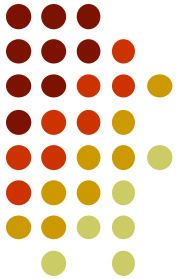


CHƯƠNG 5:
CHỮ KÝ SỐ VÀ HÀM BĂM

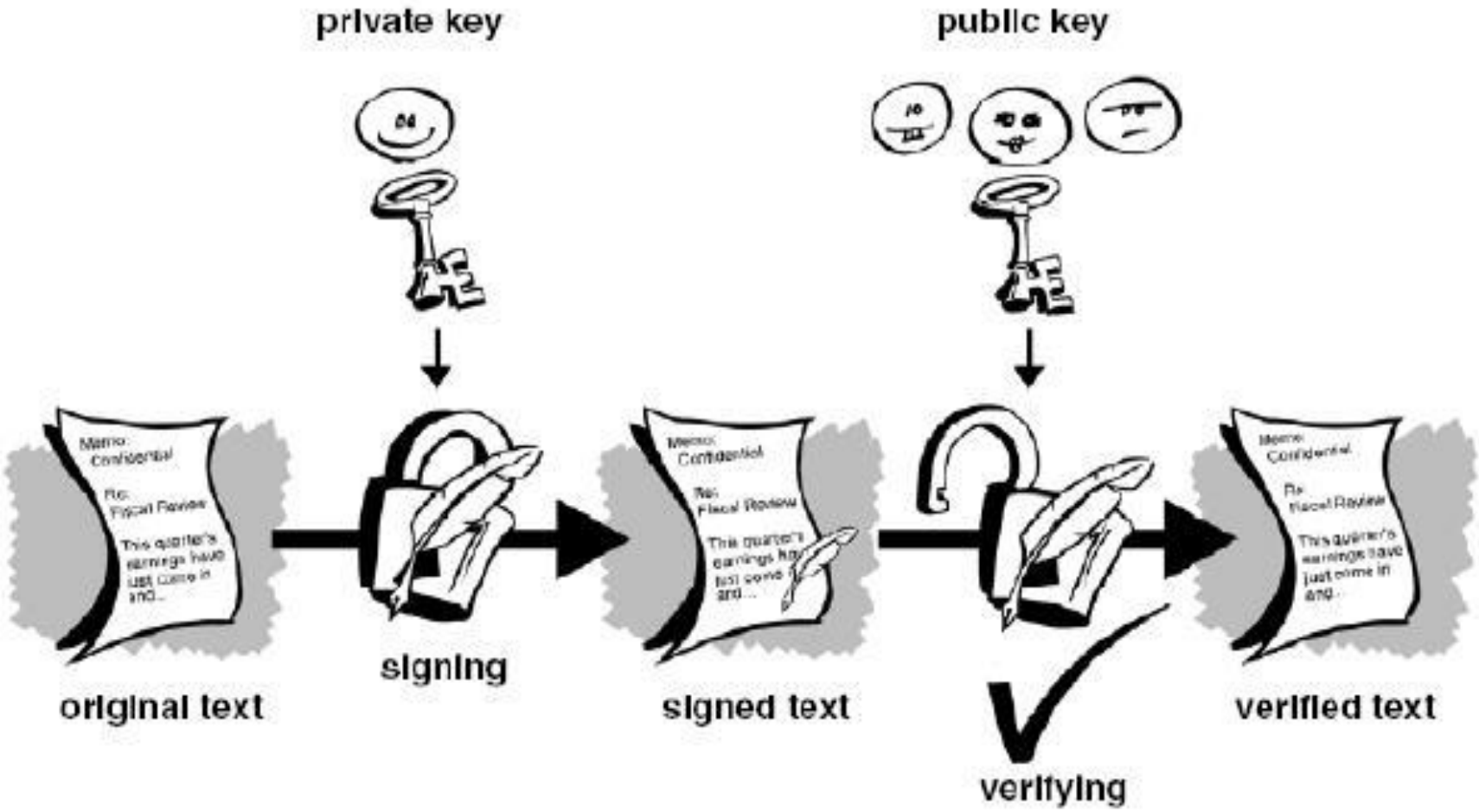
Chương 5:
Chữ ký số và hàm băm

Chữ ký số là gì?

- Một dạng chữ ký điện tử
- Dựa trên công nghệ khóa công khai (PKI)
- Mỗi người cần 1 cặp khóa gồm khóa công khai & khóa bí mật.

Khóa bí mật dùng để tạo chữ ký số (CKS)

Khóa công khai dùng để thẩm định CKS -> xác thực

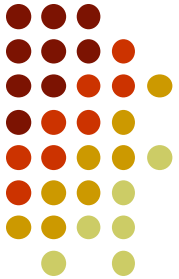


Ở chữ ký số, **người ký là người tạo ra khóa**:

-Giữ khóa bí mật để ký

-Cung cấp các khóa công khai để mọi người có thể xác thực chữ ký

Chương 5:
Chữ ký số và hàm băm



Thẩm định chữ ký số có ý nghĩa:

- Quá trình thẩm định là quá trình xác thực
- Kết quả
  - Xác thực được người gửi
  - Chống chối bỏ
  - Xác thực toàn vẹn thông tin

Sơ đồ chữ ký

Một *sơ đồ chữ ký S* là một bộ năm: $<M, S, \mathcal{K}, S_A, V_A>$

trong đó:

M là một tập hữu hạn các thông báo có thể có,

S là một tập hữu hạn các chữ ký có thể có,

$\mathcal{K}$ là một tập hữu hạn các khoá,

mỗi khoá $K \in \mathcal{K}$ gồm có hai phần $K=(K',K'')$, K' là khoá bí mật – để ký, còn K'' là khoá công khai - kiểm thử chữ ký.

Với mỗi $K=(K',K'')$, ta có:

+ *thuật toán ký* (trong S_A) $Sig_{K'}: M \rightarrow S$

+ *thuật toán kiểm thử* (trong V_A) $Ver_{K''}: M \times S \rightarrow \{đúng,sai\}$ thoả mãn điều kiện sau với mọi thông báo $x \in M$ và mọi chữ ký $y \in A$:

$$Ver_{K''}(x, y) = đúng \Leftrightarrow y = Sig_{K'}(x).$$

Thủ tục ký:

- Đối tượng A (người ký) tạo ra chữ ký cho văn bản m ∈ M bằng việc thực hiện các bước sau:
  - Tính $\boldsymbol{s = S_A(m)}$
  - Truyền cặp (m,s) trong đó s được gọi là chữ ký của văn bản m

Thủ tục kiểm thử:

- Việc kiểm thử chữ ký s trên văn bản m do A tạo ra, đối tượng B (người kiểm thử) sẽ thực hiện:
  - Sử dụng hàm kiểm thử V_A của A

    Tính $\boldsymbol{u = V_A(m,s)}$
  - Nếu u = True → B chấp nhận chữ ký
  - Nếu u = False → B từ chối

Chương 5:
Chữ ký số và hàm băm

Hệ chữ ký điện tử theo tiếp cận ban đầu nói trên là khá đơn giản và phạm phải nhược điểm lớn:

- **Chữ ký quá dài, dài đúng bằng tài liệu**
- **Diễn ra rất lâu, thời gian tỷ lệ với độ dài văn bản.**
- Kẻ tấn công có thể dễ dàng phá hệ thống chữ ký này bằng kiểu **tấn công lắp ghép khối** (thay đổi thứ tự, thêm hay bớt khối …)

Chương 5:
Chữ ký số và hàm băm

Giải pháp đầy đủ là có thêm sự hộ trợ của hàm băm, tức là "Băm" tài liệu trước khi ký

- Một hàm băm *H* sẽ lấy ở đầu vào một thông tin *X* có kích thước bất kỳ và sinh kết quả ra là một chuỗi *hX=h*(*X*) có độ dài cố định, thường là nhỏ hơn nhiều so với kích thước của *X*. Chuỗi này thường được gọi là cốt yếu, hay cốt (digest) của thông tin *X*.

- Ví dụ: Thông tin *X* có thể là một tệp độ dài hàng trăm Kb trong khi cốt của nó chỉ là một khối có độ dài 128bit.

Chương 5:
Chữ ký số và hàm băm

Để đảm bảm an toàn cao, chống được tấn công giả mạo chữ ký, chúng ta cần sử dụng các hàm băm mật mã có các thuộc tính như sau:

- **Lấy đầu vào là một xâu với độ dài bất kỳ và sinh ra một xâu với độ dài cố định.**
- **Có tính một chiều (one - way):** biết *X*, có thể dễ dàng tính được giá trị băm h_X nhưng không thể tính ngược được *X* khi chỉ biết h_X
- **Có tính phi đụng độ cao** (collision free), tức là thực tế không thể tìm được hai thông tin X khác X' sao cho *H*(*X*) = *H*(*X'*)

Chương 5:
Chữ ký số và hàm băm

- ***MD5 (Rivest 1992)***

  Đây là một trong các hàm băm có tiếng nhất và được sử dụng thông dụng:

  + Nó lấy vào các khối đầu vào 512 bit và sinh ra các giá trị băm 128 bit.

  + Được tin là phi đụng độ và one-way

  + Thuật toán MD5 được thiết kế cho phép chạy tốt nhất trên các máy tính 32 bit. Nó sử dụng các phép toán đơn giản như phép cộng modulo 32, do đó thích hợp với việc mã hoá cho các bộ xử lý 32 bit.

Chương 5:
Chữ ký số và hàm băm

SHA (Secure Hash Function)

Đây là một thuật toán được đề xuất và bảo trợ bởi cơ quan NIST để sử dụng đối với hệ chữ ký DSA (cũng là một dự chuẩn cho chữ ký điện tử). Nó cho giá trị băm là 160 bit và được thiết kế với cùng một tiếp cận như MD5.

HAVAL

Một hệ băm của Australia cho phép thay đổi kích thước giá trị băm. Cấu trúc rất giống như MD5.

Chương 5:
Chữ ký số và hàm băm

Snefru Mekle (1989)

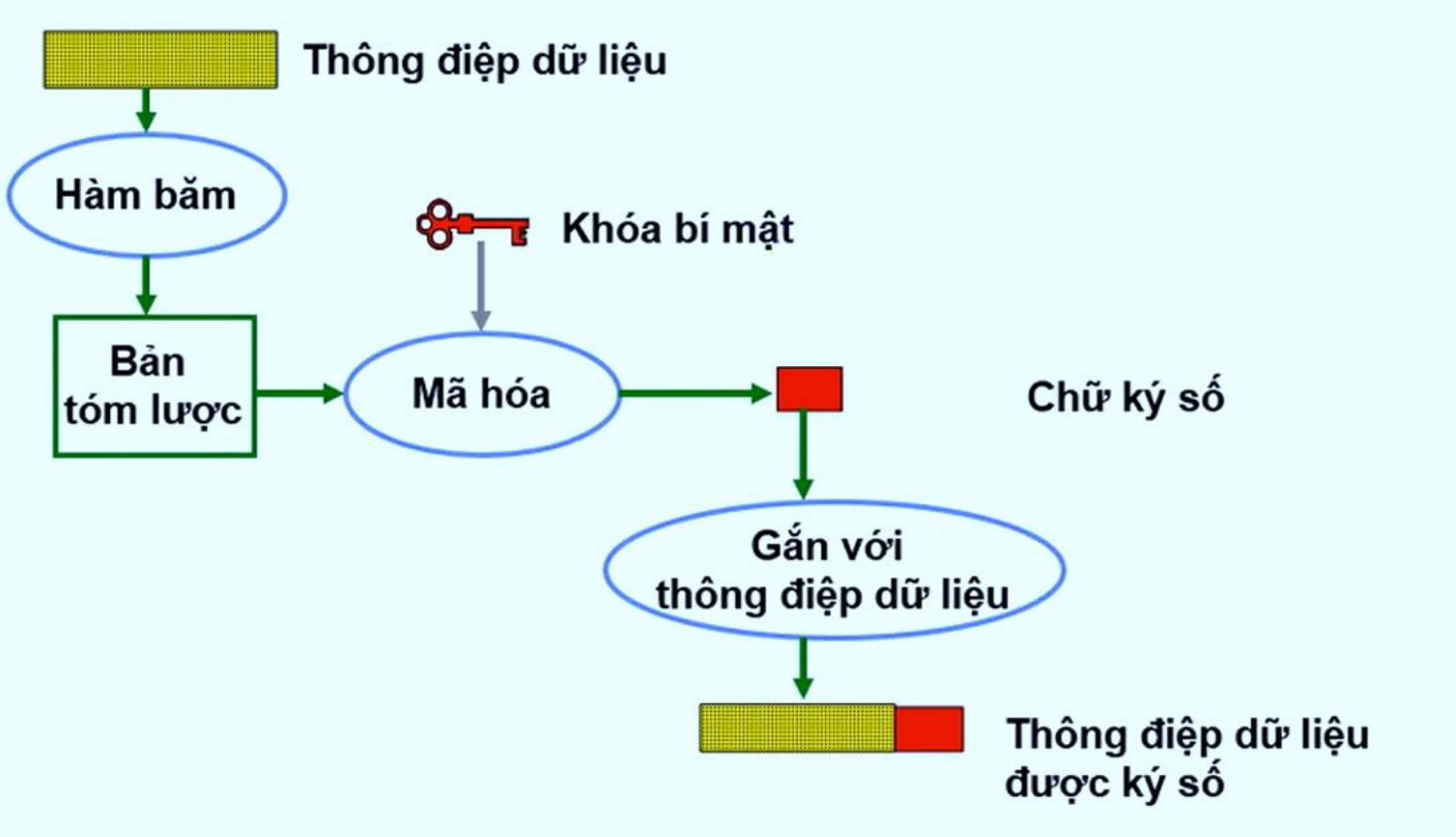
+ Là hàm băm có khóa (keyed hash function)

+ Cho phép 1 trong 2 lựa chọn kích thước giá trị băm là 128 bit và 256 bit

+ Eli Biham đã chỉ ra một đụng độ cho trường hợp 128 bit

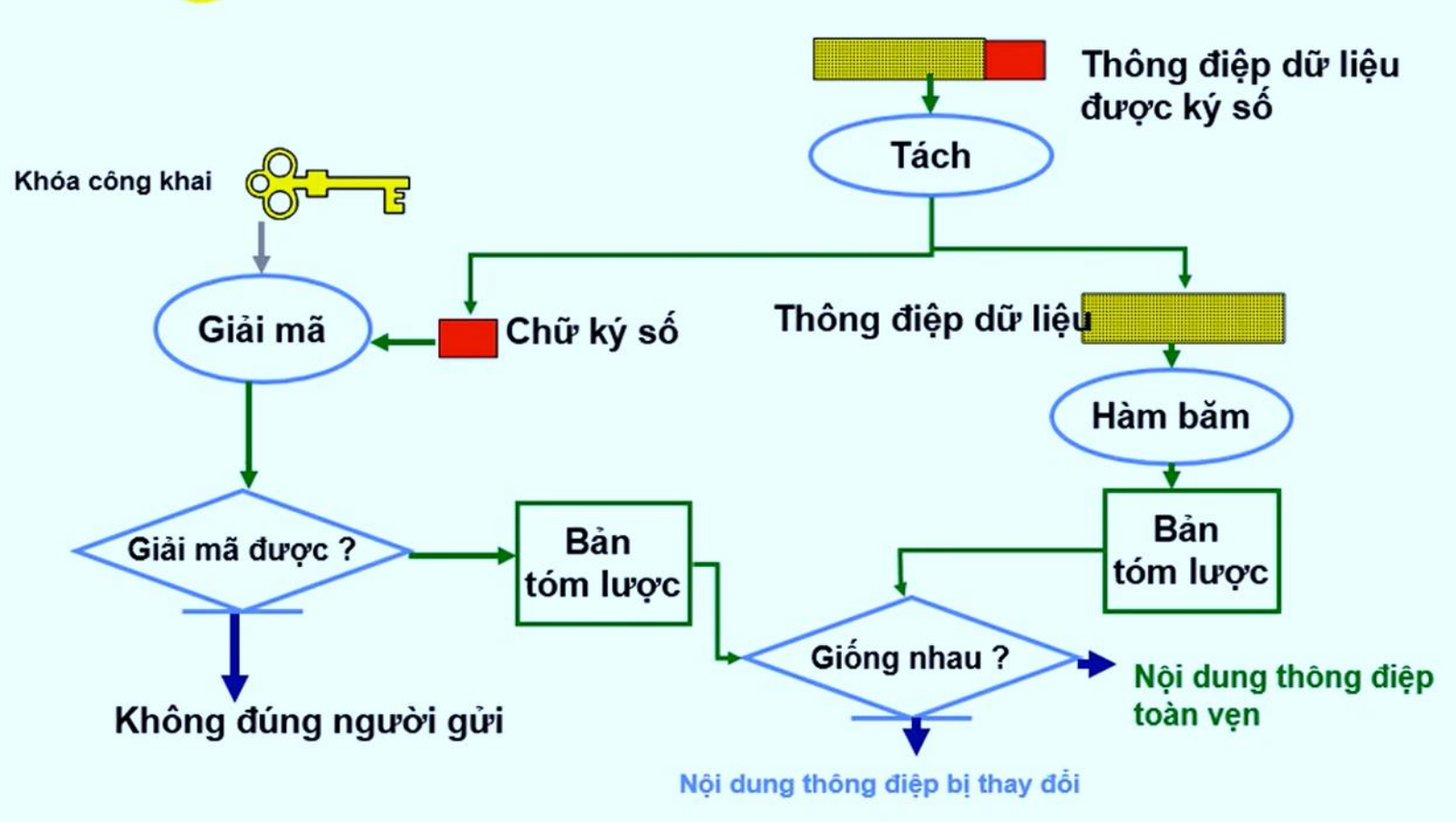
Chương 5:
Chữ ký số và hàm băm

Tạo chữ ký số



Chương 5:
Chữ ký số và hàm băm

Thẩm định chữ ký số



HỆ CHỮ KÝ SỐ RSA

Dựa vào ưu điểm của hệ mã RSA, nếu thiết lập được sơ đồ chữ ký dựa trên bài toán phân tích ra thừa số nguyên tố thì độ an toàn của chữ ký sẽ rất cao

Việc thiết lập sơ đồ xác thực chữ ký RSA rất đơn giản, ta chỉ cần đảo ngược hàm mã hóa với giải mã.

Thuật toán sinh khóa cho chữ ký RSA

(do bên A thực hiện)

1. Sinh hai số nguyên tố lớn p và q có giá trị xấp xỉ nhau
2. Tính $n = p.q$ và $\phi(n) = (p-1).(q-1)$
3. Chọn một số ngẫu nhiên e_A , $1 < e_A < \phi(n)$,

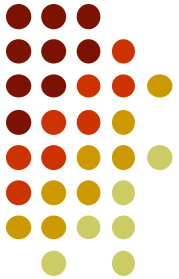
   sao cho $gcd(e_A, \phi(n)) = 1$
4. Sử dụng thuật toán Euclide mở rộng để tính số d_A , $1 < d_A < \phi(n)$, sao cho $e_A . d_A \equiv 1 (mod\ \phi(n))$
5. Khóa kiểm thử là: (n, d_A)
6. Khóa ký là: (e_A)

Thuật toán: Ký và kiểm thử RSA

- Ký: do người A thực hiện
  - Sử dụng khóa ký (e_A) theo thuật toán trên
  - Chọn một bản thông điệp m, trong khoảng [1, n-1]
  - Tính: y = m^{e_A} mod n
  - Nhận được chữ ký (m,y)

- Kiểm thử: do người B thực hiện
  - Lấy khóa kiểm thử (n, d_A). Khóa này được công khai
  - Nếu m = y^{d_A} mod n → TRUE và ngược lại → FALSE

Ví dụ 1:



- p=17, q=23 ➔ n=391
- e_A =3, phi= 352
- d_A=235

$Key_{sig}=(e_A)$, $Key_{ver} = (n,d_A)$

- M=[98 111 109]

Ký: được bản đã ký là sig=[55 304 37], gửi đi (M, sig)

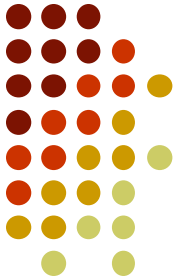
Xác thực được message=[98 111 109] ➔ đúng

Ví dụ 2 :

Cho p = 13, q = 17, e=7

M = [64 112 97]

Ký và xác thực văn bản M?



HỆ CHỮ KÝ SỐ KHÁC RSA

Hệ chữ ký Elgama

Chuẩn chữ ký DSA