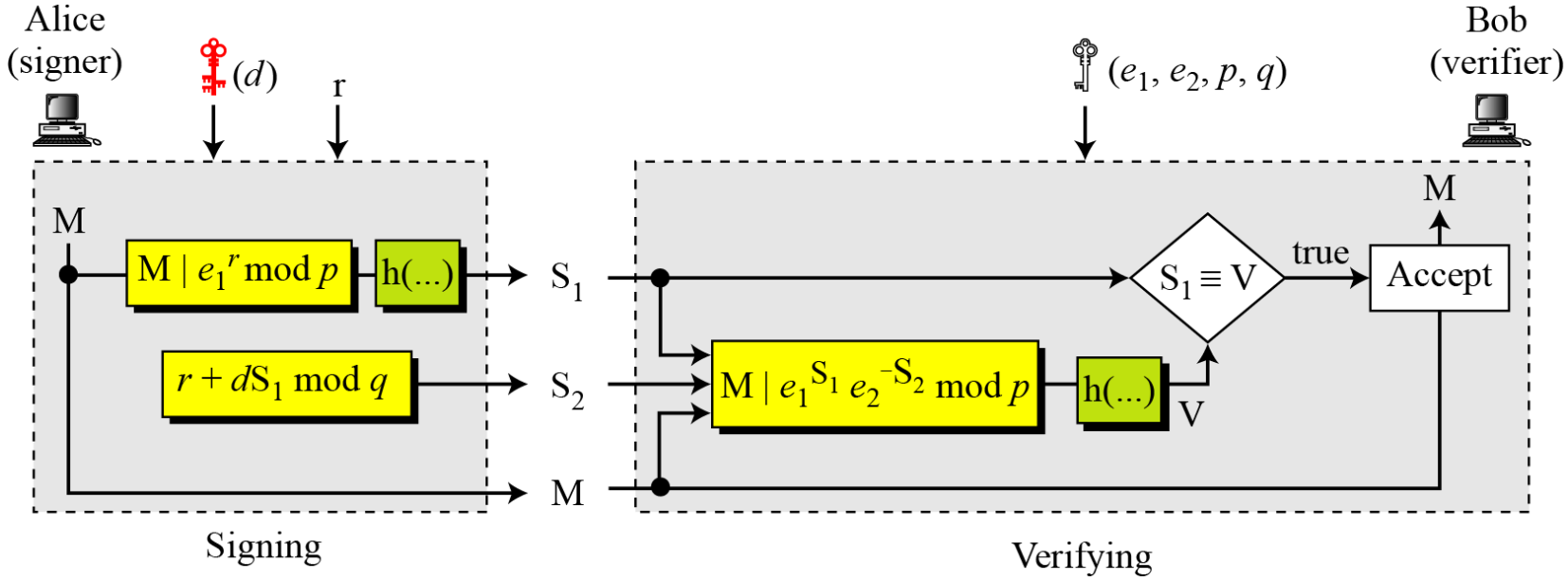
Schnorr Digital Signature Scheme

Tạo và Thẩm tra chữ ký

M: Message — r: Random secret — | : Concatenation

S_1, S_2: Signatures — (d): Alice's private key — h(...): Hash algorithm

V: Verification — (e_1, e_2, p, q): Alice's public key

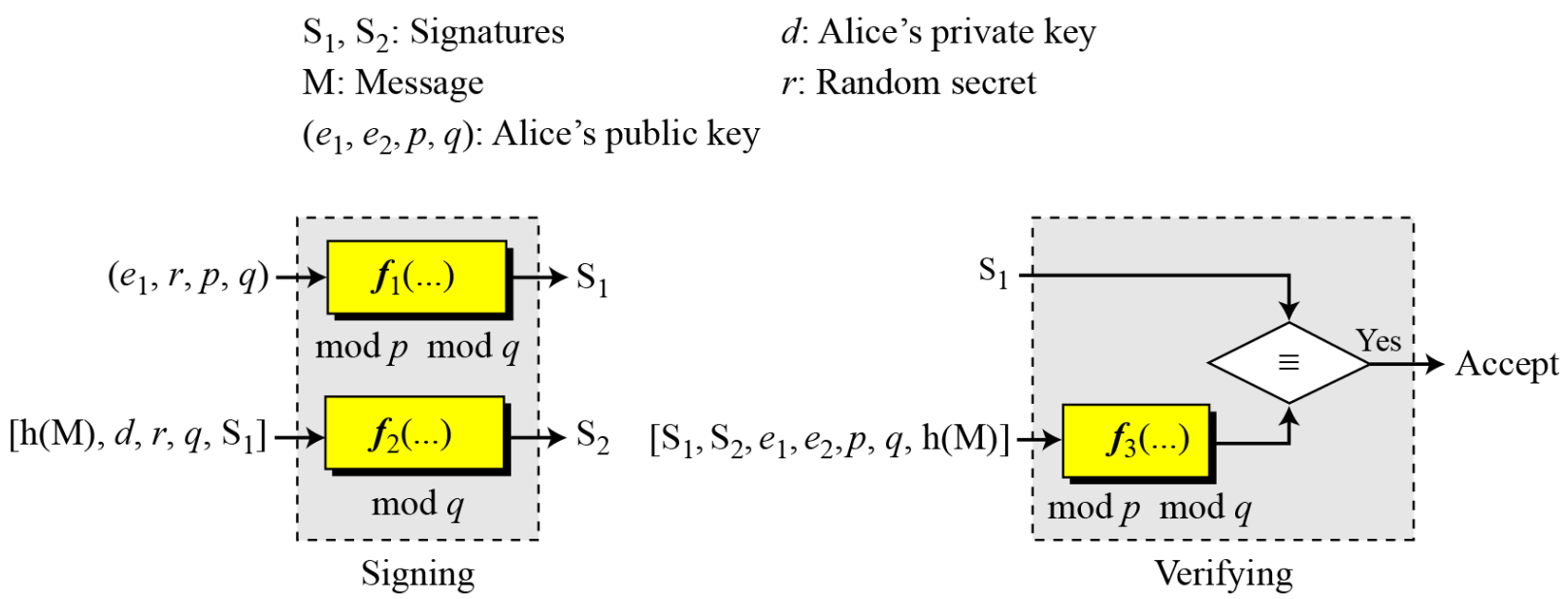


Digital Signature Standard (DSS)

- NIST đã công bố chuẩn xử lý thông tin liên ban FIPS 186, được biết như là Digital Signature Standard (DSS)
- DSS được đề xuất năm 1991 và hiểu chỉnh lại 1993, 1996 có một hiệu chỉnh nhỏ, năm 2000, một phiên bản mở rộng của chuẩn được phát hành như FIPS 186-2, 2009 cập nhật FIPS 186-3. Phiên bản cuối cùng hợp nhất các thuật tóan chữ ký số dựa trên mật mã RSA và đường cong Eliptic

Digital Signature Standard (DSS)

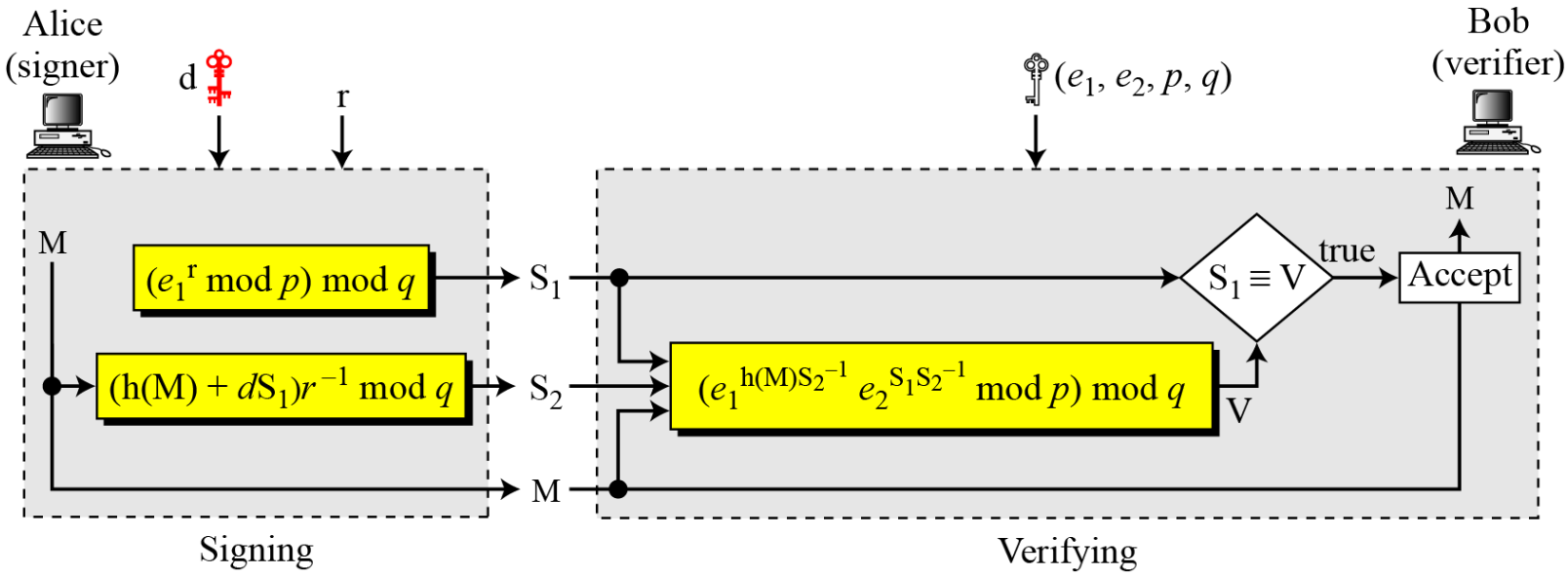
- Ý tưởng tổng quát của chữ ký DSS



Digital Signature Standard (DSS)

- **Tạo và Thẩm tra chữ ký**

M: Message
S_1, S_2: Signatures
V: Verification
r: Random secret
d: Alice's private key
(e_1, e_2, p, q): Alice's public key
h(M): Message digest



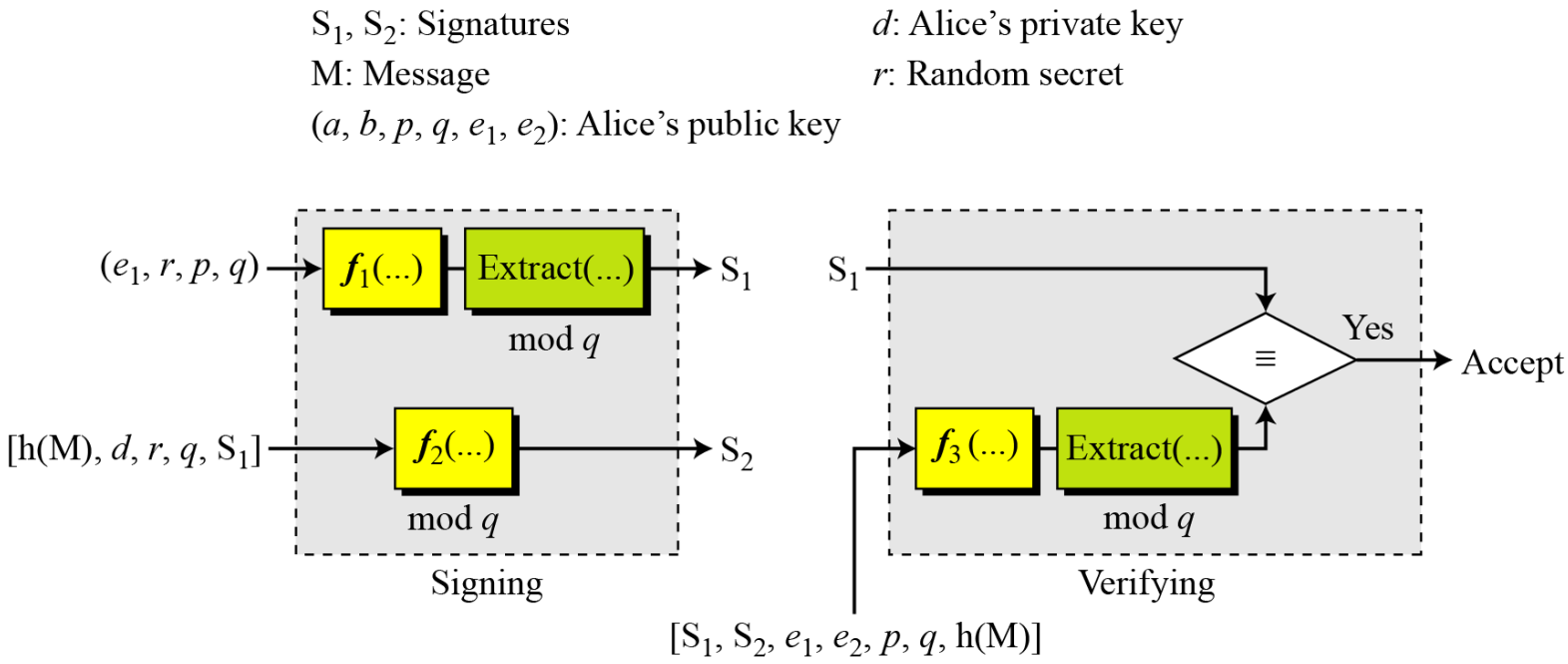
Digital Signature Standard (DSS)

Lưu ý:

- Các tính toán chữ ký DSS nhanh hơn tính toán của chữ ký RSA khi dùng cùng giá trị p
- Chữ ký DSS là nhỏ hơn chữ ký Elgamal bởi vì q nhỏ hơn p

Elliptic Curve Digital Signature Scheme

- Ý tưởng tổng quát của chữ ký EC



Elliptic Curve Digital Signature Scheme

Phát sinh khóa

- Chọn một đường cong elliptic $E_p(a, b)$.
- Chọn số nguyên tố q, chọn private key d (số nguyên)
- Chọn $e_1(\ldots, \ldots)$, một điểm trên đường cong.
- Tính $e_2(\ldots, \ldots) = d \times e_1(\ldots, \ldots)$.
- Public key là (a, b, p, q, e_1, e_2); private key là d.

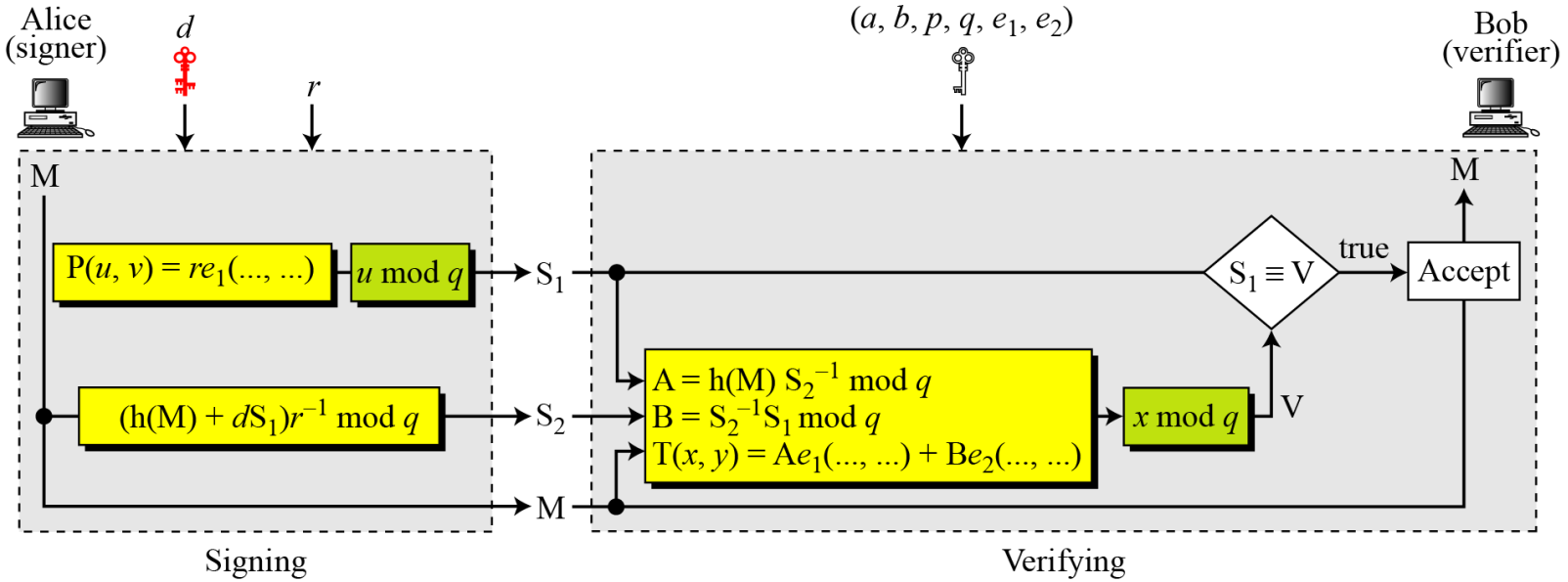
Elliptic Curve Digital Signature Scheme

Tạo và Thẩm tra chữ ký

M: Message
S_1, S_2: Signatures
V: Verification

r: Random secret
d: Alice's private key
(a, b, p, q, e_1, e_2): Alice's public key

P(u, v), T(x, y): Points on the curve
h(M): Message digest
A, B: Intermediate results



Những biến thể chữ ký

- **Time Stamped Signatures**
  - Một tài liệu được ký cần được gắn nhãn thời gian (Timestamped) để ngăn chặn tài liệu bị phát lại (replay) bởi đối phương
  - Ví dụ: Alice ký một yêu cầu đối với ngân hàng của cô ta, Bob chuyển tiền cho Eve. Tài liệu yêu cầu này có thể bị chặn và phát lại bởi Eve nếu không có nhãn thời gian gắn trên tài liệu

Những biến thể chữ ký

Blind Signatures

- Giả sử có một tài liệu mà chúng ta muốn có chữ ký mà không muốn tiết lộ nội dung của tài liệu đối với người ký.
- Ví dụ: Nhà khoa học phát minh ra một lý thuyết rất quan trọng mà cần được ký bởi công chứng viên, công chứng viên sẽ ký nhưng sẽ không biết gì về nội dung của phát minh.

Những biến thể chữ ký

Blind Signatures

- Các bước thực hiện:
  - Bob tạo một thông điệp, ẩn (Blind) nó, và gửi thông điệp ẩn này cho Alice
  - Alice ký thông điệp ẩn và trả về chữ ký trên thông điệp ẩn.
  - Bob bỏ ẩn chữ ký để thu về chữ ký trên thông điệp gốc

Ứng dụng của chữ ký số

- Chữ ký số trong các giao dịch thư điện tử, ký vào các email để các đối tác, khách hàng của bạn biết có phải bạn là người gửi thư không.
- Sử dụng dụng chữ ký số này để đầu tư chứng khoán trực tuyến, mua bán hàng trực tuyến, có thể dùng để thanh toán online, chuyển tiền trực tuyến mà không sợ bị mất cắp tiền như với đối với các tài khoản VISA, Master.
- Sử dụng với các ứng dụng chính phủ điện tử, các cơ quan nhà nước trong tương lai sẽ làm việc với nhân dân hoàn toàn trực tuyến và một cửa.
- Sử dụng để kê khai nộp thuế trực tuyến hoặc khai báo với cơ quan hải quan và tiến hành thông quan trực tuyến.

Ứng dụng của chữ ký số

- Sử dụng chữ ký số với các ứng dụng quản lý của doanh nghiệp của mình với mức độ tin cậy, bảo mật và xác thực cao hơn rất nhiều.
- Để ký hợp đồng với các đối tác làm ăn hoàn toàn trực tuyến trên mạng mà không cần gặp nhau, chỉ cần ký vào file hợp đồng và gửi qua email.
- Khoản 4, Điều 1, Luật số 21/2012/QH 13 ban hành ngày 20 tháng 11 năm 2012 sửa đổi, bổ sung một số điều của Luật quản lý thuế thì nghĩa vụ của người nộp thuế có bổ sung như sau: “Nếu người nộp thuế là tổ chức kinh doanh tại địa bàn có cơ sở hạ tầng về công nghệ thông tin phải thực hiện kê khai, nộp thuế, giao dịch với cơ quan quản lý thuế thông qua phương tiện điện tử theo quy định của pháp luật về giao dịch điện tử.

Lợi ích của chữ ký số

- **Tiết kiệm được thời gian và chi phí** trong quá trình hoạt động giao dịch điện tử.
- **Linh hoạt trong cách thức** ký kết các văn bản hợp đồng, buôn bán,… có thể diễn ra ở bất kỳ nơi đâu, ở bất kỳ thời gian nào.
- **Đơn giản hóa quy trình chuyển**, gửi tài liệu, hồ sơ cho đối tác khách hàng, cơ quan tổ chức.
- **Bảo mật danh tính của cá nhân**, doanh nghiệp an toàn.
- **Thuận lợi trong việc nộp hồ sơ thuế**, kê khai thuế cho doanh nghiệp khi chỉ cần sử dụng **chữ ký điện tử** thực hiện các giao dịch điện tử là có thể hoàn thành xong các quá trình đó.
- **Bảo mật danh tính của cá nhân**, doanh nghiệp một cách an toàn.

Giá trị pháp lý của chữ ký điện tử

- Phương pháp tạo **chữ ký điện tử** cho phép xác minh được người ký và chứng tỏ được sự chấp thuận của người ký đối với nội dung thông điệp dữ liệu.
- Phương pháp tạo chữ ký phải đủ tin cậy và phù hợp với mục đích mà theo đó thông điệp dữ liệu được tạo ra và gửi đi.
- Trong trường hợp pháp luật quy định văn bản cần được đóng dấu của cơ quan, tổ chức thì yêu cầu đó đối với một thông điệp dữ liệu được xem là đáp ứng nếu thông điệp dữ liệu đó được ký bởi **chữ ký điện tử** của cơ quan, tổ chức đáp ứng các điều kiện quy định tại khoản 1 Điều 22 của Luật Giao dịch Điện tử và **chữ ký điện tử** đó có chứng thực.

Giá trị pháp lý của chữ ký số

- Chữ ký số được tạo ra khi chứng thư số có hiệu lực và có thể kiểm tra được bằng khoá công khai ghi trên chứng thư số có hiệu lực đó.
- Chữ ký số được tạo ra bằng khoá bí mật tương ứng với khoá công khai ghi trên chứng thư số do tổ chức có thẩm quyền cấp.
- Khóa bí mật chỉ thuộc sự kiểm soát của người ký tại thời điểm ký.
- Khóa bí mật và nội dung thông điệp dữ liệu chỉ gắn duy nhất với người ký khi người đó ký số thông điệp dữ liệu.

Sử dụng chữ ký số

- Quá trình sử dụng chữ ký số có hai giai đoạn: Tạo chữ ký (sử dụng khóa bí mật để ký số) và kiểm tra chữ ký (kiểm tra khóa công khai có hợp lệ hay không).
- Để sử dụng chữ ký số cần phải đăng ký chứng thư số và tạo khóa bí mật lưu vào trong PKI Token với các nhà cung cấp dịch vụ chứng thực chữ ký số. Các chương trình ứng dụng phải hỗ trợ chức năng ký số, khi đó việc sử dụng khá đơn giản, người ký chỉ cần cắm thiết bị Token vào cổng USB, nhập PIN code bảo vệ Token và nhắp chuột vào nút lệnh ký số trong chương trình ứng dụng.

Sử dụng chữ ký số

- Chữ ký số không giống như chữ ký bình thường ở chỗ mỗi lần ký, người sử dụng sẽ dùng khóa bí mật để tạo chữ ký và mỗi lần ký sẽ là một chữ ký khác nhau. Dựa vào các công cụ phần mềm được cung cấp, các đối tác có thể kiểm tra chứng thư để xác định chữ ký.
- Cách kiểm tra là so sánh tính đồng nhất của khóa công khai trên các chữ ký số của người gửi với khóa công khai của Trung tâm Chứng thực chữ ký số quốc gia (Root Certification Authority - Root CA) thuộc Bộ Thông tin - Truyền thông.

Các nhà cung cấp chữ ký số

- Hiện nay có 5 nhà cung cấp dịch vụ chứng thực chữ ký số công cộng là VNPT/VDC, Viettel, Bkis, Nacencomm và FPT.
- Các đơn vị này đã đưa ra thị trường đầy đủ các loại chữ ký số phục vụ kê khai thuế qua mạng, giao dịch ngân hàng, chứng khoán, hải quan điện tử, ký và mã hóa email, văn bản... đáp ứng cho các đối tượng cá nhân, tổ chức, doanh nghiệp và các trang web.
- Thủ tục đăng ký tương tự như đăng ký các dịch vụ viễn thông, tuy nhiên do đặc thù pháp lý của chữ ký số, tương đương với chữ ký tay, nên có thể phải cần thêm một số giấy tờ xác thực nguồn gốc thông tin của doanh nghiệp hay người sử dụng cá nhân chặt chẽ hơn (ví dụ bản sao giấy tờ có công chứng của doanh nghiệp...).

ĐĂNG KÝ DỊCH VỤ CHỮ KÝ SỐ NCCA

NC CA – gói 4 năm: ~~3.080.000đ~~ Giảm chỉ còn: 1.600.000đ

- Miễn phí USB Chữ ký số
- Tặng phần mềm kế toán Fast
- Bàn giao, cài đặt tận nơi
- Hỗ trợ chữ ký số 24/7.
- Tư vấn, hỗ trợ kê khai thuế

ĐĂNG KÝ DỊCH VỤ CHỮ KÝ SỐ EFY-CA

EFY Ca – gói 3 năm: ~~3.080.000đ~~ Giảm chỉ còn: 1.600.000đ

- Miễn phí USB Chữ ký số
- Tặng phần mềm kế toán Misa
- Bàn giao, cài đặt tận nơi
- Hỗ trợ chữ ký số 24/7.
- Tư vấn, hỗ trợ kê khai thuế

ĐĂNG KÝ DỊCH VỤ CHỮ KÝ SỐ VNPT CA

VNPT Ca – gói 4 năm: ~~3.080.000đ~~ Giảm chỉ còn: 2.000.000đ

- Miễn phí USB Chữ ký số
- Tặng phần mềm kế toán Misa
- Bàn giao, cài đặt tận nơi
- Hỗ trợ chữ ký số 24/7.
- Tư vấn, hỗ trợ kê khai thuế

ĐĂNG KÝ DỊCH VỤ CHỮ KÝ SỐ FPT CA

FPT Ca – gói 3 năm: ~~3.107.000đ~~ Giảm chỉ còn: 1.890.000đ

- Miễn phí USB Chữ ký số;
- Tặng phần mềm kế toán Misa
- Bàn giao, cài đặt tận nơi
- Hỗ trợ chữ ký số 24/24
- Nộp môn bài, thuế quý miễn

BẢNG GIÁ ĐĂNG KÝ DỊCH VỤ CHỮ KÝ SỐ VINA CA

Vina Ca – gói 3 năm: ~~3.108.000đ~~ Giảm chỉ còn: 2.000.000đ

- Miễn phí USB Chữ ký số;
- Tặng phần mềm kế toán Misa
- Bàn giao, cài đặt tận nơi
- Hỗ trợ chữ ký số 24/24
- Tư vấn, hỗ trợ kê khai thuế

BẢNG GIÁ ĐĂNG KÝ DỊCH VỤ CHỮ KÝ SỐ NEW CA

New Ca – gói 3 năm: ~~3.109.000đ~~ Giảm chỉ còn: 1.500.000đ

- Miễn phí USB Chữ ký số;
- Tặng phần mềm kế toán Misa
- Bàn giao, cài đặt tận nơi
- Hỗ trợ chữ ký số 24/24
- Tư vấn, hỗ trợ kê khai thuế

Chứng thư số

- Là một **văn bản cung cấp khóa công khai**
- được cung cấp bởi một tổ chức gọi là **tổ chức cung cấp dịch vụ chứng thư số** (certificate authority, hay viết tắt là CA).
- Chứng thư số hoạt động nhờ vào nguyên lý **bên thứ ba tin cậy** (trusted third party – TTP), ở đây bên thứ ba chính là CA. Thông thường, 2 bên giao tiếp với nhau không tin nhau, tuy nhiên, nếu họ cùng tin vào một bên thứ ba (TTP), và bên thứ ba đã xác thực 2 bên này, thì 2 bên này sẽ tin tưởng lẫn nhau.

Chứng thư số

- "Chứng thư số" là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp nhằm cung cấp thông tin định danh cho khóa công khai của một cơ quan, tổ chức, cá nhân, từ đó xác nhận cơ quan, tổ chức, cá nhân là người ký chữ ký số bằng việc sử dụng khóa bí mật tương ứng (theo Khoản 7, Điều 3, Nghị định 130/2018/NĐ-CP)

Nội dung của chứng thư số theo chuẩn X.509

Tiêu chuẩn về *Chứng thư số* dựa trên cơ sở hạ tầng *khóa công khai* phổ biến nhất hiện này là X.509 được ban hành bởi ITU-T (International Telegraph Union - Telecom, Tổ chức viễn thông quốc tế (về lĩnh vực viễn thông), thuộc Liên hợp quốc).

Những nội dung thông tin cơ bản theo chuẩn X.509

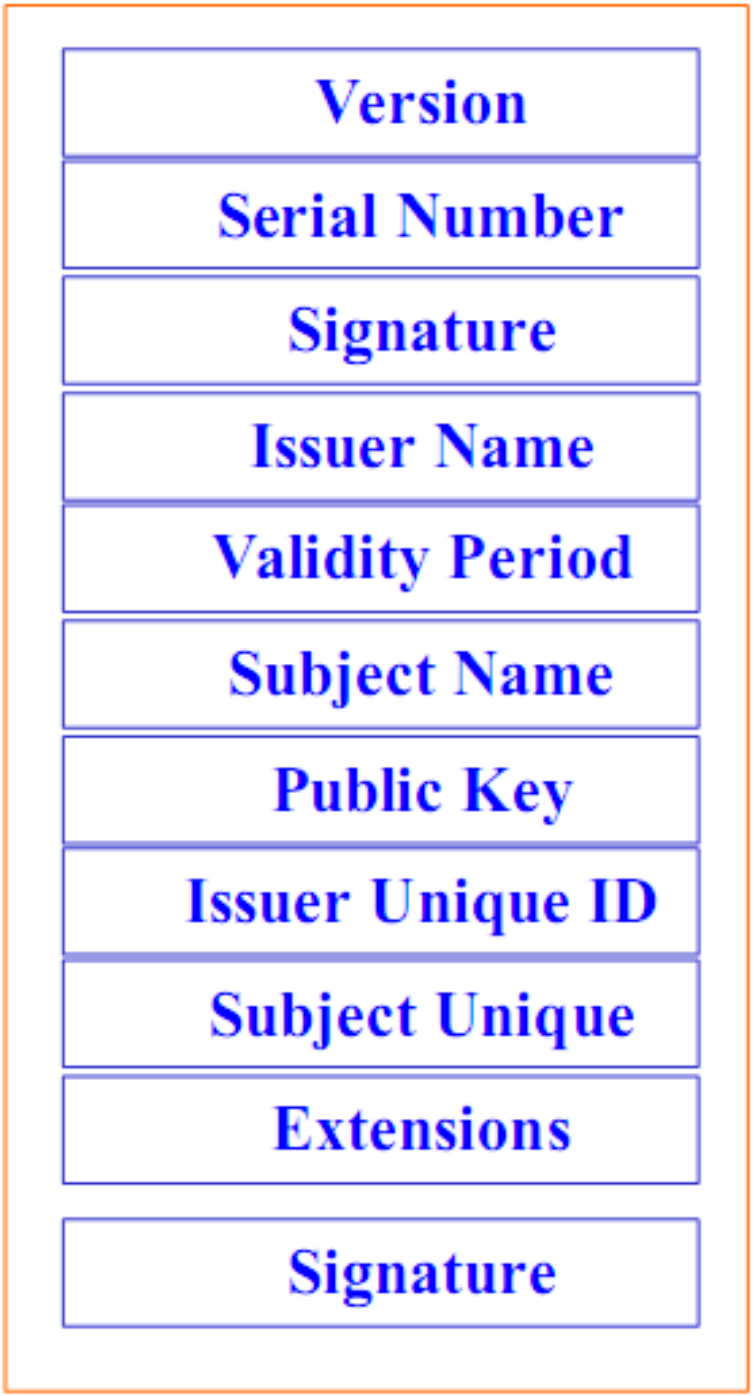
Version: Chỉ định phiên bản của chứng nhận X.509.

Serial Number: Số loạt phát hành được gán bởi CA. Mỗi CA nên gán một mã số loạt 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).

Issuer Name: Tên tổ chức CA phát hành chứng thực.(Theo chuẩn X.500 thì gọi là Tên phân biệt - X.500 Distinguised Name, X.500 DN). Hai CA khác nhau không được sử dụng cùng một tên phát hành.

Validity Period: gồm hai giá trị chỉ định khoảng



thời gian mà giấy chứng nhận có hiệu lực: not-before và not-after.

Not-before: *thời gian chứng nhận bắt đầu có hiệu lực;*

Not-after: *thời gian chứng nhận hết hiệu lực.*

Các giá trị thời gian này được đo theo chuẩn thời gian Quốc tế, chính xác đến từng giây.

Subject Name: *Tên chủ thể được cấp chứng thực.*

Public Key: *Chìa khoá công khai của chủ thể được cấp chứng thực.*

Issuer Unique ID&Subject Unique ID: *Được đưa vào sử dụng từ X.509 phiên bản 2, 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. (Mới được đưa ra trong X.509 phiên bản 3).*

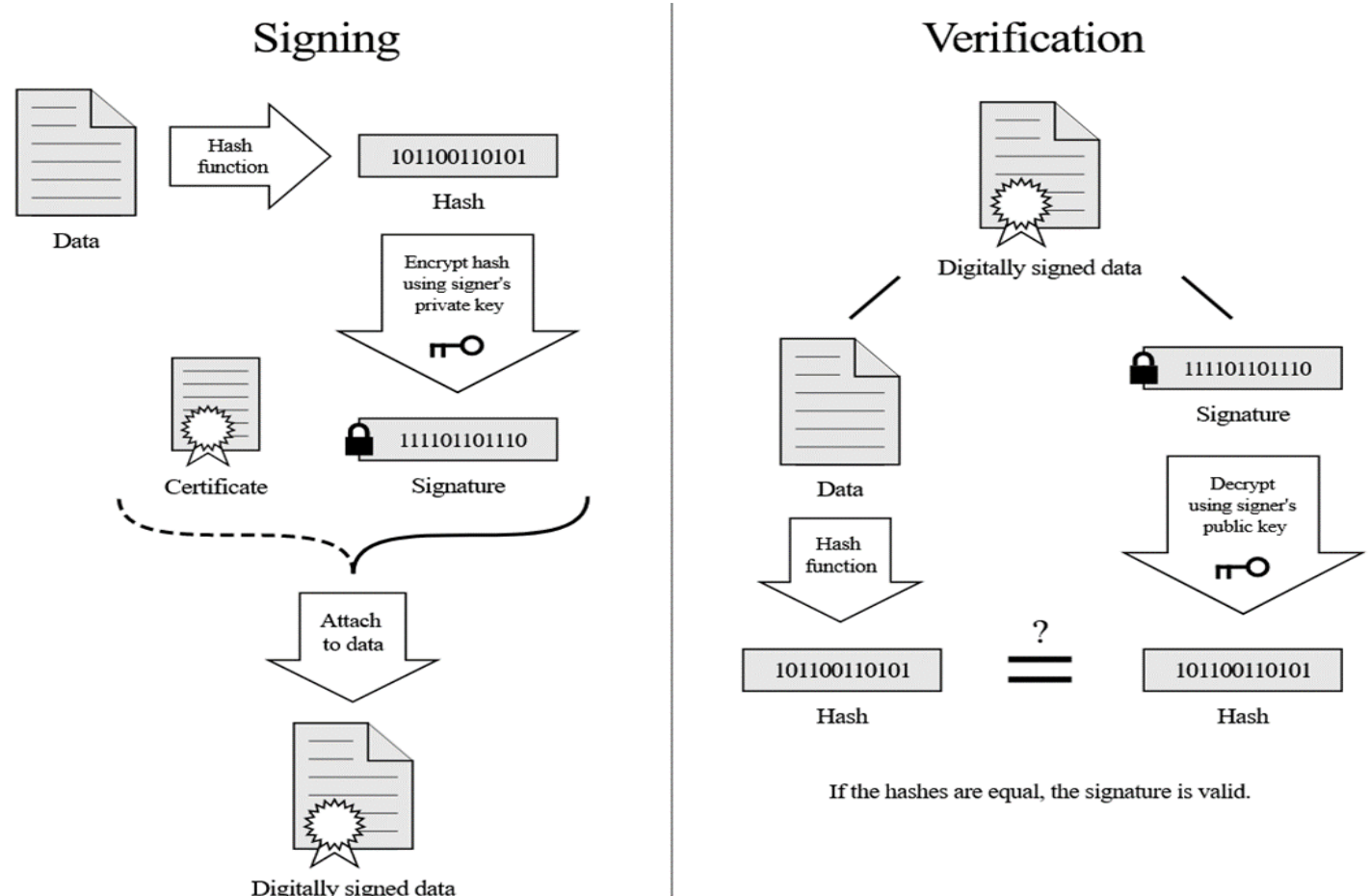
Signature: *chữ ký số được tổ chức CA áp dụng.*

Tổ chức CA tạo chữ ký bằng khóa bí mật với kiểu thuật toán mã được quy định trong trường thuật toán chữ ký.

Chữ ký bao gồm tất cả các phần khác trong giấy chứng nhận. (Qua đó thể hiện CA chứng nhận cho tất cả các thông tin khác trong giấy chứng thực, chứ không chỉ cho tên chủ thể và khóa công khai).

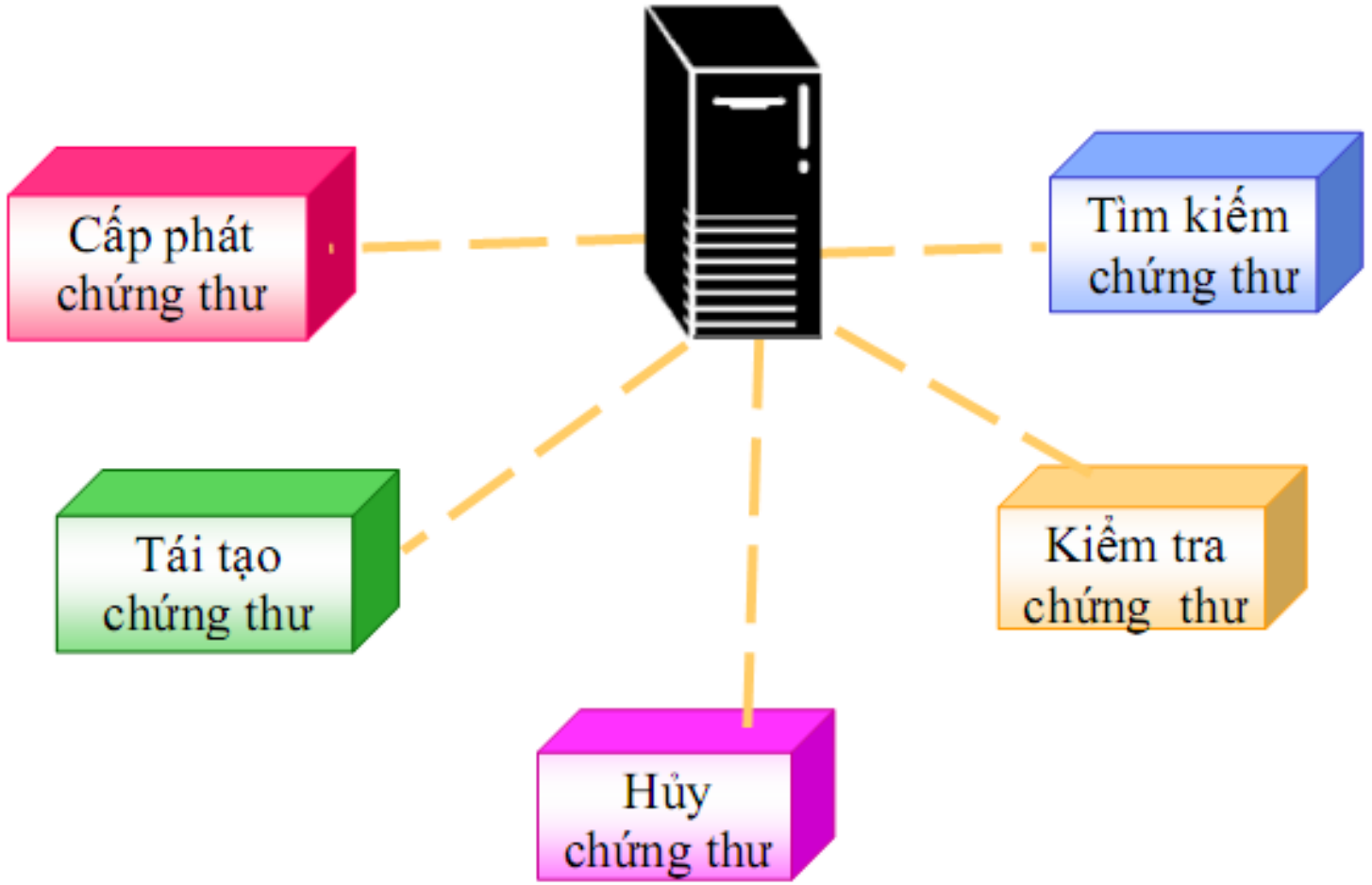
Chứng thư số

Chữ ký với chứng thư số

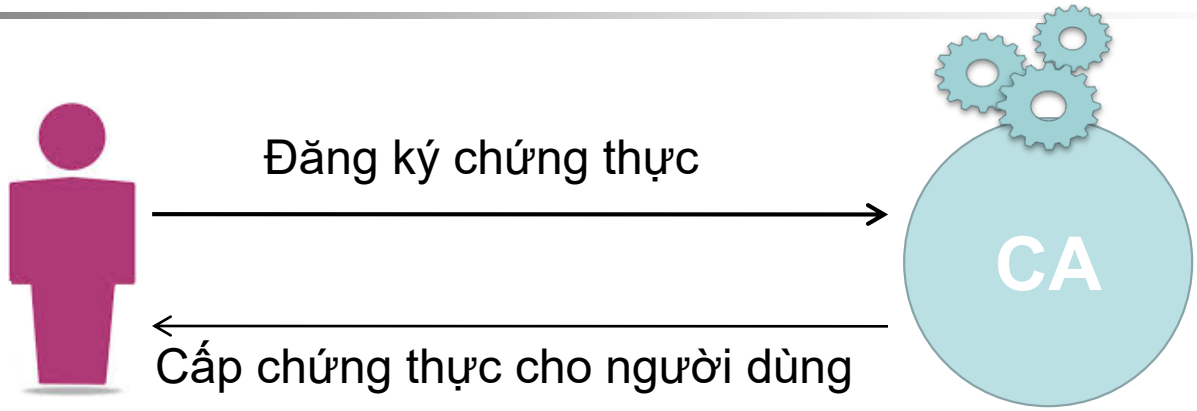


Cơ quan thẩm quyền phát hành chứng thư số (CA)

Các chức năng cơ bản

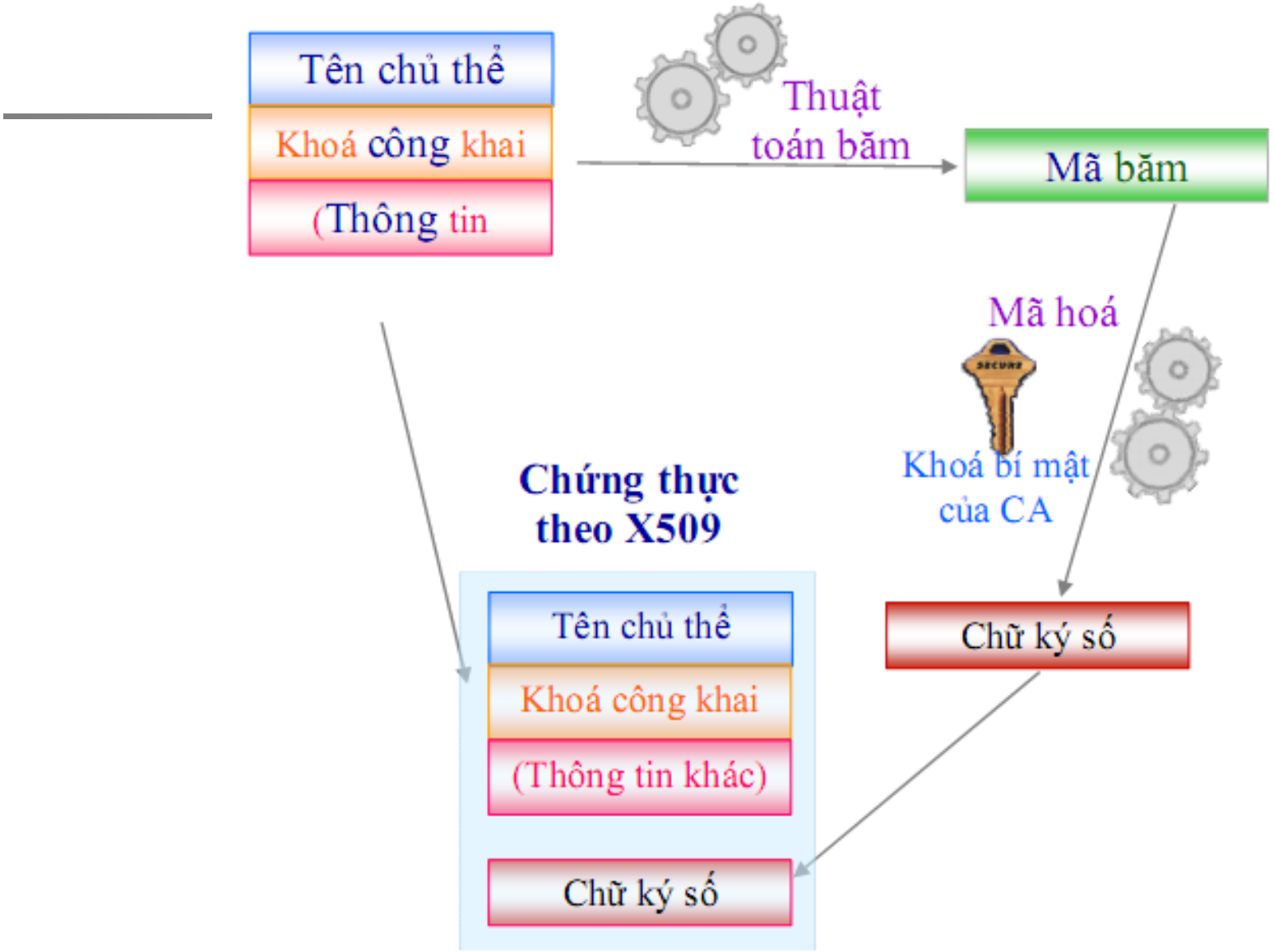


Cấp phát chứng thư số

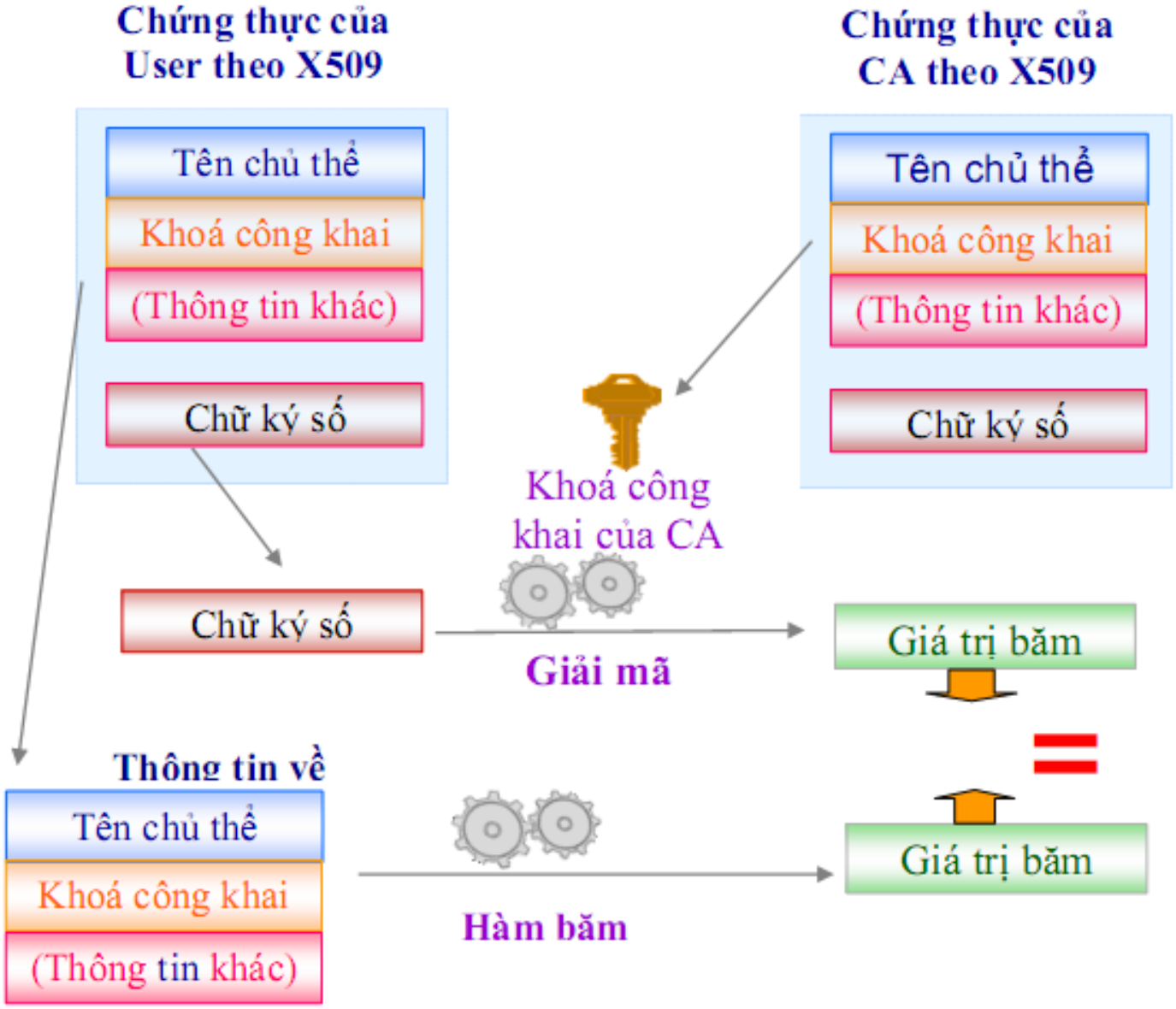


- Sinh cặp chìa khóa bất đối xứng an toàn
- Tránh xung đột chứng thực
- Hoặc tránh định danh giống nhau

Sơ đồ tạo chứng thư số



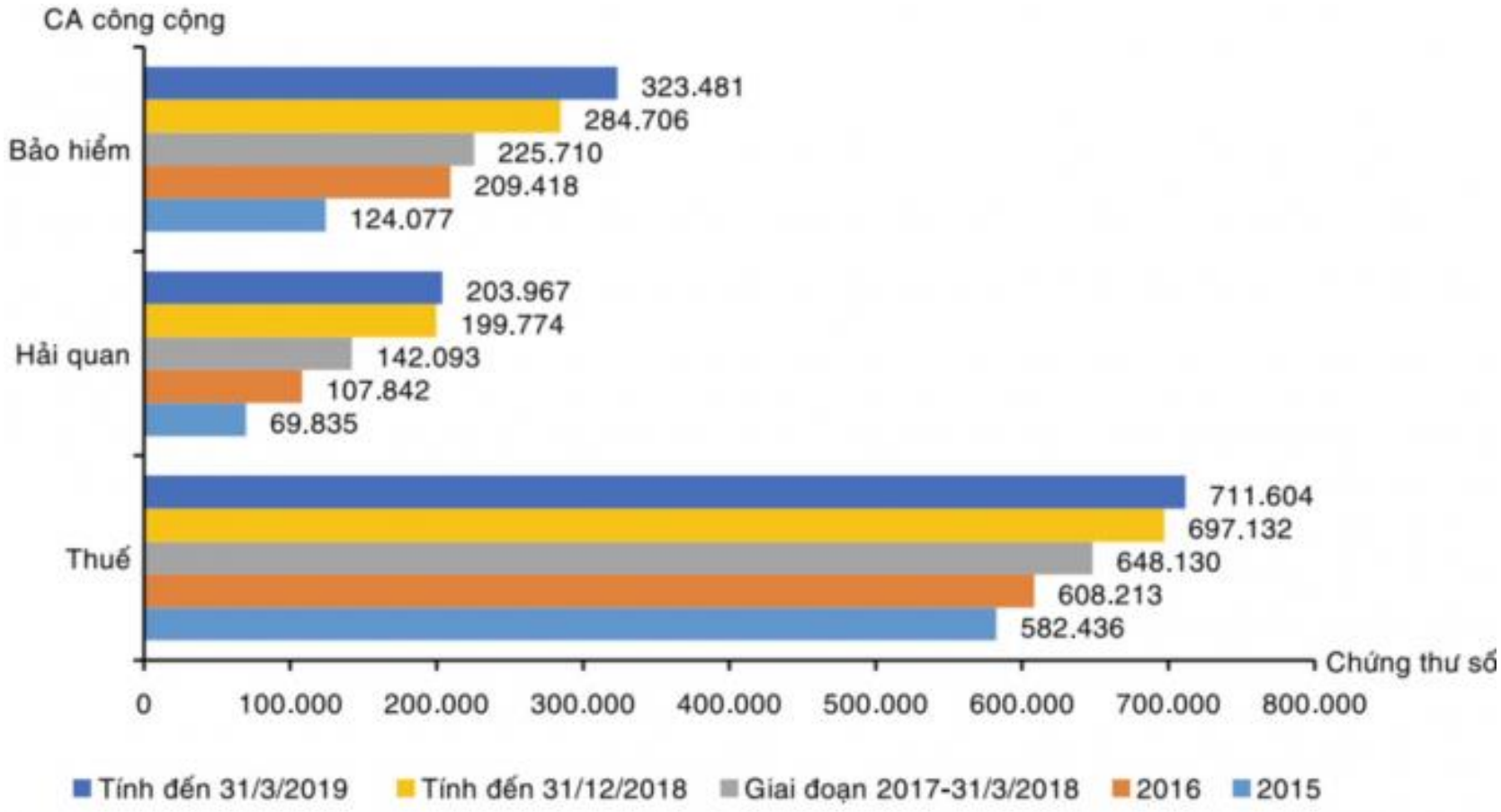
Sơ đồ kiểm tra chứng thư số



Ứng dụng của chứng thư số

- Sử dụng nhiều trong các hoạt động giao dịch thương mại điện tử, đặc biệt trong thanh toán trực tuyến của ngân hàng.
- Chứng thực số sẽ giúp ngân hàng đảm bảo các khách hàng không thể chối bỏ các giao dịch của mình.
- Chứng thư số hiện còn được sử dụng như một dạng của chứng minh thư nhân dân. Tại các nước phát triển, chứng thư số (CA) được tích hợp vào các con chíp nhớ nằm trong thẻ tín dụng để tăng khả năng bảo mật, chống giả mạo, cho phép chủ thẻ xác minh danh tính của mình trên các hệ thống khác nhau như xe bus, thẻ rút tiền ATM, hộ chiếu điện tử tại các cửa khẩu, kiểm soát hải quan …

Tình hình sử dụng chữ ký số - Việt Nam



Tình hình sử dụng chữ ký số - Việt Nam

- Đối với lĩnh vực chứng khoán, tính đến 31/3/2019, Ủy ban Chứng khoán Nhà nước đã cung cấp 133 dịch vụ công trực tuyến ứng dụng chữ ký số để xác thực, trong đó có 13 dịch vụ công mức độ 4.
- Ủy ban Chứng khoán Nhà nước sử dụng chữ ký số trong các hệ thống như: Hệ thống giám sát giao dịch chứng khoán, Phần mềm quản lý báo cáo thống kê nội bộ; hệ thống cơ sở dữ liệu quản lý công ty quản lý quỹ và quỹ đầu tư; hệ thống cơ sở dữ liệu quản lý công ty chứng khoán; hệ thống cơ sở dữ liệu quản lý nhà đầu tư nước ngoài; Hệ thống công bố thông tin

Tình hình sử dụng chữ ký số - Việt Nam

Ứng dụng chữ ký số trong lĩnh vực quân sự, quốc phòng

- Cục Cơ yếu (Bộ Tổng Tham mưu) chịu trách nhiệm bảo đảm chứng thư số, cung cấp dịch vụ xác thực "Chữ ký số" chuyên dùng Chính phủ cho các tổ chức và cá nhân trong Bộ Quốc phòng.
- Đến tháng 3/2021, Cục Cơ yếu đã cấp hơn 130 chứng thư số cho các tổ chức và hơn 1.600 chứng thư số cá nhân

Tình hình sử dụng chữ ký số - Việt Nam

Ứng dụng chữ ký số trong lĩnh vực quân sự, quốc phòng

- Các công cụ ký số cho các tệp tin, tệp văn bản định dạng PDF và thư viện tích hợp ký số trên thư điện tử, trang thông tin điện tử, ký số trên nền tảng di động cũng được ngành Cơ yếu bảo đảm cho các đơn vị.
- Các đơn vị phối hợp với Cục Cơ yếu để tích hợp sử dụng dịch vụ chữ ký số trong các hoạt động chuyên ngành, với các ứng dụng tiêu biểu như: Phần mềm Hệ thống Quản lý văn bản và hồ sơ công việc mới của Bộ Quốc phòng; Hệ thống Biên phòng điện tử; Hệ thống Phòng họp không giấy tờ tại Tổng cục Hậu cần; Phần mềm Quản lý hồ sơ khám chữa bệnh của Bệnh viện Quân y 105 (Tổng cục Hậu cần); Phần mềm Quản lý ngành Xe - Máy (Cục Xe - Máy, Tổng cục Kỹ thuật)... Tuy nhiên, do tính chất đặc thù trong hoạt động quân sự, quốc phòng, việc ứng dụng chữ ký số trong Bộ Quốc phòng vẫn còn những hạn chế nhất định.

Câu hỏi và bài tập

1. Những đặc tính nào mà chữ ký số nên có?
2. Những yêu cầu nào mà một chữ ký số cần phải thỏa mãn?
3. Thực hành
4. Ví dụ
5. Xác thực điện tử

Câu hỏi và bài tập

1. Cho $a = 13$, $p = 20$. Tìm giá trị nghịch đảo của a trong phép *modulo p* dùng thuật toán Euclid mở rộng (xem phụ lục 2).
2. Cho $n = 17$, lập bảng tương tự như Bảng 4-1. Liệt kê các *primitive root* của n.
3. Áp dụng thuật toán bình phương liên tiếp tính 7^{21} *mod* 13
4. Cho $p = 5$, $q = 11$, $e = 7$. Tính khóa riêng (d, N) trong phương pháp RSA.
5. Thực hiện mã hóa và giải mã bằng phương pháp RSA với $p = 3$, $q = 11$, $e = 7$, $M = 5$ theo hai trường hợp mã hóa bảo mật và mã hóa chứng thực.
6. Alice chọn $p = 7$, $q = 11$, $e = 17$, Bob chọn $p = 11$, $q = 13$, $e = 11$:
   a. Tính khóa riêng K_{RA} của Alice và K_{RB} của Bob
   b. Alice muốn gởi cho Bob bản tin $M = 9$ vừa áp dụng chứng thực và bảo mật như ở sơ đồ 4-3. Hãy thực hiện quá trình mã hóa và giải mã.
7. Xét thuật toán Miller-Rabin (xem phụ lục 2). Với số 37, cho biết kết quả của thuật toán Miller-Rabin trong các trường hợp sau đây của a: 9, 17, 28.
8. Dùng thuật toán Miller-Rabin, kiểm tra tính nguyên tố của số 169.

Câu hỏi và bài tập

1. Những đặc tính nào mà chữ ký số nên có?
2. Những yêu cầu nào mà một chữ ký số cần phải thỏa mãn?

THANKS YOU