HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN

An ninh mạng thông tin

TEL1401

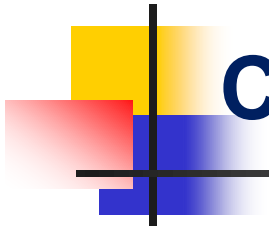
Giảng viên: TS. Phạm Anh Thư

Điện thoại/E-mail: 0912528188

thupa80@yahoo.com, thupaptit@gmail.com

Bộ môn: Mạng viễn thông - KhoaViễn thông 1

Học kỳ/Năm biên soạn: I/ 2022-2023



Chương 3: Các giải thuật toàn vẹn dữ liệu

3.1 Hàm băm (Hash)

3.2 Mã xác thực bản tin (MAC- Message Authentication Code)

3.3 Chữ ký điện tử

Đặt vấn đề

M

Alice

Kênh truyền

Bob

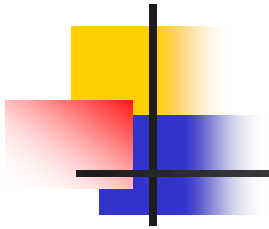
Trudy

M’

Thay đổi nội dung M thành M’

M”

Hoặc, bản tin M” giả danh Alice



Đặt vấn đề

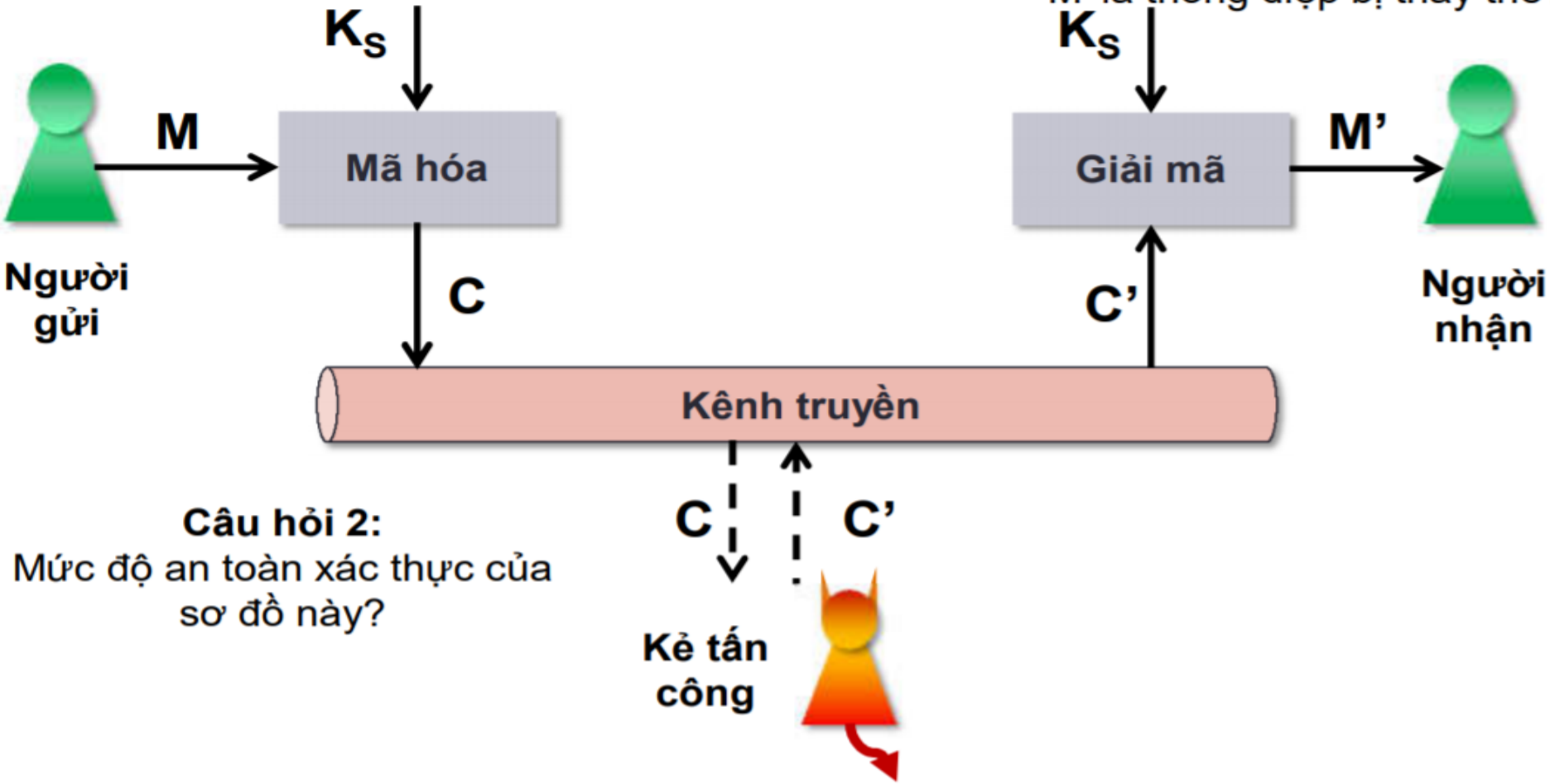
- Chương 2 và 3 đã đưa ra các phương pháp mật mã hóa, để bảo đảm tính chứng thực chúng ta đã giả thiết một thông điệp có ý nghĩa thì phải có một cấu trúc nào đó
  - VD: câu văn chỉ có ý nghĩa khi chữ cái được kết hợp với nhau theo các quy tắc từ vựng và ngữ pháp=> nếu Trudy can thiệp sửa đổi bản mã thì bản giải mã sẽ là một chuỗi bít vô nghĩa, và người nhận biết được là dữ liệu đã bị thay đổi.

Đặt vấn đề

- Bản tin phải được xác minh:
  - Nội dung toàn vẹn: bản tin không bị sửa đổi
    - ✓Bao hàm cả trường hợp Bob cố tình sửa đổi
  - Nguồn gốc tin cậy:
    - ✓Bao hàm cả trường hợp Alice phủ nhận bản tin
    - ✓Bao hàm cả trường hợp Bob tự tạo thông báo và "vu khống" Alice tạo ra thông báo này
  - Đúng thời điểm
  - →Các dạng tấn công điển hình vào tính xác thực: Thay thế (Substitution), Giả danh (Masquerade), tấn công phát lại (Reply attack), Phủ nhận (Repudiation)

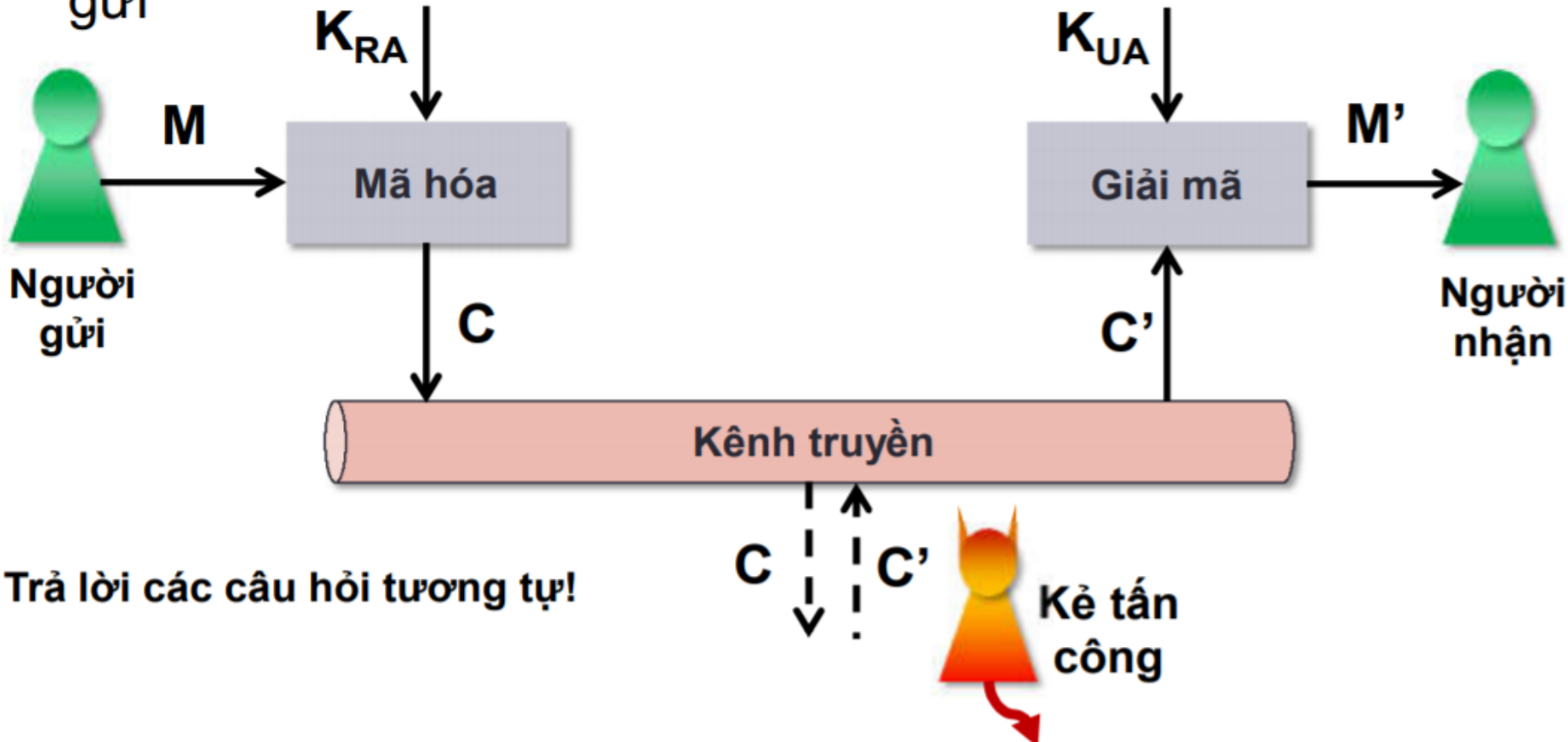
Đặt vấn đề

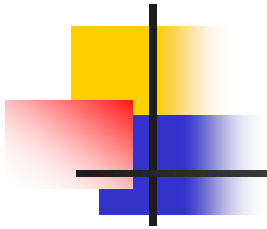
- Nhắc lại sơ đồ mật mã khóa đối xứng



Đặt vấn đề: Sơ đồ mật mã hóa khóa công khai

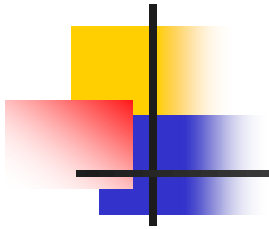
- Chúng ta đã biết sơ đồ bí mật: mã hóa bằng khóa công khai của người nhận
- Sơ đồ xác thực: mã hóa bằng khóa cá nhân của người gửi





Đặt vấn đề

- Tuy nhiên, trong thực tế có nhiều loại dữ liệu mà các bít gần như là ngẫu nhiên. VD: dữ liệu hình ảnh bitmap hay âm thanh =>chấp nhận rằng bất cứ dãy bít nào cũng có thể có ý nghĩa
- Do vậy, phương pháp mã hóa đối xứng và mã hóa công khai không thể bảo đảm tính chứng thực
- Để giải quyết vấn đề chứng thực: mã hóa phải vận dụng khái niệm *redundancy* của lĩnh vực truyền số liệu, tức thêm vào một ít dữ liệu (checksum) để biến bản tin, *từ dãy bít ngẫu nhiên, trở thành dãy bít có cấu trúc*.



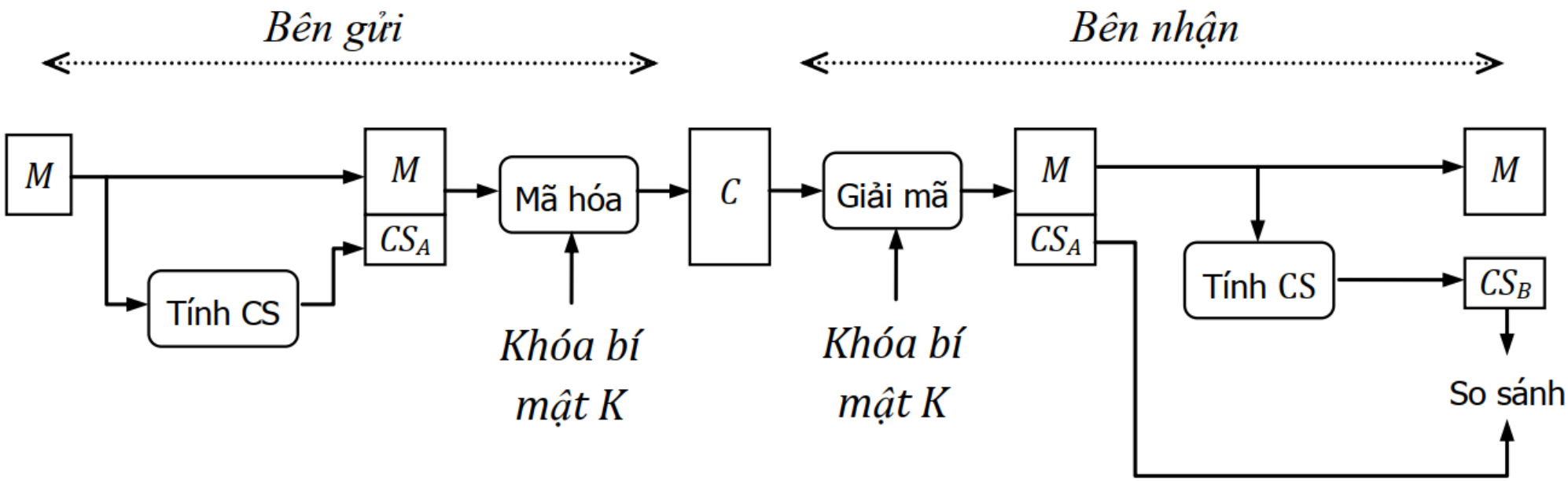
Đặt vấn đề

- Trong quá trình truyền, do tác động *nhiễu* của môi trường, bản tin lúc đến đích có thể bị sai lệch so với bản tin ban đầu trước khi truyền. Để phát hiện nhiễu, một đoạn bít ngắn gọi là checksum (CRC) được tính toán từ dãy bít của bản tin, và gắn vào sau bản tin để tạo redundancy, và được truyền cùng với bản tin đến đích.
- Trong phương pháp CRC không khó để tìm ra hai dãy bít khác nhau mà *có cùng CRC*. Có nghĩa là có thể xảy ra lỗi mà không phát hiện được. Tuy nhiên xác suất ngẫu nhiên xảy ra lỗi trên đường truyền mà làm cho dãy bít truyền và dãy bít nhận có cùng giá trị CRC là rất thấp.

Đặt vấn đề

- Nếu áp dụng cơ chế checksum vào chứng thực thông điệp:

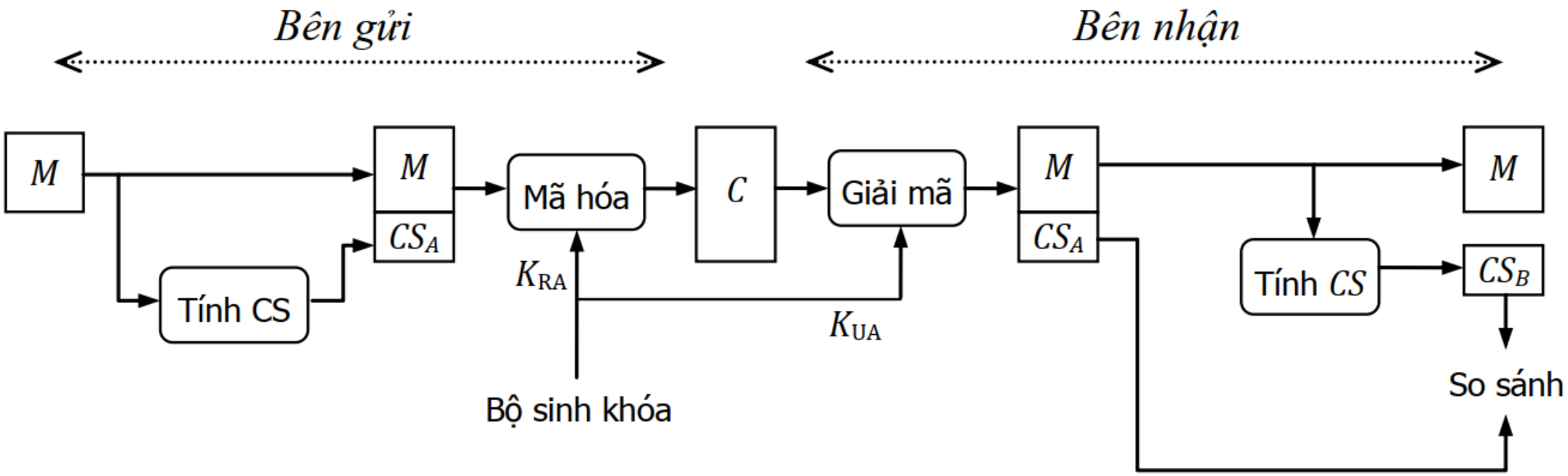
Mô hình chứng thực mã hóa đối xứng có dùng checksum



Đặt vấn đề

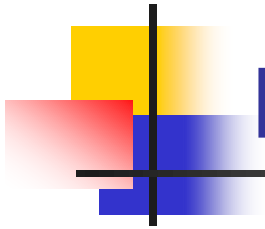
- Nếu áp dụng cơ chế checksum vào chứng thực thông điệp:

Mô hình chứng thực mã hóa khóa công khai dùng checksum



Đặt vấn đề

- Nếu Trudy sửa bảng mã C, thì bản giải mã của Bob, ký hiệu M_T và CS_T, sẽ mất đi tính cấu trúc. Nghĩa là checksum CS_B mà Bob tính được từ M_T không giống với CS_T. Và Bob biết được là bản tin bị thay đổi đường truyền. Nếu hàm checksum có độ phức tạp cao thì xác suất để $CS_B = CS_T$ là rất thấp.
- Ngoài ra còn có hai phương thức chứng thực thông điệp khác mà chúng ta sẽ tìm hiểu trong chương này là mã chứng thực thông điệp MAC và hàm băm (Hash function).



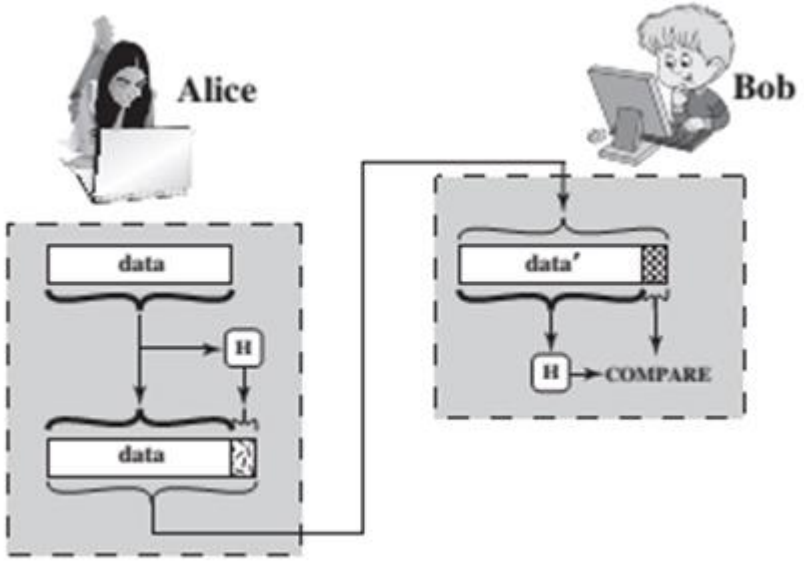
Hàm băm

- Hàm băm được xem là thuật toán mã hoá linh hoạt nhất trong các loại thuật toán mã hoá
- Được sử dụng rộng rãi trong nhiều ứng dụng bảo mật và giao thức Internet.
- Hàm băm được sử dụng trong cơ chế xác thực bản tin để cung cấp một giá trị băm, thường được gọi là bản tin rút gọn.

Hàm băm

- Cơ chế hoạt động:

  - Người gửi tính toán một giá trị băm từ các bít trong bản tin và truyền đi đồng thời bản tin và giá trị băm đó.

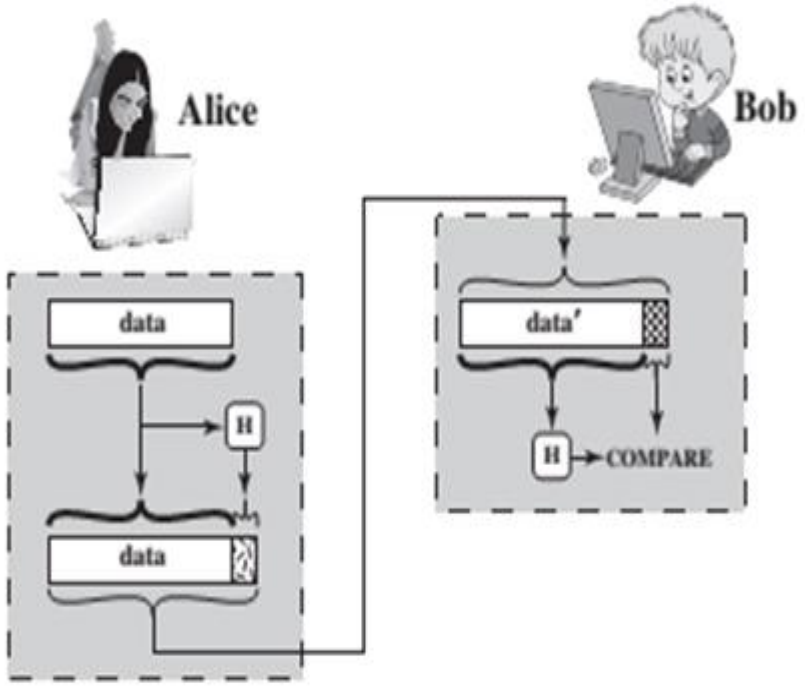


(a) Use of hash function to check data integrity

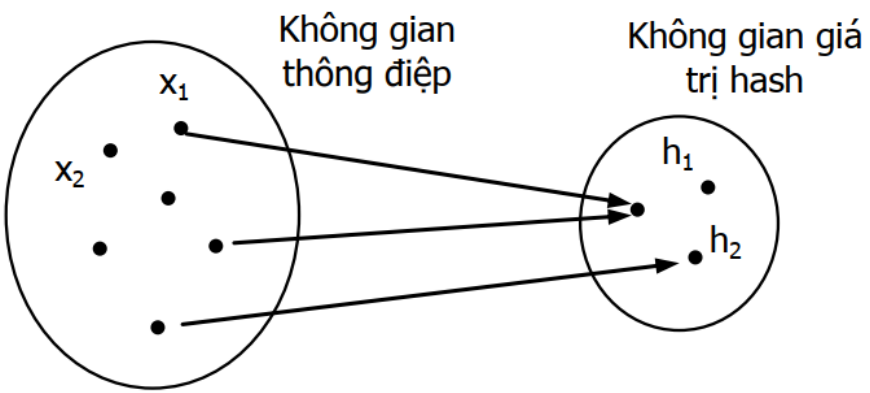
Hàm băm

- Cơ chế hoạt động:

- Người nhận cũng thực hiện việc tính giá trị băm tương tự từ các b trong bản tin nhận được và so sánh với giá trị băm được gửi kèm
- Nếu như các giá trị băm được so sánh không trùng với nhau thì có nghĩa là bản tin nhận được (hoặc các giá trị băm) đã bị thay đổi.



(a) Use of hash function to check data integrity

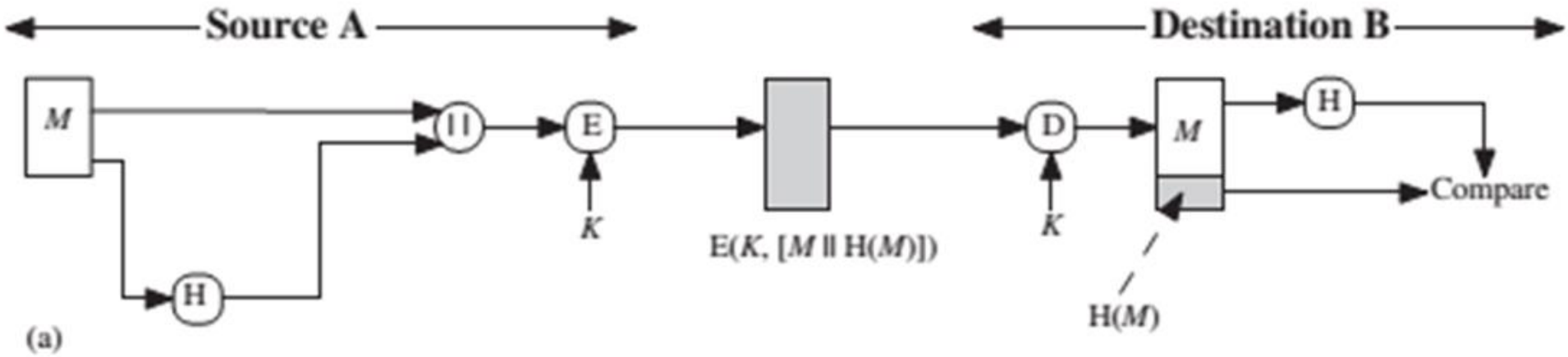


Hàm băm

- *Hàm băm H*: thực hiện phép biến đổi:
  - Đầu vào: bản tin có kích thước bất kỳ
  - Đầu ra: giá trị *digest h = H(M)*có kích thước *n* bit cố định (thường nhỏ hơn rất nhiều so với kích thước bản tin đầu vào)
- Chỉ thay đổi 1 bit đầu vào, làm thay đổi hoàn toàn giá trị đầu ra
- Ví dụ:
  - Đầu vào: “The quick brown fox jumps over the lazy dog”
  - Mã băm: 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
  - Đầu vào: “The quick brown fox jumps over the lazy cog”
  - Đầu ra: de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3

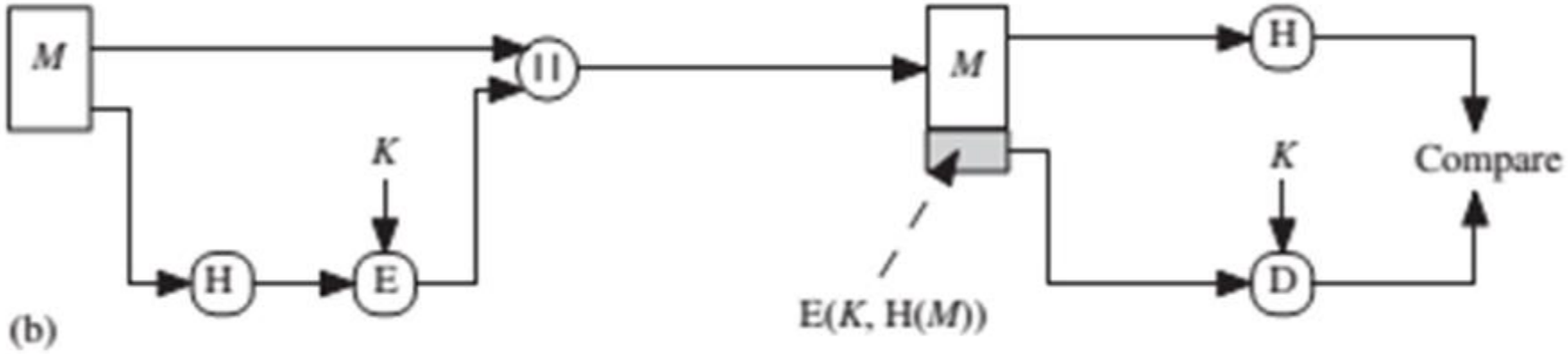
Hàm băm

- **Cách áp dụng hàm băm trong việc xác thực bản tin:**
  - Mã băm được nối vào bản tin, sau đó được mã hoá bởi mã hoá đối xứng. Vì chỉ có A và B biết khoá bí mật nên bản tin được đảm bảo truyền từ A và không bị sửa đổi. Do cả mã băm và bản tin đều được mã hoá nên tính bảo mật cũng được cung cấp trong trường hợp này.



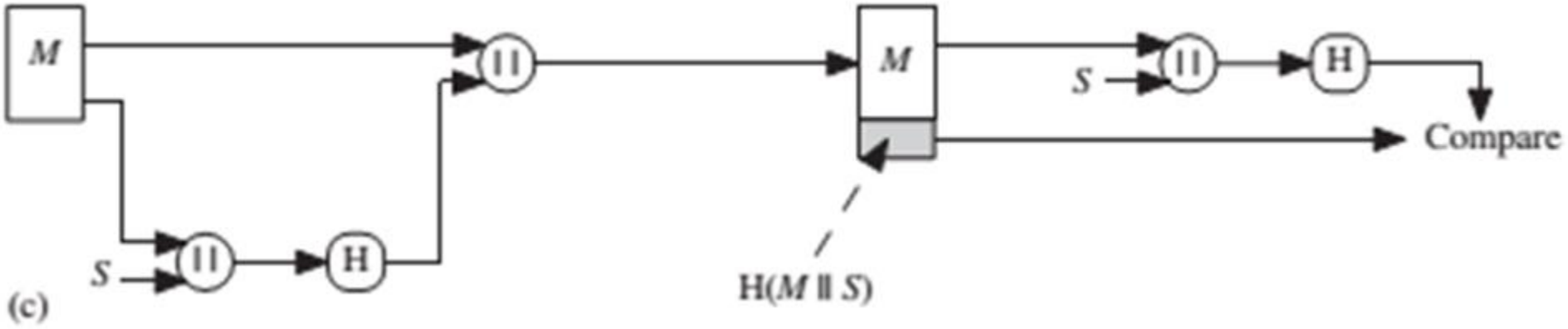
Hàm băm

- **Cách áp dụng hàm băm trong việc xác thực bản tin:**
  - Chỉ có các mã băm được mã hoá bằng mã hoá đối xứng. Điều này giúp giảm gánh nặng xử lý cho các ứng dụng không yêu cầu bảo mật.



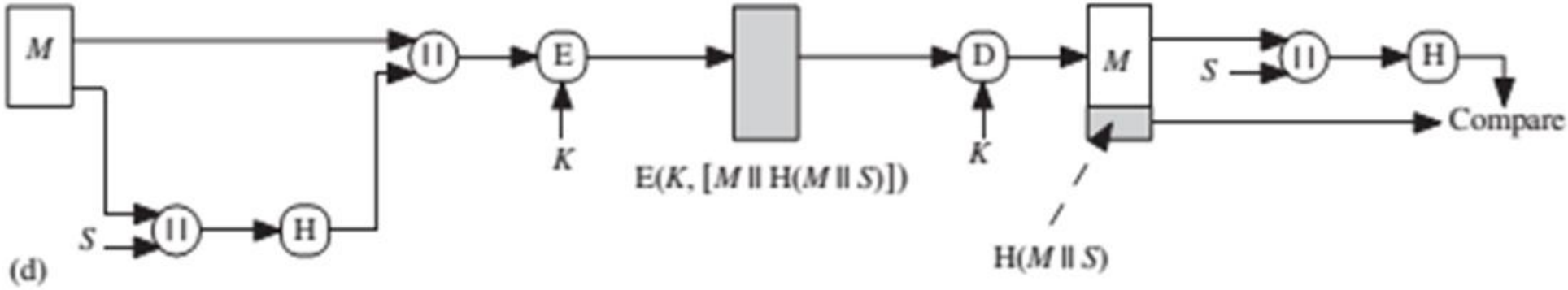
Hàm băm

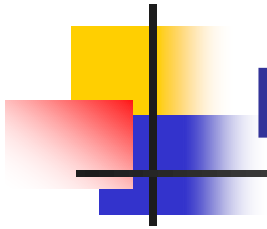
- **Cách áp dụng hàm băm trong việc xác thực bản tin:**
  - Giả sử bên gửi và nhận chia sẻ một giá trị bí mật *S*. Giá trị này được nối vào bản tin *M* và được sử dụng để tính toán giá trị băm. Sau đó, giá trị băm này được cộng với bản tin và truyền đi. Tại đầu nhận, B cũng có khả năng tính toán giá trị băm vì nó cũng biết *S*. Vì chỉ có A và B biết *S*, nên kẻ xấu không thể sửa đổi hoặc làm giả bản tin. Trong phương pháp này, tính bảo mật không được cung cấp.



Hàm băm

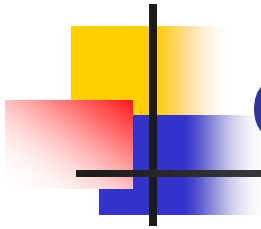
- **Cách áp dụng hàm băm trong việc xác thực bản tin:**
  - Phương pháp này khác phương pháp (c) ở việc tính bảo mật được thêm vào để mã hoá toàn bộ bản tin và mã băm trước khi truyền đi.





Hàm băm

- Khi tính bảo mật không cần thiết thì phương pháp (b) ưu việt hơn hai phương pháp (a) và (d) do phải tính toán ít hơn. Thậm chí việc tránh mã hoá như trong phương pháp (c) ngày càng nhận được nhiều sự quan tâm hơn bởi:
  - Mã hoá bằng phần mềm tương đối chậm
  - Chi phí cho việc mã hoá bằng phần cứng là không nhỏ
  - Mã hoá bằng phần cứng phù hợp hơn trong việc mã hoá dữ liệu lớn
  - Các thuật toán mã hoá thường bị giới hạn bởi các bằng sáng chế



Các yêu cầu của hàm băm

Phương pháp checksum CRC cho phép hai dãy bít có cùng checksum, thì hàm băm $H(x)$ là một hàm tính checksum mạnh thỏa mãn các yêu cầu sau:

1) H có thể áp dụng cho các thông điệp x với các độ dài khác nhau
2) Kích thước của output $h = H(x)$ là cố định và nhỏ
3) Tính một chiều: với một h cho trước, không thể tìm lại được x sao cho $h = H(x)$ (về mặt thời gian tính toán)
4) Tính chống trùng yếu: cho trước một x, không thể tìm $y \neq x$ sao cho $H(x) = H(y)$
5) Tính chống trùng mạnh: không thể tìm ra cặp x, y bất kỳ ($x \neq y$) sao cho $H(x) = H(y)$, hay nói cách khác nếu $H(x) = H(y)$ thì có thể chắc chắn rằng $x = y$

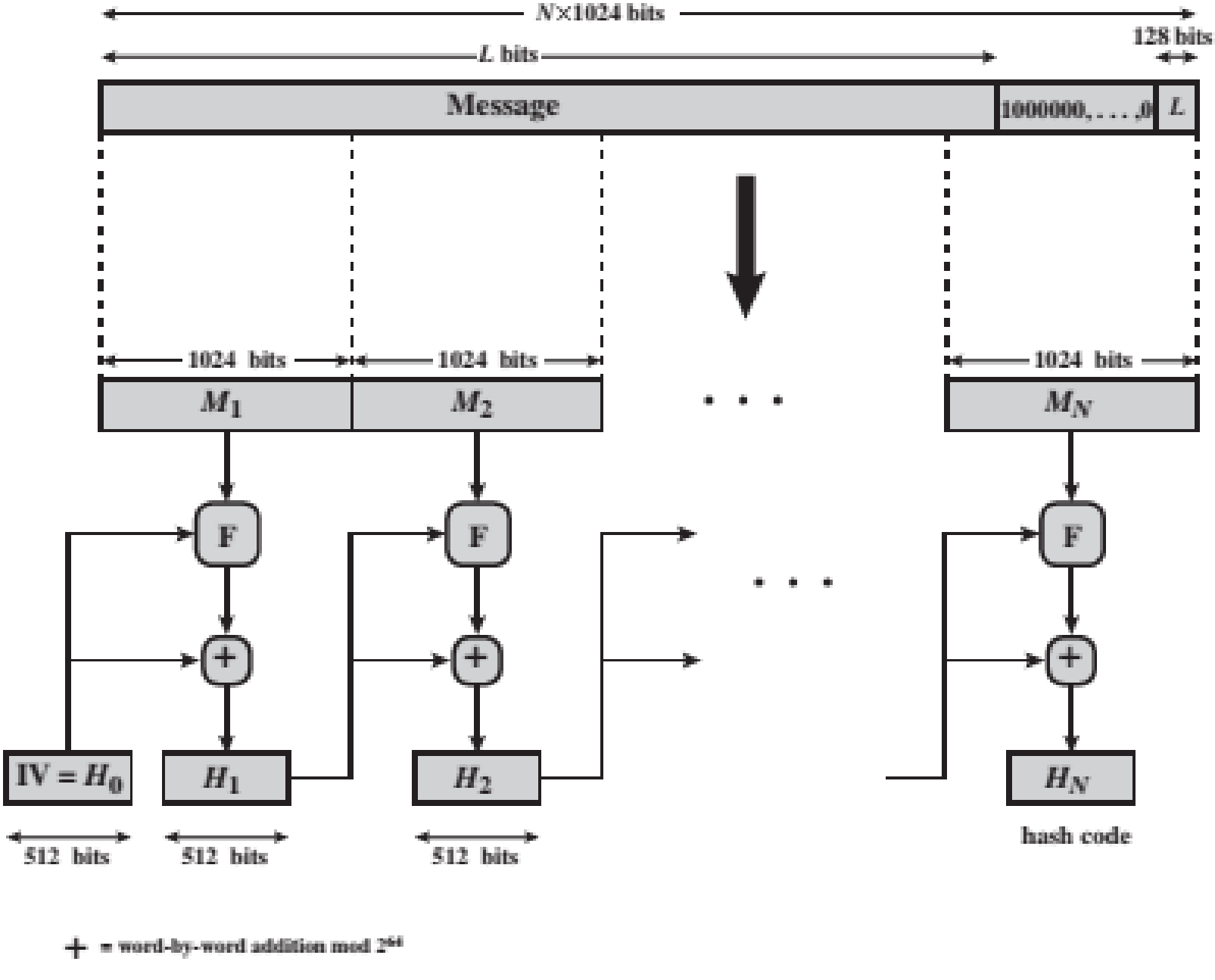
Các hàm hash

- MD: MD5 hash function (RFC 1321)
  - 128-bit.
- SHA: SHA-1, SHA-2, Sha-3
  - US standard [NIST, FIPS PUB 180-1]
- Whirlpool

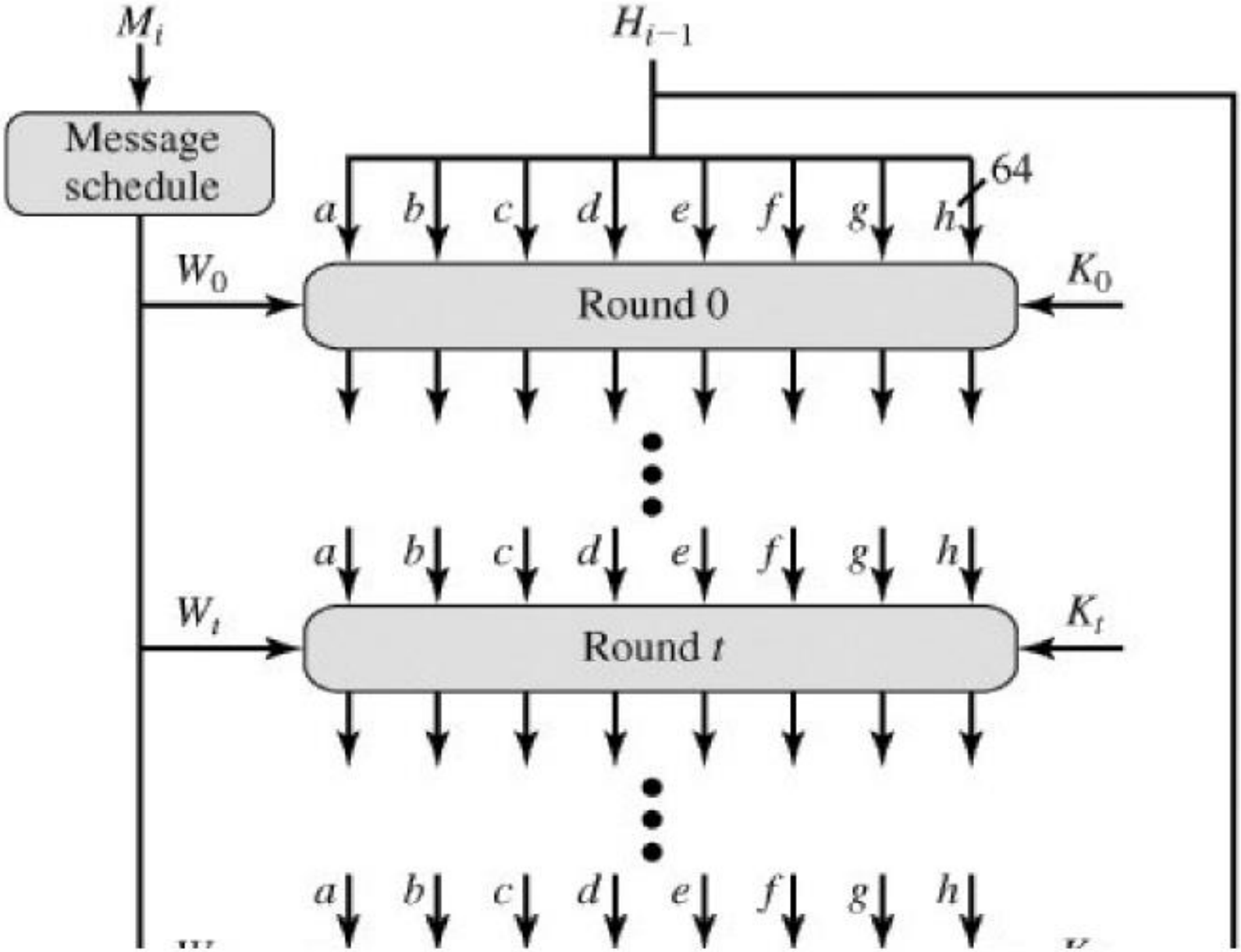
Các hàm hash SHA

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block Size	512	512	512	1024	1024
Word Size	32	32	32	64	64
Number of Steps	80	64	64	80	80

SHA-512

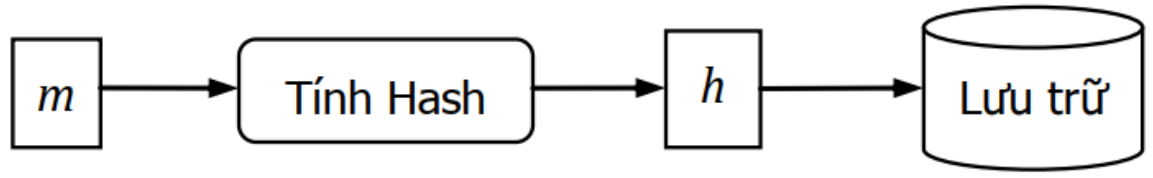

N×1024 bits
L bits
128 bits
Message
1000000, . . . ,0
L
1024 bits
1024 bits
1024 bits
M1
M2
MN
F
F
F
+
+
+
IV = H0
H1
H2
HN
512 bits
512 bits
512 bits
hash code
+ = word-by-word addition mod 2^64

Quá trình xử lí SHA-512

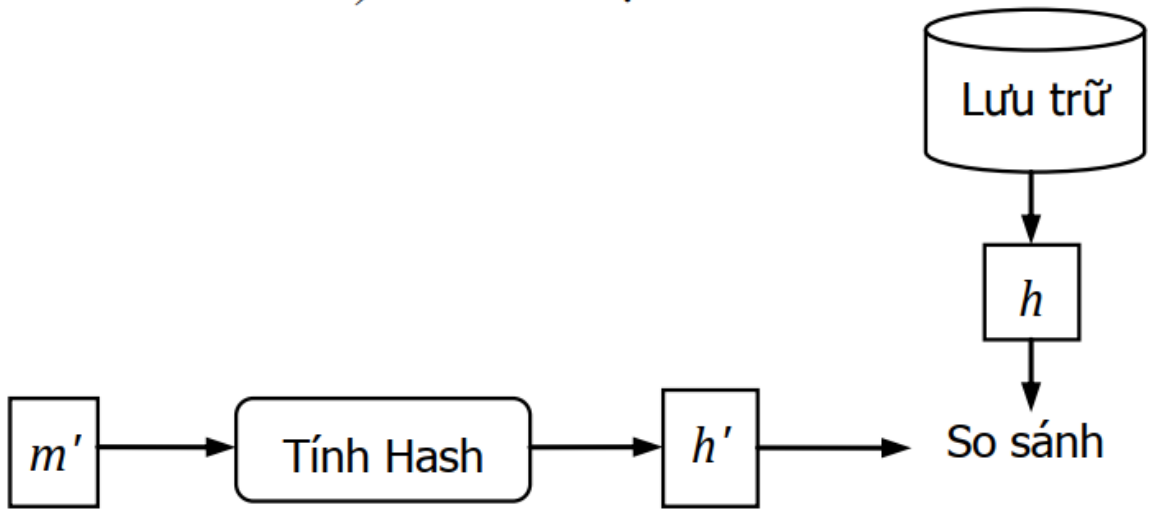


Ứng dụng của hàm băm

- Ứng dụng lưu trữ mật khẩu:
  - Khi người sử dụng đăng ký mật khẩu, giá trị băm của mật khẩu được tính bằng một hàm băm nào đó (MD5 hay SHA-1,…)
  - Giá trị băm được lưu trữ vào file hay cơ sở dữ liệu

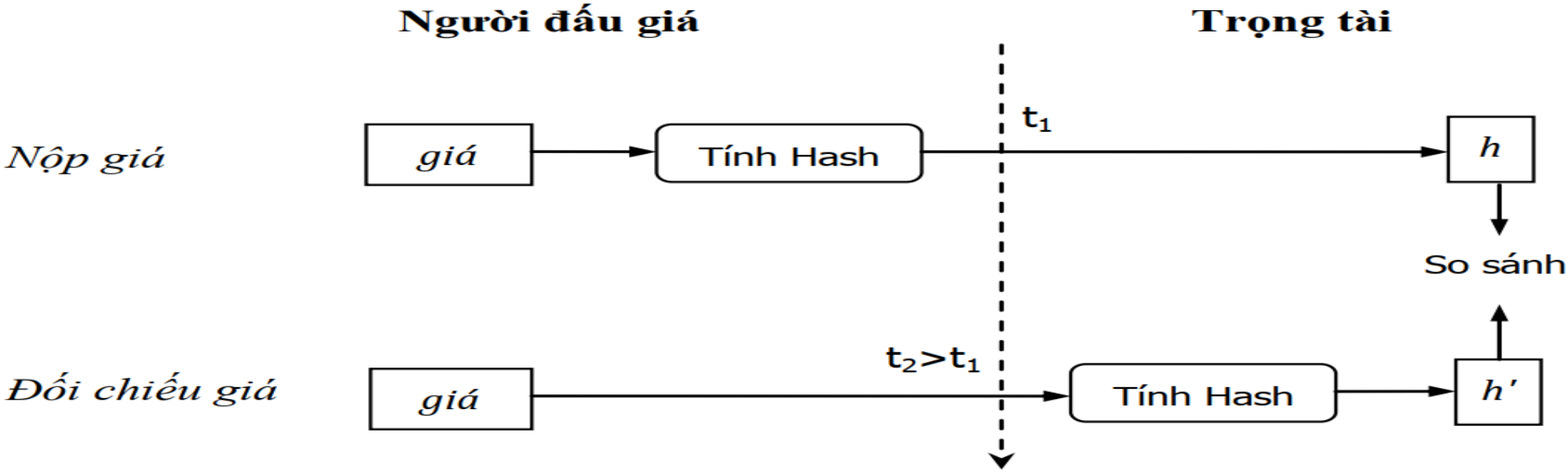


a) Lưu trữ mật khẩu



b) Chứng thực mật khẩu, theo tính chống trùng, nếu h'=h thì m'=m

Ứng dụng của hàm băm



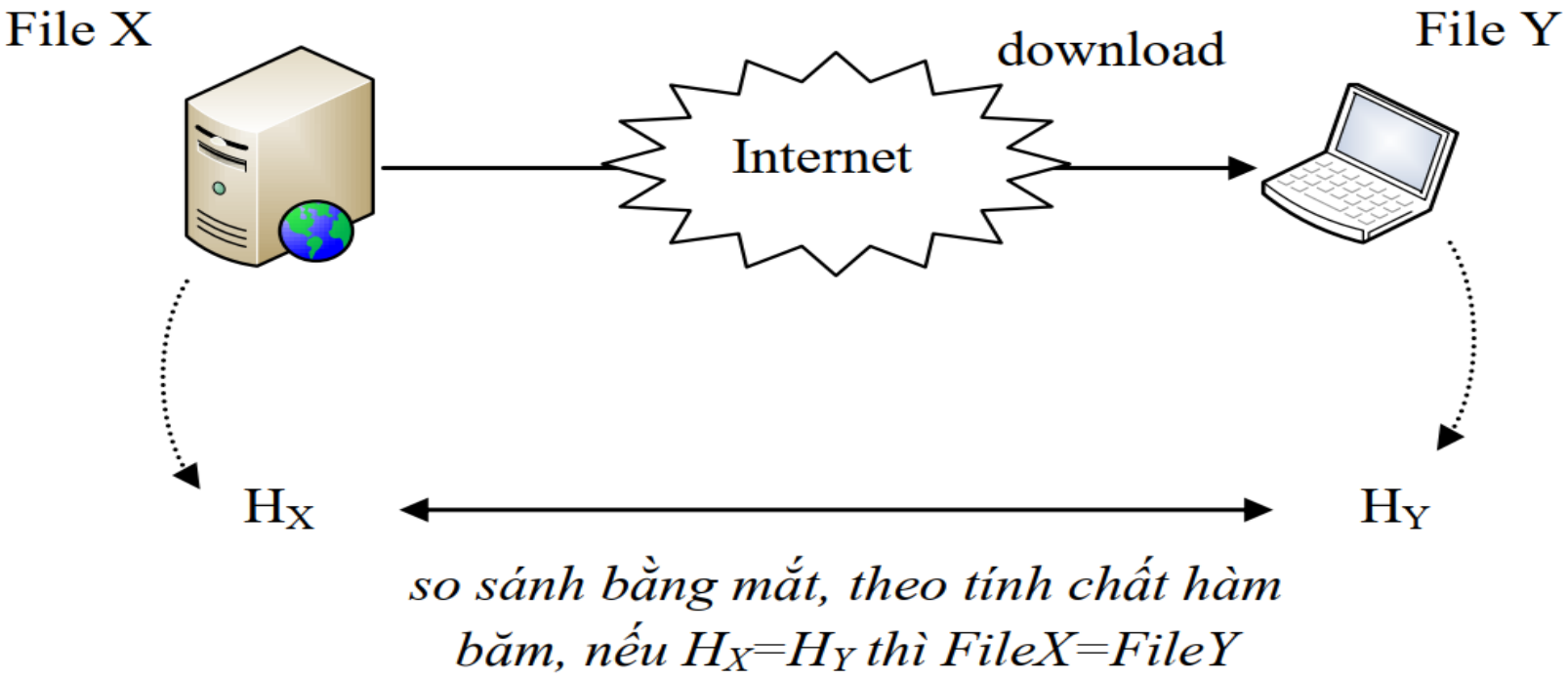
- Đấu giá trực tuyến:

- Mức giá bỏ thầu của Alice và Bob sẽ được tính các giá trị băm tương ứng và chỉ cung cấp cho trọng tài các giá trị băm này
- Vì hàm băm là một chiều, nếu trọng tài và Trudy bắt tay nhau thì cũng không thể biết được giá của Alice và Bob
- Khi công bố, Trọng tài sẽ tính các giá trị băm tương ứng và so sánh với các giá trị băm đã nộp để bảo đảm rằng mức giá mà Alice, Bob và Trudy là đúng với ý định ban đầu

Ứng dụng của hàm băm

Download dữ liệu:

- Khi download file từ mạng internet, nếu chất lượng mạng không tốt thì có thể xảy ra lỗi trong quá trình download làm cho file tại máy client khác với file trên server. Hàm băm có thể giúp chúng ta phát hiện ra những trường hợp bị lỗi như vậy.

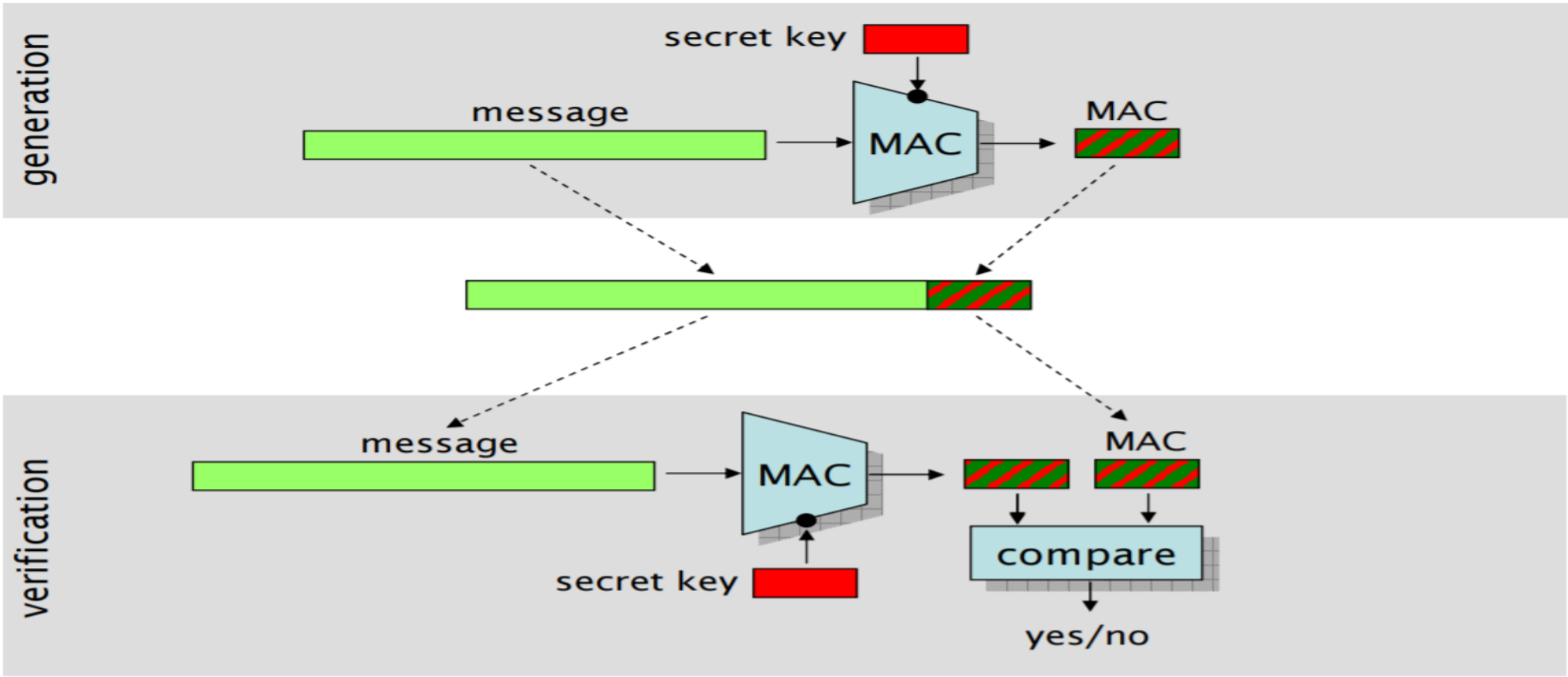


Mã chứng thực/xác thực bản tin

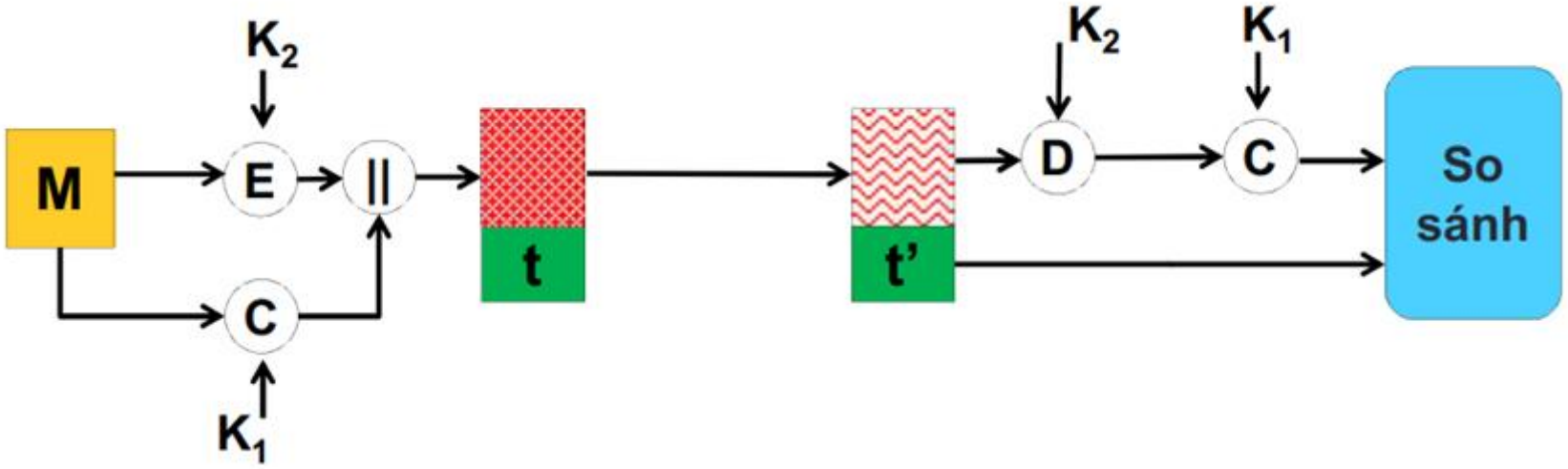
- Mã chứng thực bản tin (MAC) có thể coi là một dạng checksum của mã hóa, được tính theo công thức $MAC = C(M, K)$, trong đó:
  1) *M* là thông điệp cần tính *MAC*
  2) *K* là khóa bí mật được chia sẻ giữa người gửi và người nhận
  3) *C* là hàm tính *MAC*
- MAC: Một hàm của bản tin và khóa bí mật tạo ra giá trị có chiều dài cố định có chức năng như một ký hiệu xác thực.

Mã chứng thực/xác thực bản tin

- Mô hình MAC để chứng thực bản tin, không có tính bảo mật

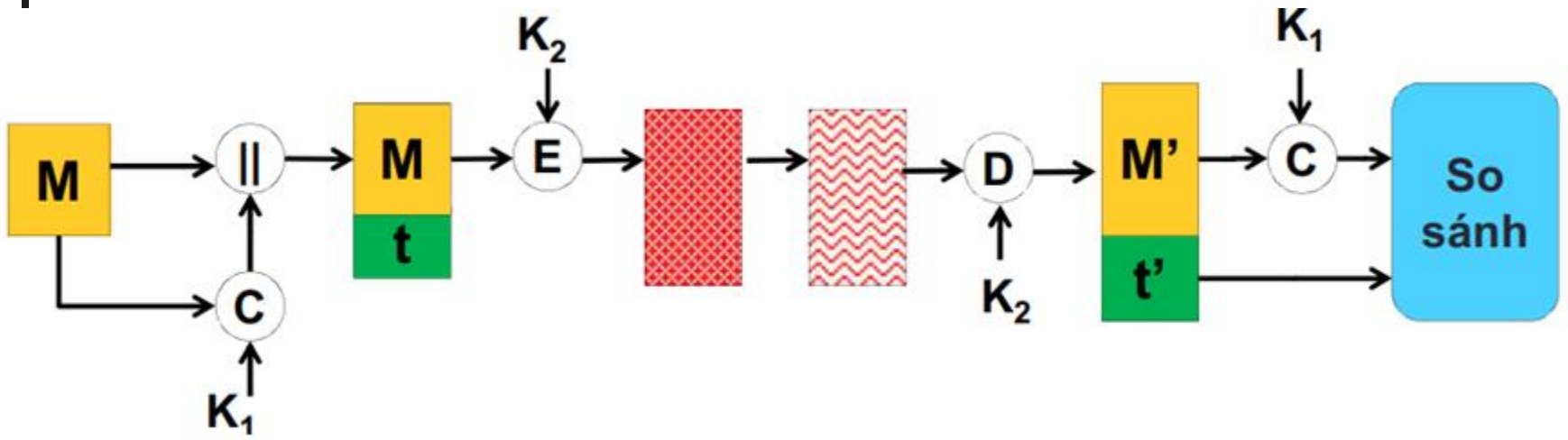


Một số sơ đồ sử dụng mã MAC



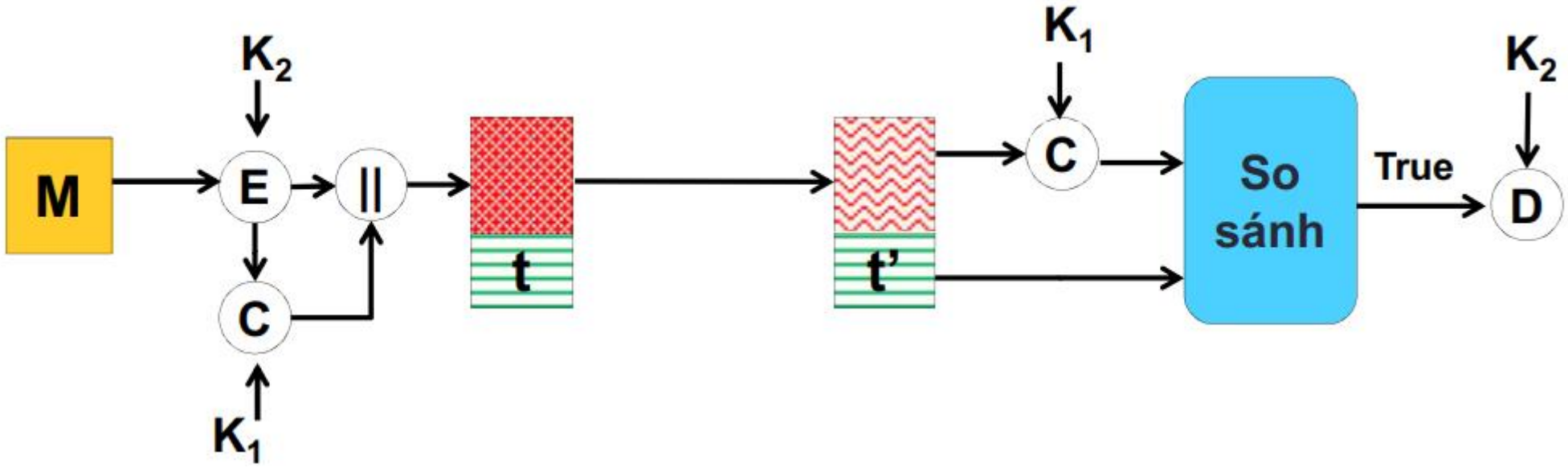
- Tính bảo mật có thể được cung cấp bằng cách sử dụng mật mã hóa bản tin

Một số sơ đồ sử dụng mã MAC



- Cung cấp tính chứng thực và tính bảo mật, do toàn bộ bản tin được truyền một cách bảo mật sử dụng mật mã hóa bản tin sau thuật toán MAC

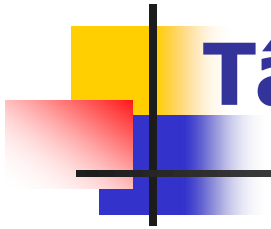
Một số sơ đồ sử dụng mã MAC



- Tính bảo mật có thể được cung cấp bằng cách sử dụng mật mã hóa bản tin trước thuật toán MAC

Các yêu cầu cho mã xác thực bản tin

- Nếu một kẻ tấn công quan sát M và MAC(K,M), sẽ là không khả thi với kẻ tấn công nếu tạo một bản tin M’ cùng nhãn (MAC) với M
- MAC(K,M) nên có phân bố chuẩn đối với các bản tin được lựa chọn ngẫu nhiên, M và M’, xác suất để MAC(K,M)= MAC(K,M’) là 2^{-n}, trong đó n là số bit trong nhãn.
- Cho M’ là kết quả của sự chuyển đổi nào đó của M, M’=f(M).Ví dụ, f có thể là một số thao tác nghịch đảo một hoặc nhiều bit. Khi đó: Pr[MAC(K,M)= MAC(K,M’)] =2^{-n}



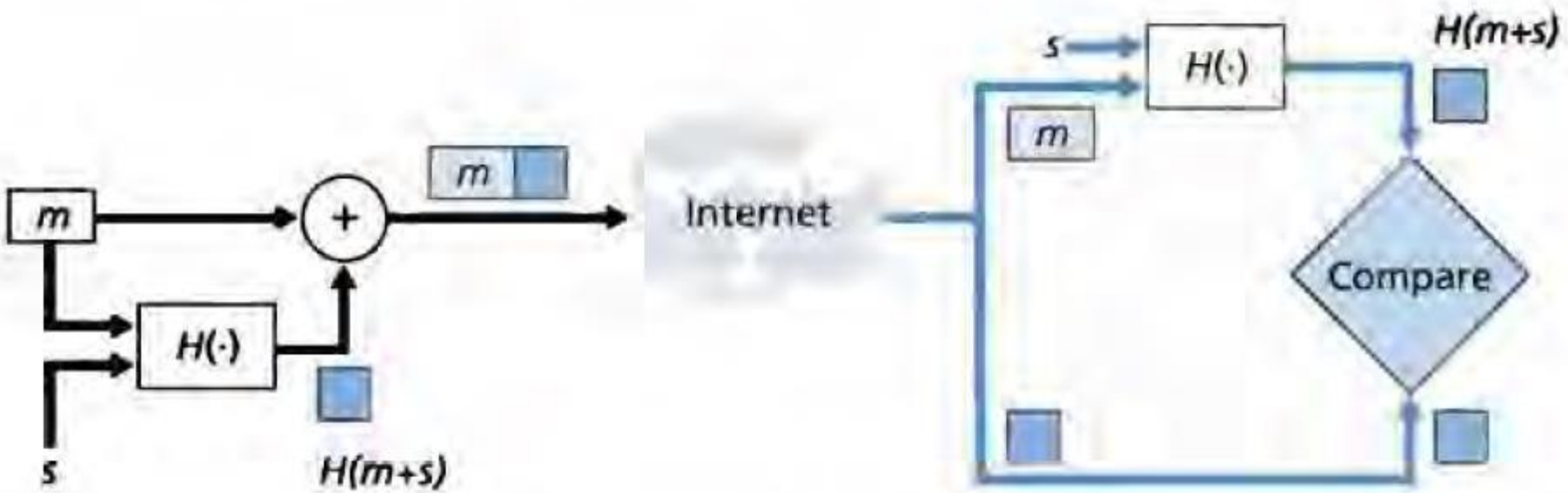
Tấn công MAC

- *Tấn công vét cạn*
  - Tấn công không gian khóa
  - Tấn công giá trị MAC.
- *Phân tích mã*

Hai chuẩn hàm MAC

- Để giúp các nhà phát triển ứng dụng tích hợp MAC vào sản phẩm khác nhau, viện tiêu chuẩn và công nghệ quốc gia của Mỹ (NIST) đưa ra hai chuẩn về hàm MAC.
  - HMAC (Keyd-Hash Messasge Authentication Code): sử dụng hàm băm thực hiện chức năng MAC
  - CMAC (Cipher Message Authentication Code - CMAC): sử dụng mã khối để thực hiện chức năng MAC

MAC dựa trên hàm băm (HMAC)



Key:

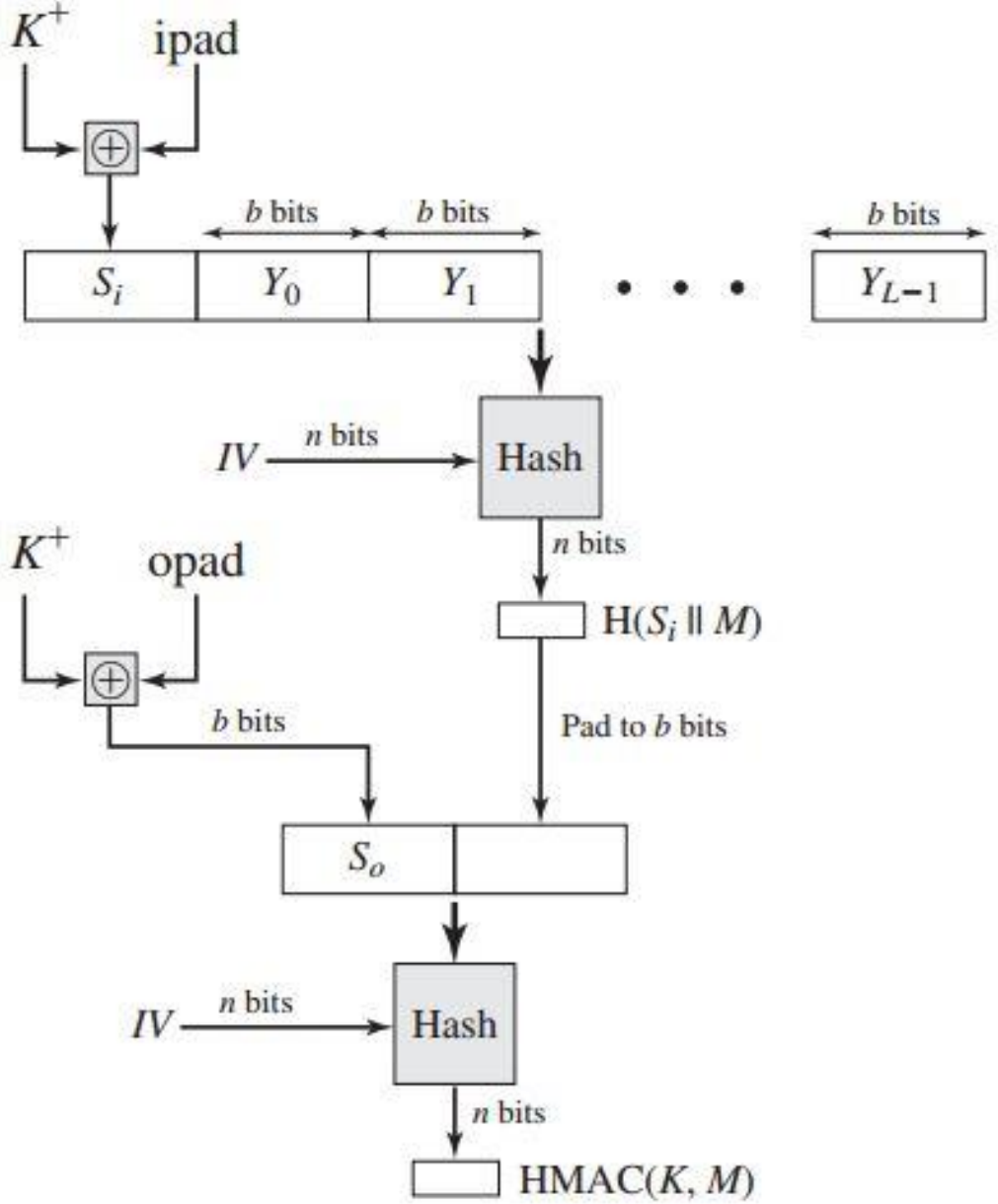
m = Message

s = Shared secret

Động lực của mối quan tâm này là:

- Các hàm băm mã hóa như là MD5 hay SHA thực hiện nhanh hơn trong phần mềm so với mã khối đối xứng như DES.
- Thư viện mã cho các hàm băm mã hóa được phổ biến rộng rãi

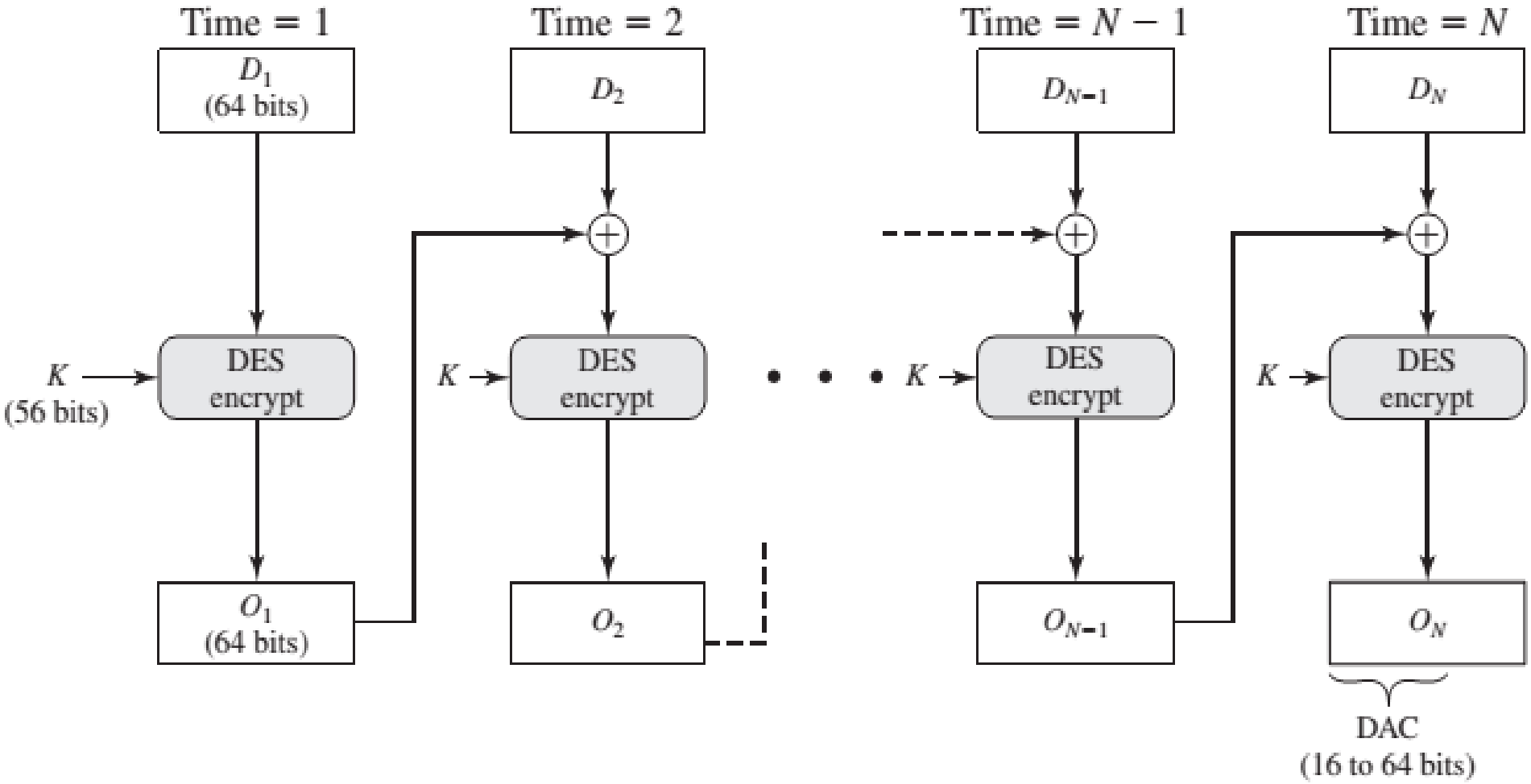
Kiến trúc HMAC



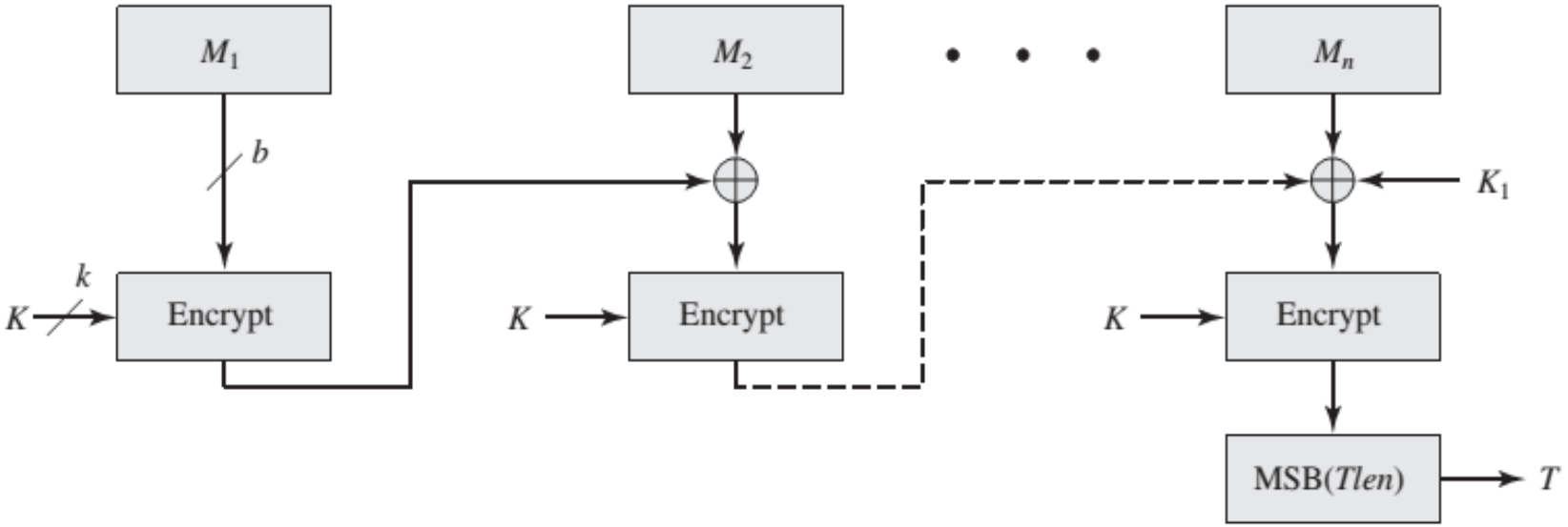
$$\text{ipad} = 00110110, 00110110, \ldots, 00110110$$

$$\text{opad} = 01011100, 01011100, \ldots, 01011100.$$

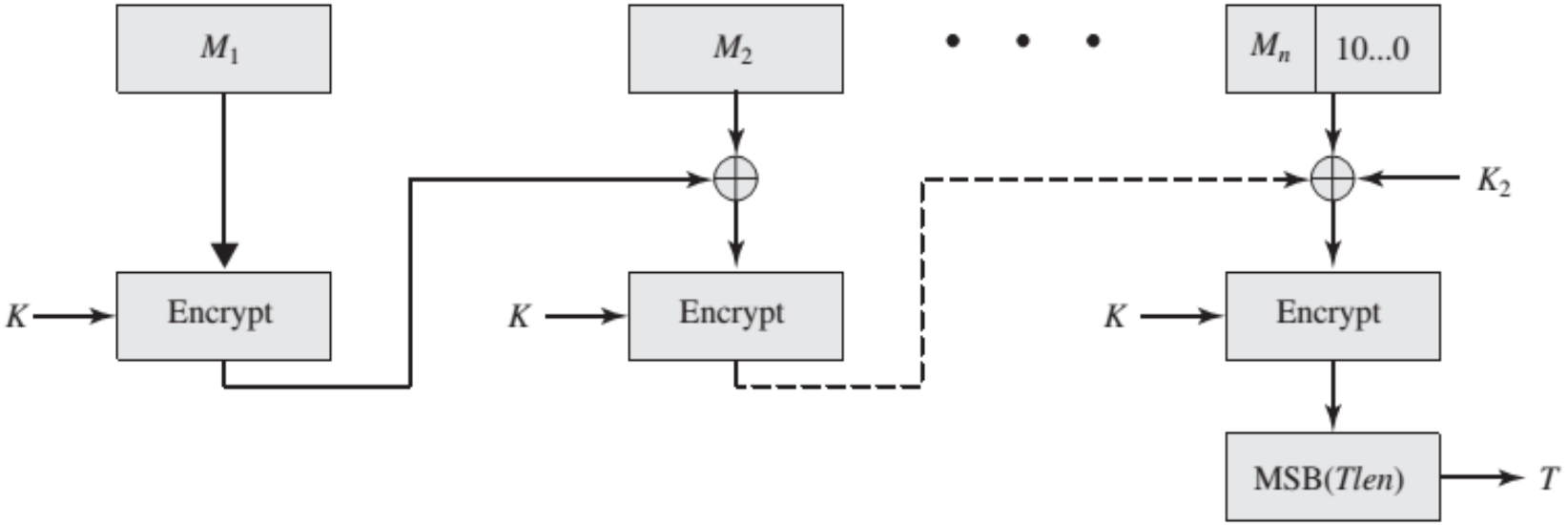
MAC dựa trên mật mã khối – thuật toán DAA



CMAC



(a) Message length is integer multiple of block size



(b) Message length is not integer multiple of block size

Mật mã được xác thực (1)
(Authenticated Encryption)

- Là các hệ thống mật mã hóa với mục đích bảo vệ đồng thời cả tính bảo mật và xác thực
- Nhiều ứng dụng và giao thức yêu cầu cả hai hình thức an ninh này
- Tuy nhiên, thường hai dịch vụ này đã được thiết kế riêng biệt
- Có bốn phương pháp chung để cung cấp cả mật mã và xác thực cho một bản tin M

Mật mã được xác thực (2)

- **Băm và mật mã hóa (H->E):**
  - Đầu tiên tính toán mã hàm băm trên bản tin M
  - Thực hiện mã hóa bản tin đã được thêm hàm băm:

$$\mathrm{E}(K,(M \,||\, h))$$

Mật mã được xác thực (3)

- **Xác thực rồi mật mã hóa (A->E):**
  - Sử dụng hai khóa.
  - Đầu tiên xác thực bản rõ bằng tính toán giá trị MAC

$$T = \mathrm{MAC}(K_1, M)$$

  - Mật mã hóa bản tin được thêm mã xác thực bản tin.

$$\mathrm{E}(K_2, [M \,||\, T])$$

  - Tiếp cận này được thực hiện bởi các giao thức SSL/TLS.

Mật mã được xác thực (4)

- **Mật mã hóa rồi nhận thực (E->A):**
  - Sử dụng hai khóa.
  - Đầu tiên mã hóa bản tin thành bản mã

$$C = \mathrm{E}(K_1, M)$$

  - Xác thực bản mã với T để tạo thành cặp (C, T).

$$T = \mathrm{MAC}(K_2, \mathrm{C})$$

  - Tiếp cận này được sử dụng trong giao thức IPSec.

Mật mã được xác thực (5)

- **Độc lập mã hóa và nhận thực (E + A):**
  - Sử dụng hai khóa.
  - Mật mã hóa bản tin thành bản mã,

$$C = \mathrm{E}(K_1, M)$$

  - Xác thực bản rõ với T để tạo thành cặp (C, T).

$$T = \mathrm{MAC}(K_2, M)$$

  - Hoạt động này có thể được thực hiện độc lập và được ứng dụng trong giao thức SSH.

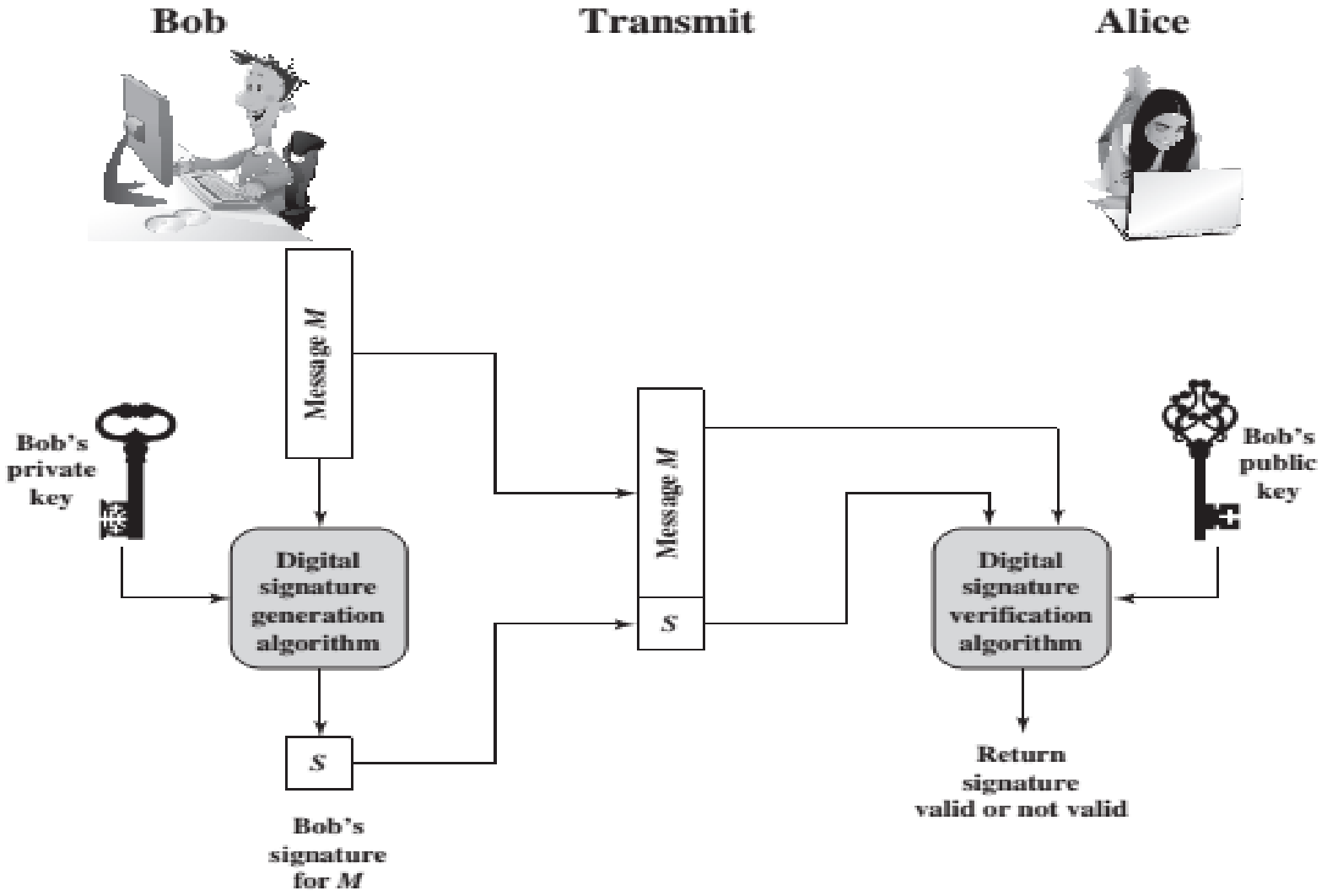
Chữ ký số (Digital signature)

- Chữ ký số: là dạng chữ ký điện tử, phụ thuộc vào văn bản gửi đi (khác chữ ký truyền thống).
- Với MAC: 1 bên tạo MAC, 1 bên thẩm định tính toàn vẹn
- Với DS: 1 bên tạo ra chữ ký, nhiều bên thẩm tra chữ ký
- Dựa trên công nghệ khóa công khai (mỗi người cần 1 cặp khóa công khai và khóa bí mật)
- Khóa bí mật dùng để tạo chữ ký số
- Khóa công khai dùng để xác thực chữ ký số

Chữ ký số (Digital signature)

- Chữ ký số cung cấp
  - Tính hợp pháp của người gửi
  - Tính toàn vẹn của dữ liệu
  - Tính chống chối bỏ
- Chữ ký số là hàm của các tham số:
  - Văn bản gốc
  - Thông tin bí mật của người gửi (khóa bí mật)
  - Thông tin công khai trên mạng (khóa công khai)
  - Mã xác thực để đảm bảo tính toàn vẹn của dữ liệu

Quá trình tổng quát tạo chữ ký số



Chữ ký số (Digital signature)

- Mục đích của chữ ký số:
  - Xác thực: xác định ai là chủ của bản tin
  - Tính toàn vẹn: kiểm tra xem bản tin có bị thay đổi không
  - Tính chống thoái thác: ngăn chặn người dùng từ chối đã tạo ra và gửi bản tin đó

Chữ ký số

Nếu chỉ dùng mã xác thực:

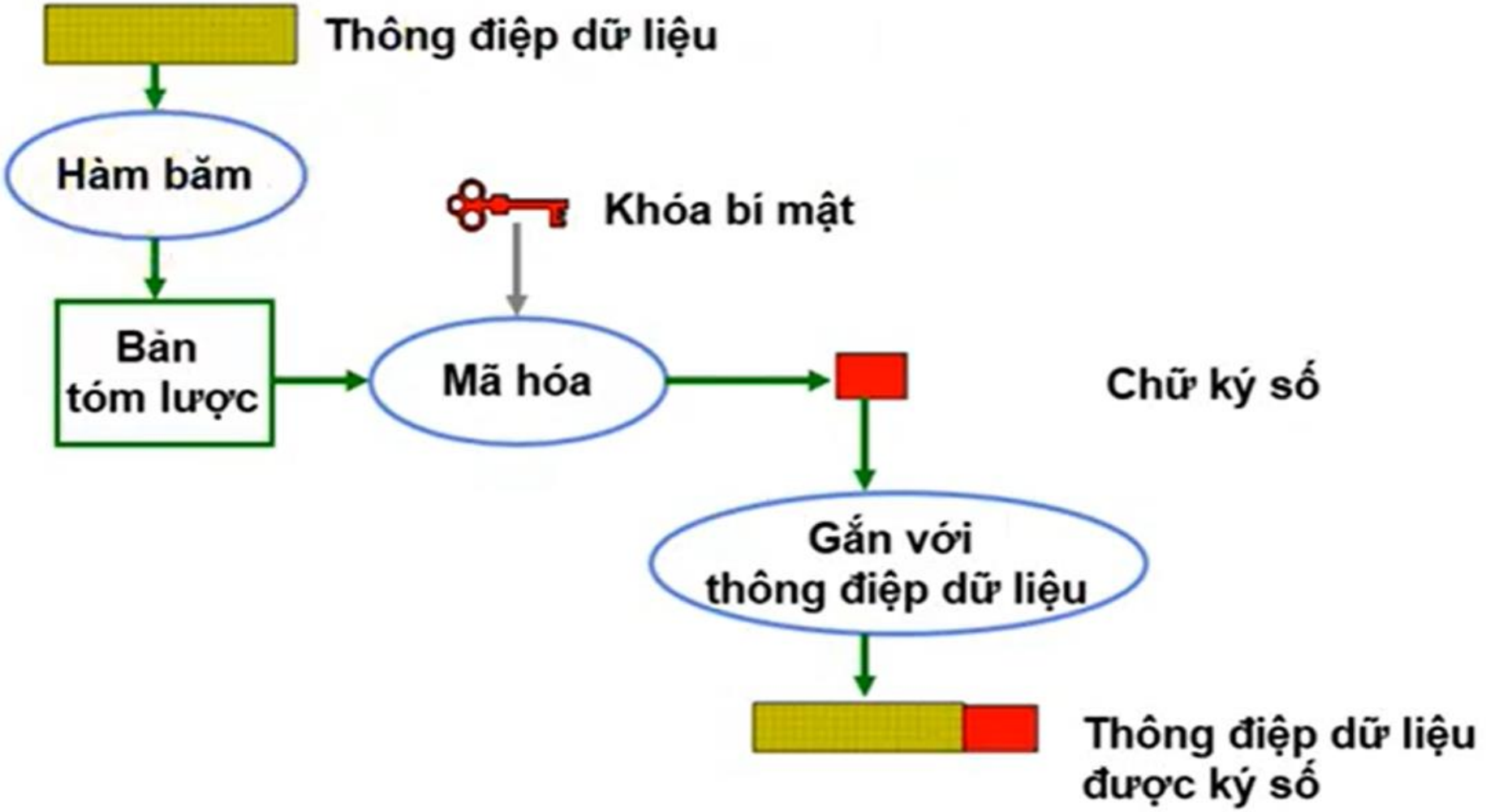
1. Chống được giả mạo của bên thứ 3
2. Không bảo vệ thông điệp bị giả mạo hay hiệu chỉnh nội dung từ 1 trong 2 bên tham gia (Từ chối trách nhiệm)

Chữ ký điện tử:

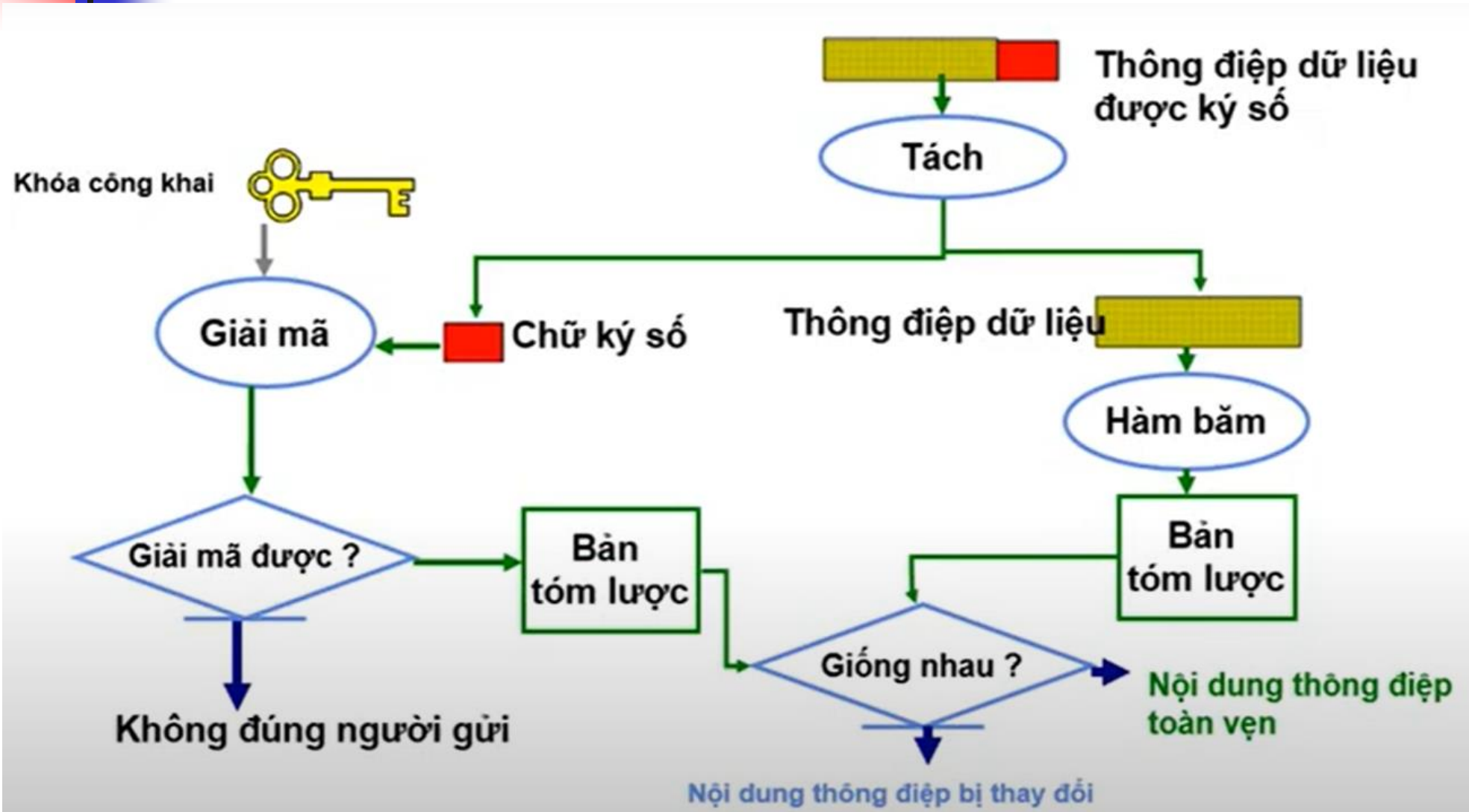
1. Có khả năng kiểm tra người ký và thời gian ký.
2. Xác thực được nội dung thông tin tại thời điểm ký.
3. Chữ ký phải được kiểm tra bởi các bên thứ ba để giải quyết tranh chấp.

- Người gửi ký tài liệu, thiết lập chủ quyền cho tài liệu
- Người nhận chứng minh được cho mọi người chính người gửi đã ký tài liệu.

Chữ ký số sử dụng hàm băm: Tạo chữ ký số



Chữ ký số: Xác thực chữ ký số



Chữ ký số

Sơ đồ chữ ký số gồm 2 hàm

- Hàm ký Sign(SK, M)
  - Đầu vào:
    - SK: Khóa cá nhân
    - M: Văn bản cần ký
  - Đầu ra: chữ ký số S
- Hàm kiểm tra: Vfy(PK, M, S)
  - Đầu vào:
    - PK: Khóa công khai
    - M, S
  - Đầu ra: True/False

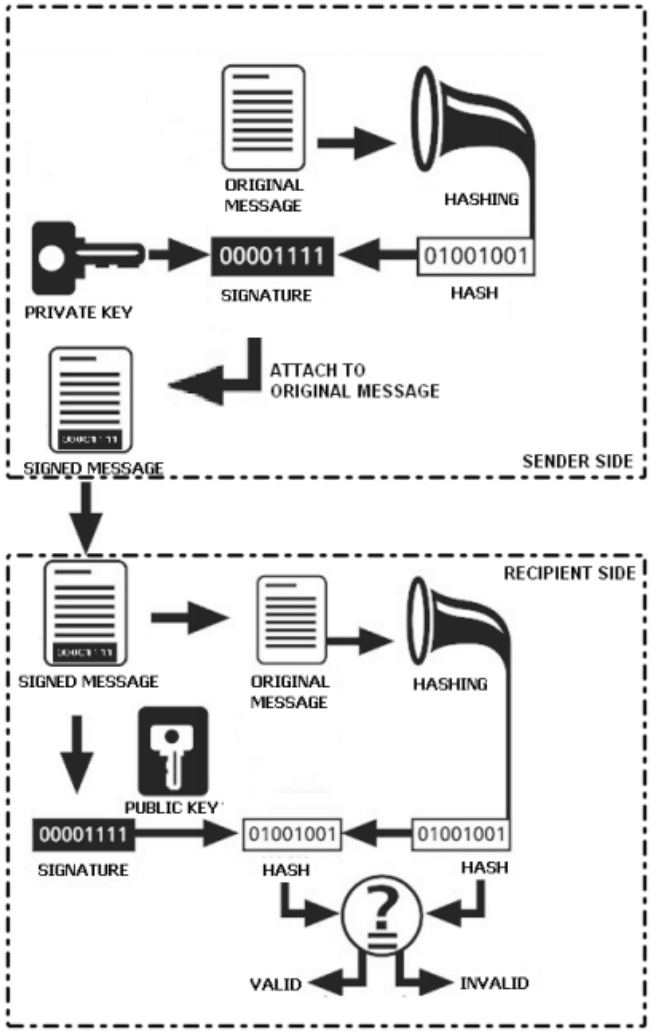
- Hàm ký phải có tính ngẫu nhiên
- Bất kỳ ai có khóa SK đều có thể tạo chữ ký

- Bất kỳ ai có khóa PK đều có thể kiểm tra chữ ký

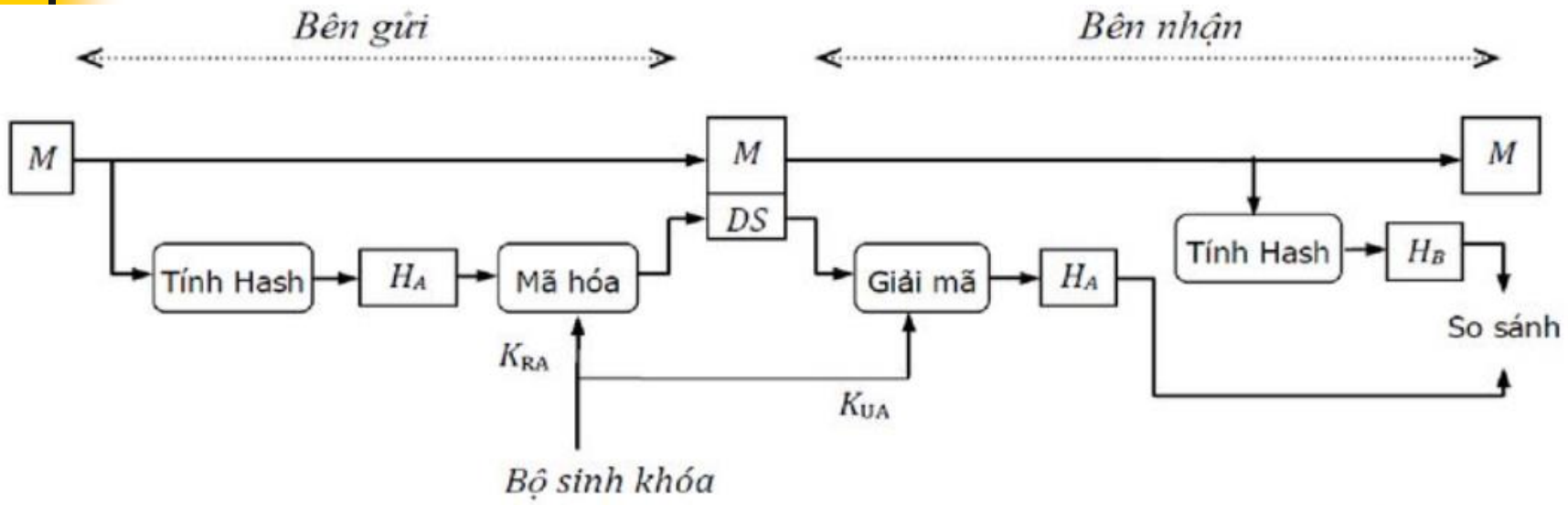
Chữ ký số

- **Phía gửi :** hàm ký
  1. Băm bản tin gốc, thu được giá trị băm H
  2. Mã hóa giá trị băm bằng khóa riêng → chữ kí số S
  3. Gắn chữ kí số lên bản tin gốc (M || S)

- **Phía nhận :** hàm xác thực
  1. Tách chữ kí số S khỏi bản tin.
  2. Băm bản tin M, thu được giá trị băm H
  3. Giải mã S với khóa công khai của người gửi, thu được H'
  4. So sánh : H' và H''. Kết luận.



Sơ đồ mô tả quá trình ký số đơn giản



DS: Data signature – chữ ký điện tử

- Trong mô hình này, Alice sau khi tính giá trị hash *HA* cho thông điệp *M* thì sẽ mã hóa *HA* bằng khóa riêng của Alice để tạo thành chữ ký điện tử *DS*. Alice gửi kèm *DS* theo *M* cho Bob.
- Bob dùng khóa công khai của Alice để giải mã chữ ký điện tử *DS* và có được giá trị hash *HA* của Alice.
- Vì Trudy không có *K*RA nên không thể sửa được HA.
- Ngoài ra, vì Alice là người duy nhất có *KRA*, nên chỉ có Alice mới có thể tạo *DS* từ *M*. Do đó Alice không thể từ chối là đã gửi bản tin.

Chữ ký số

Ưu điểm: so với chữ ký thông thường, chữ ký số có ưu thế vượt trội

- Chính xác tuyệt đối
- Kiểm định dễ dàng
- Mở đường cho các dịch vụ có độ tin cậy cao

Nhược điểm:

- Mô hình CKS chỉ đạt được nếu mỗi người sử dụng đúng 1 cặp khóa của chính mình
- Có thể xảy ra hiện tượng mạo danh người gửi. Do đó cần cơ chế xác định "ai là ai" trên toàn hệ thống

Giải pháp: Chứng thư số

Chữ kí số dựa trên RSA

Dựa trên ưu điểm của hệ mật mã RSA:

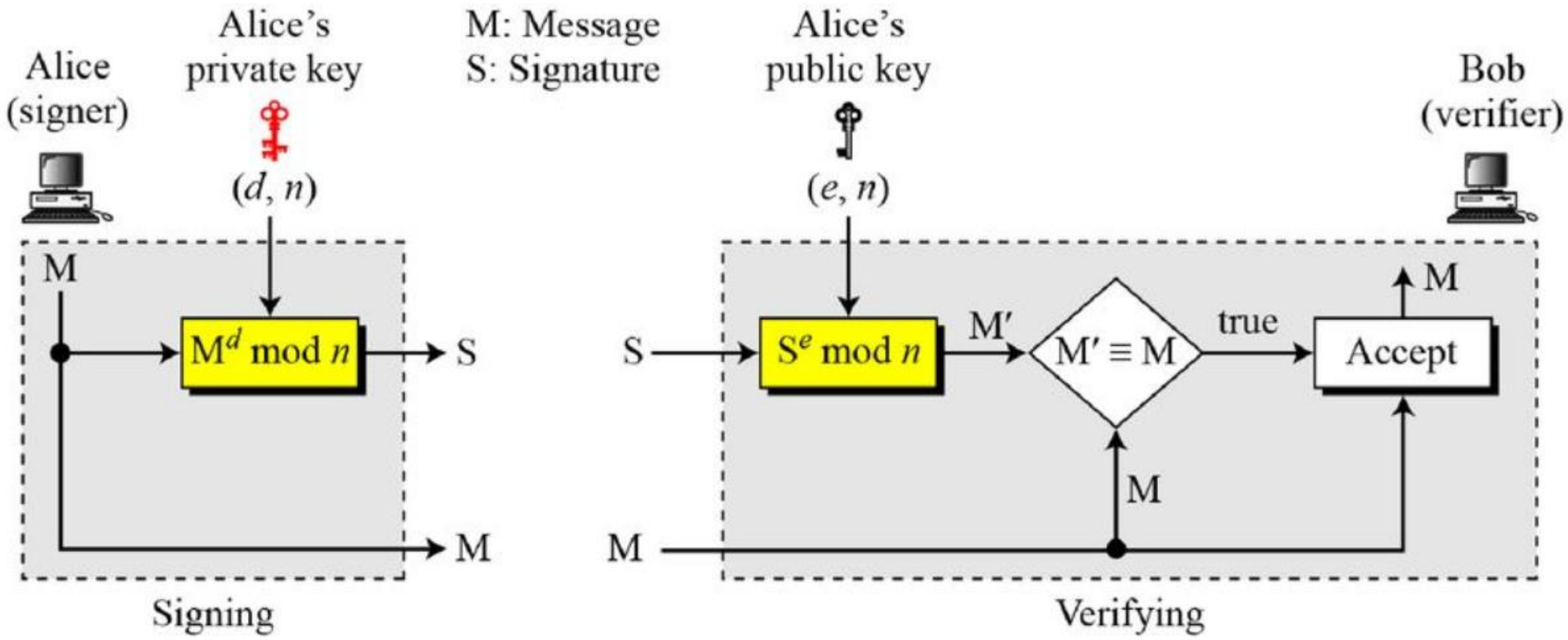
- ✓ Nếu thiết lập sơ đồ chữ ký số dựa trên bài toán phân tích ra thừa số nguyên tố thì độ an toàn của hệ thống chữ ký số này sẽ rất cao.

Thiết lập sơ đồ chữ ký số RSA đơn giản:

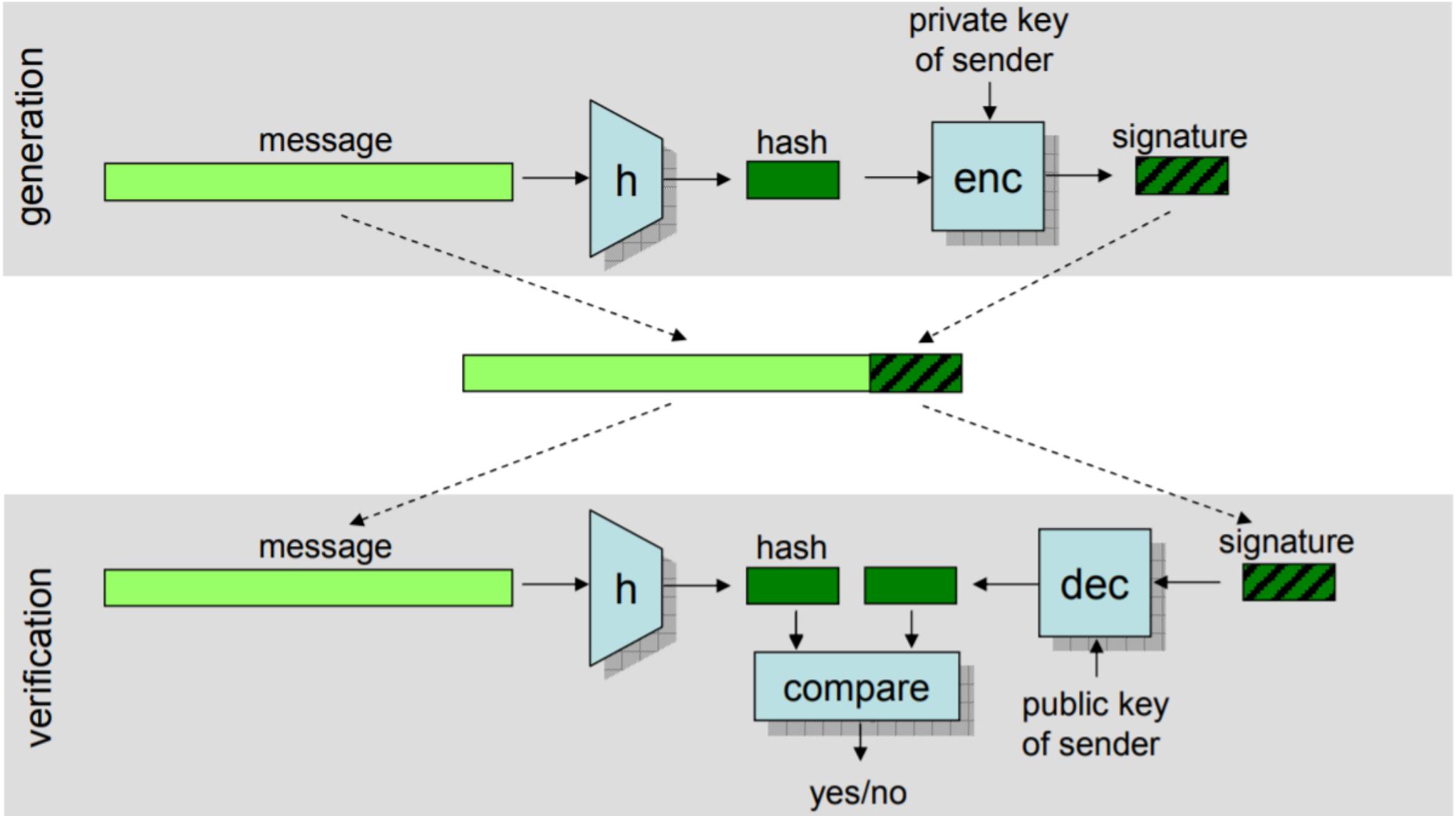
- ✓ Đảo ngược hàm mã hóa với giải mã.

Chữ kí số dựa trên RSA

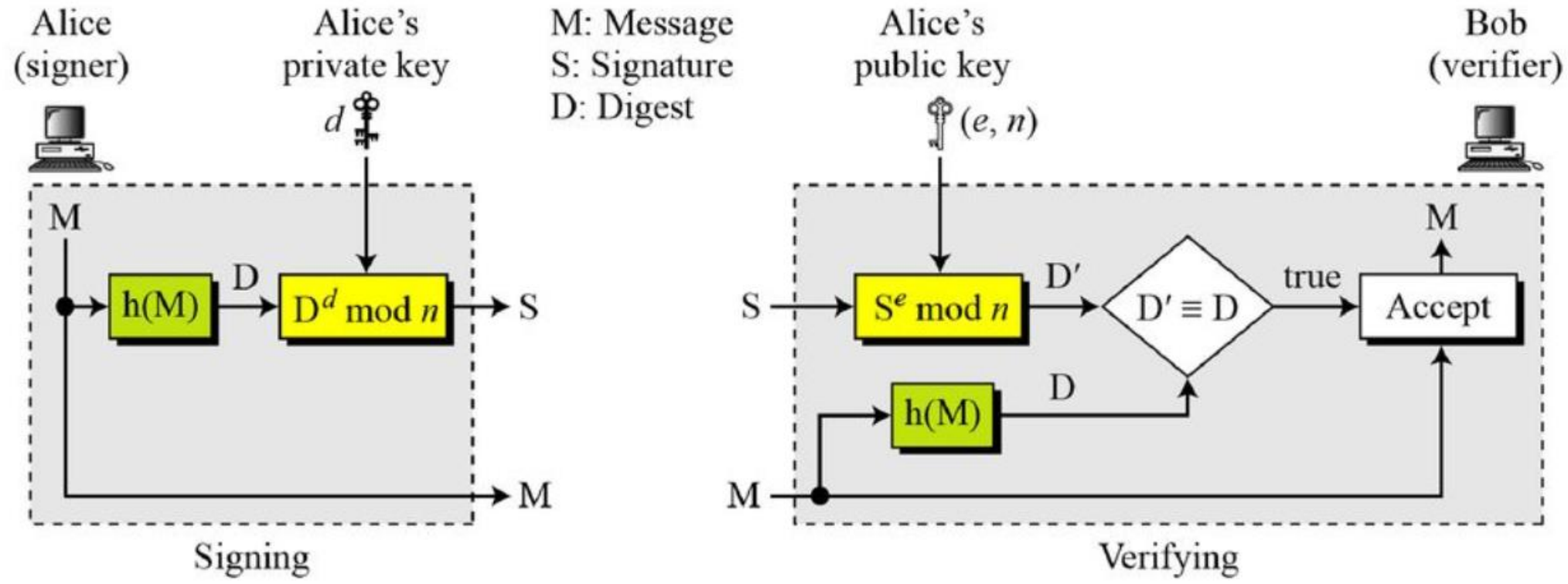
Tạo và Thẩm tra chữ ký



Chữ kí số RSA trên message digest



Chữ kí số RSA trên message digest



Bài tập chữ ký số sử dụng RSA

- Alice publishes the following data
  - $n = pq = 221$ and $e = 13$.
- Bob receives the message P = 65 and the corresponding digital signature S = 182.
- Verify the signature

Bài tập chữ ký số sử dụng RSA

- The signature is valide if
  - $P = S^e \bmod n.$
- In our case:
  - $S^e \bmod n = 182^{13} \bmod 221 = 65,$ which is valid

Digital Signature Algorithm (DSA)

Global Public-Key Components

p prime number where $2^{L-1} < p < 2^L$ for $512 \leq L \leq 1024$ and L a multiple of 64; i.e., bit length of between 512 and 1024 bits in increments of 64 bits

q prime divisor of $(p - 1)$, where $2^{N-1} < q < 2^N$ i.e., bit length of N bits

g $= h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < (p - 1)$ such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudorandom integer with $0 < x < q$

User's Public Key

$y = g^x \bmod p$

User's Per-Message Secret Number

k random or pseudorandom integer with $0 < k < q$

Signing

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1} (H(M) + xr)] \bmod q$

Signature $= (r, s)$

Verifying

$w = (s')^{-1} \bmod q$

$u_1 = [H(M')w] \bmod q$

$u_2 = (r')w \bmod q$

$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$

TEST: $v = r'$

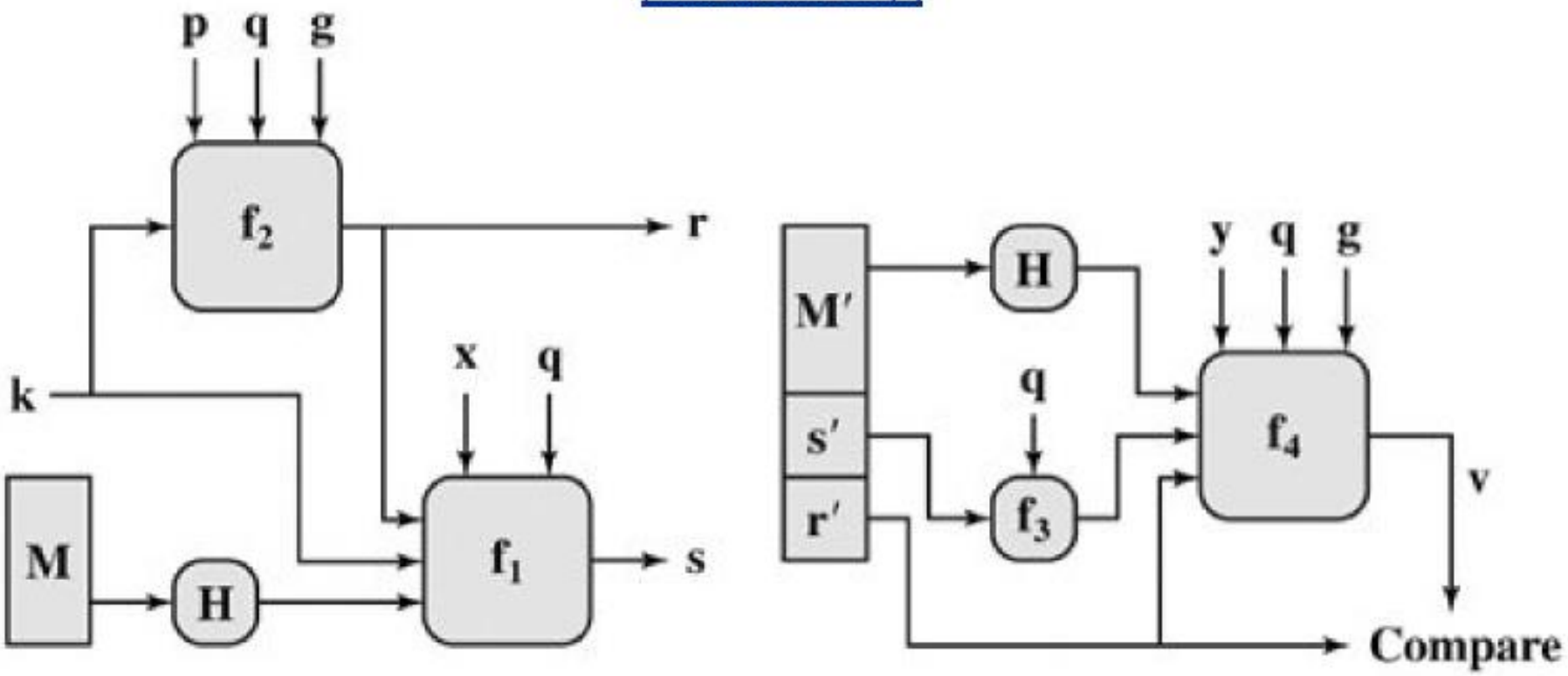
M = message to be signed

H(M) = hash of M using SHA-1

M', r', s' = received versions of M, r, s

Giải thuật DSA

[View full size image]



$s = f_1(H(M), k, x, r, q) = (k^{-1} (H(M) + xr)) \bmod q$

$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$

(a) Signing

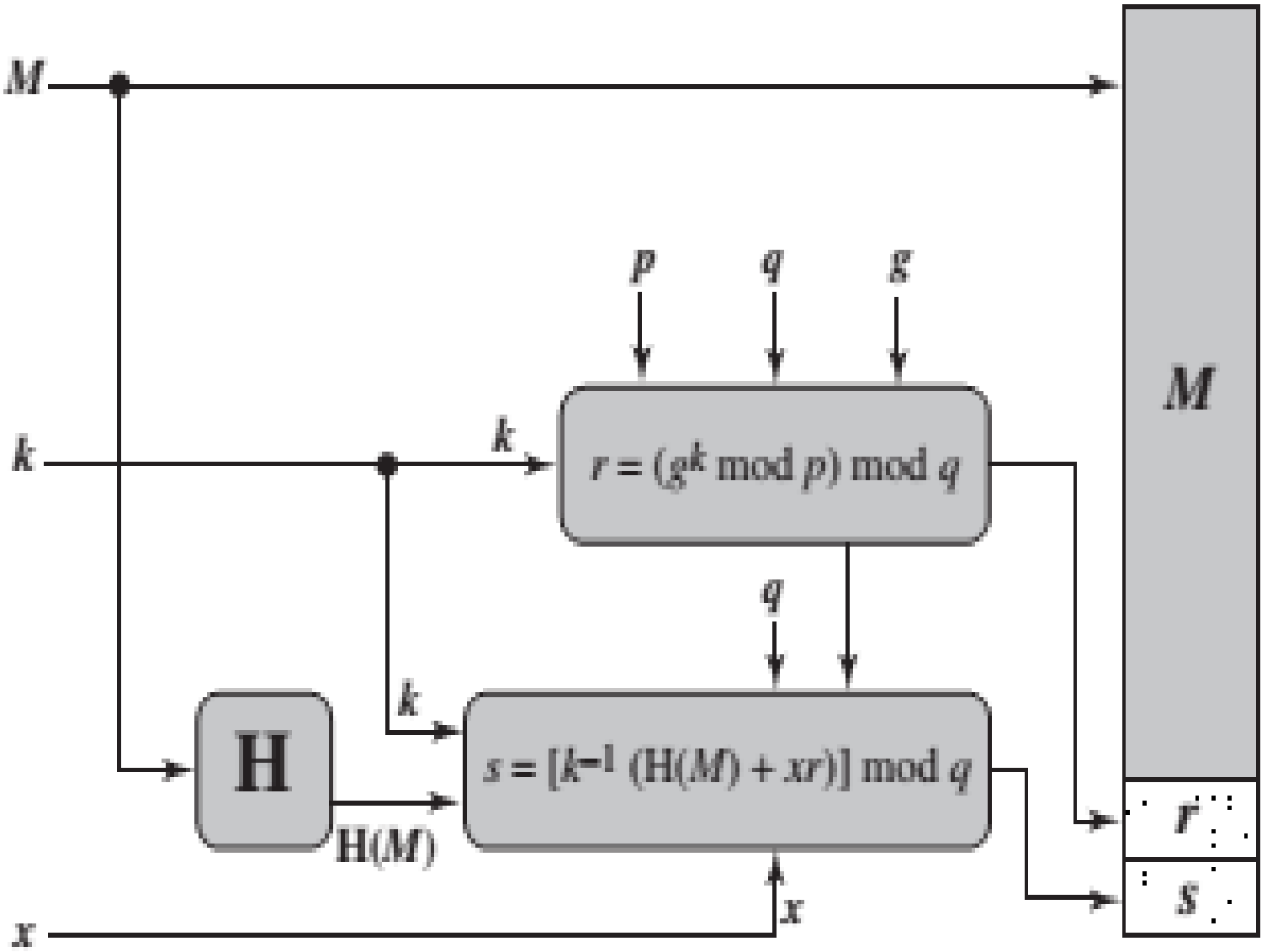
$w = f_3(s', q) = (s')^{-1} \bmod q$

$v = f_4(y, q, g, H(M'), w, r')$

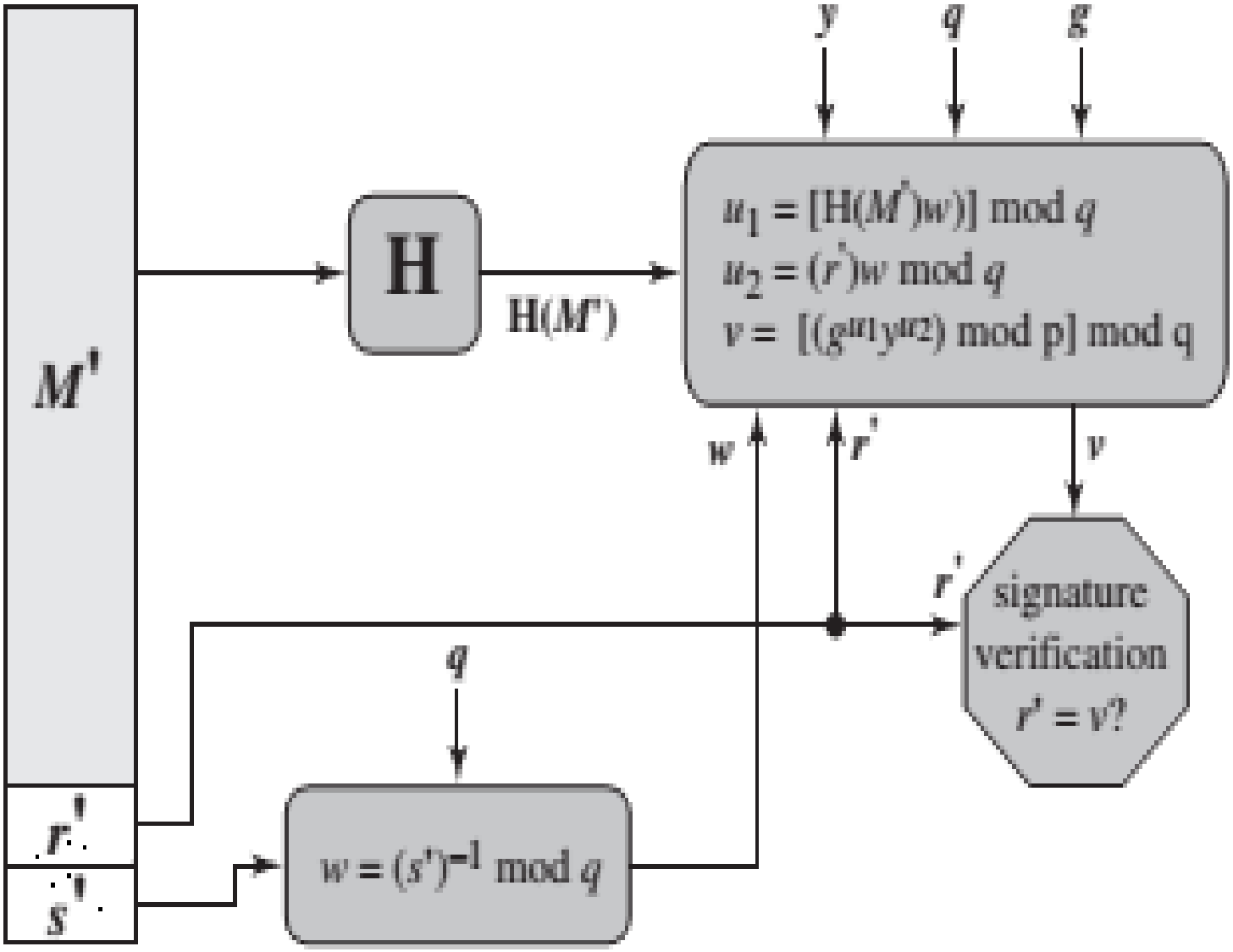
$= ((g^{(H(M')w) \bmod q} y^{r'w \bmod q}) \bmod p) \bmod q$

(b) Verifying

Giải thuật DSA - Signing



Giải thuật DSA – Verifying



Tấn công và giả mạo chữ ký số

- Dựa trên khóa công khai;
- Dựa trên các bản tin và chữ kí số;
- Dựa trên các bản tin được lựa chọn;

Tấn công, giả mạo chữ kí số:

- Phá khóa hoàn toàn: Xác định khóa riêng của người gửi;
- Giả mạo chữ kí toàn bộ: Xác định giải thuật tạo chữ kí và giả mạo chữ kí;
- Giả mạo chọn lọc: Giả mạo chữ kí số cho bản tin được chọn;
- Giả mạo chữ kí cho bản tin nào đó;

Yêu cầu của chữ ký số

- Yêu cầu 1 : Chữ ký số phải là một mẫu bít nhị phân phụ thuộc vào thông báo được ký.
- Yêu cầu 2: Chữ ký số phải dùng thông tin chỉ có đối với người gửi để tránh cả giả mạo và từ chối trách nhiệm.
- Yêu cầu 3 : Chữ ký số phải tương đối dễ được tạo ra.
- Yêu cầu 4 : Chữ ký số phải dễ được nhận ra và kiểm tra.
- Yêu cầu 5 : Chữ ký số phải không thể giả mạo được về mặt tính toán hoặc bằng cách tạo thông báo mới từ chữ ký số đã có hoặc tạo chữ ký số giả mạo cho một thông báo cụ thể.
- Yêu cầu 6 : Chữ ký số phải dễ dàng được tách ra và lưu trữ.

Chứng thư số khóa công khai

Vấn đề của khóa công khai:

- Khi A nhận được khóa công khai của B (từ Web site, e-mail, …); Làm thế nào để biết đó là khóa công khai của B, chứ không phải của người mạo danh?

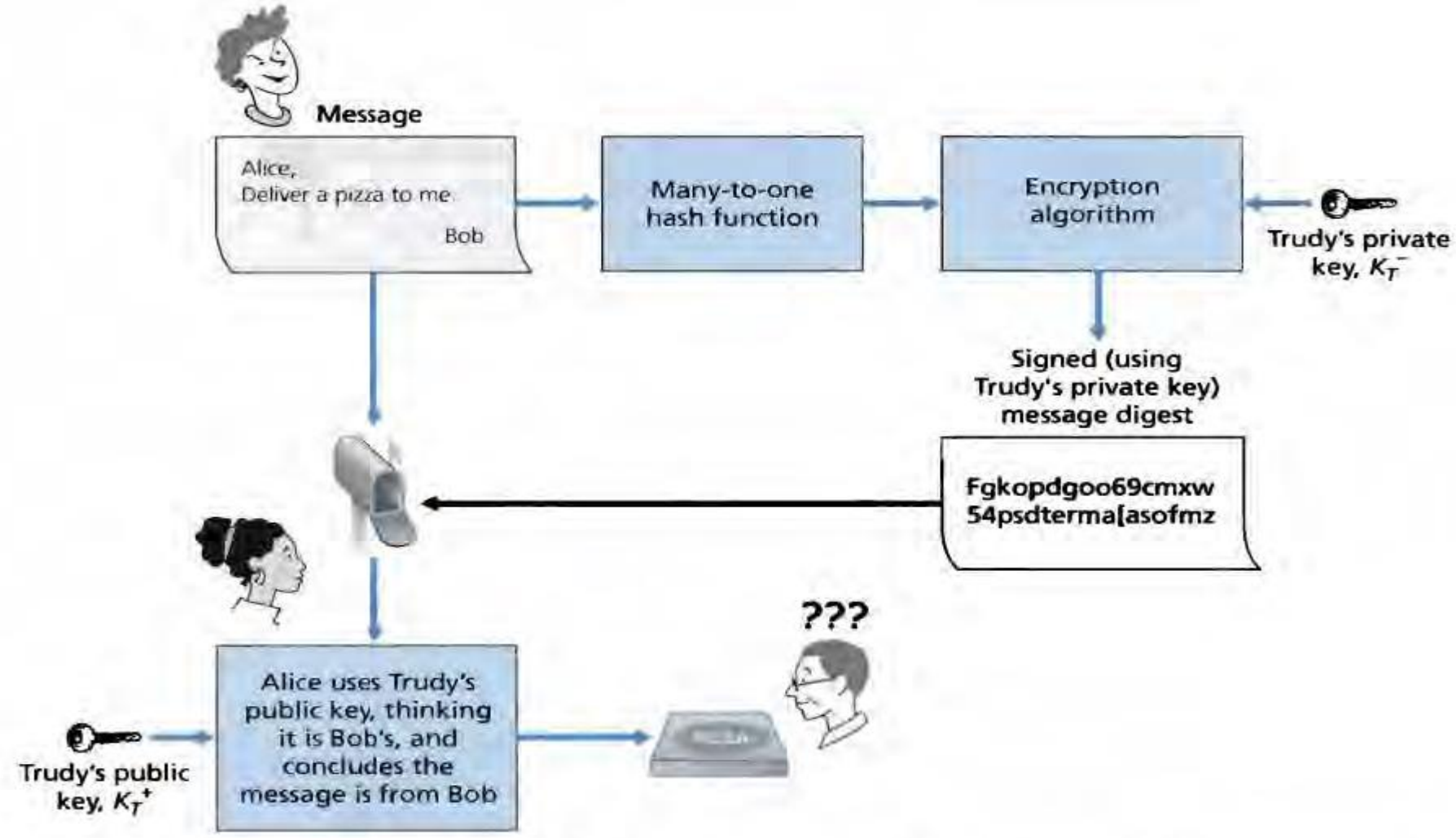
Giải pháp:

- Sử dụng chứng thư số của bên có thẩm quyền chứng thư tin cậy (trusted certification authority - CA).

Chứng thư số khóa công khai

Tại sao cần chứng thư số khóa công khai:

Giả mạo chữ ký số



Chứng thực số CA

- Certification Authority (CA): liên kết khóa công khai với thực thể cụ thể E.
- E đăng ký khóa công khai với CA.
  - E cung cấp "bằng chứng định danh" (proof of identity) cho CA.
  - CA mở chứng thư (certificate) ràng buộc E với khóa công khai của nó.
  - Chứng thư chứa khóa công khai của E được ký số bởi CA: CA thông báo "Đây chính là khóa công khai của E".

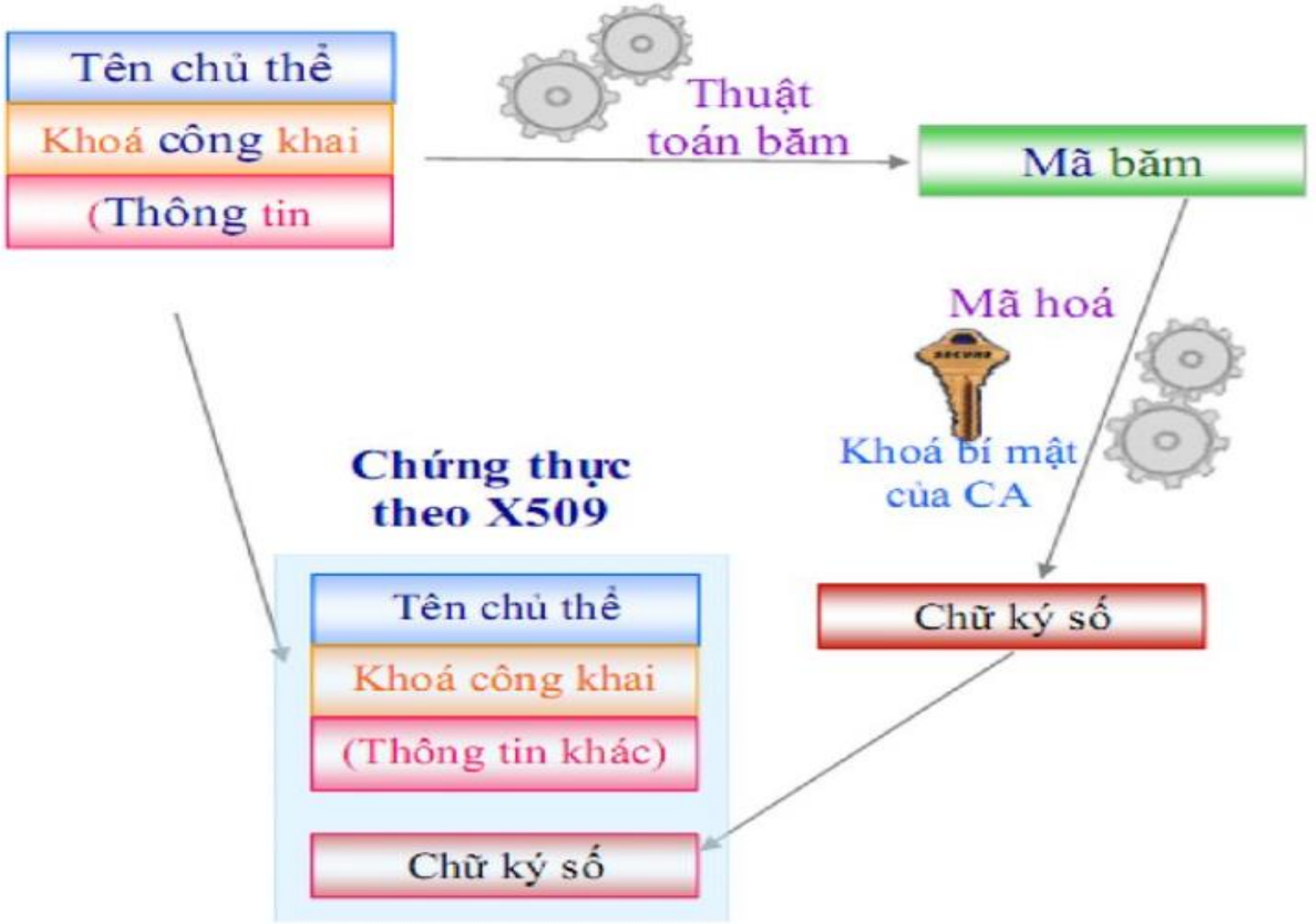
Chứng thực số

- Nội dung Chứng thư số, bao gồm:
  - Tên tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng (CA)
  - Tên của thuê bao
  - Số hiệu chứng thư số
  - Thời hạn có hiệu lực của chứng thư số
  - Khoá công khai (Public key)
  - Một số thông tin khác như: Chữ ký của CA cấp, thuật toán mã hóa,…

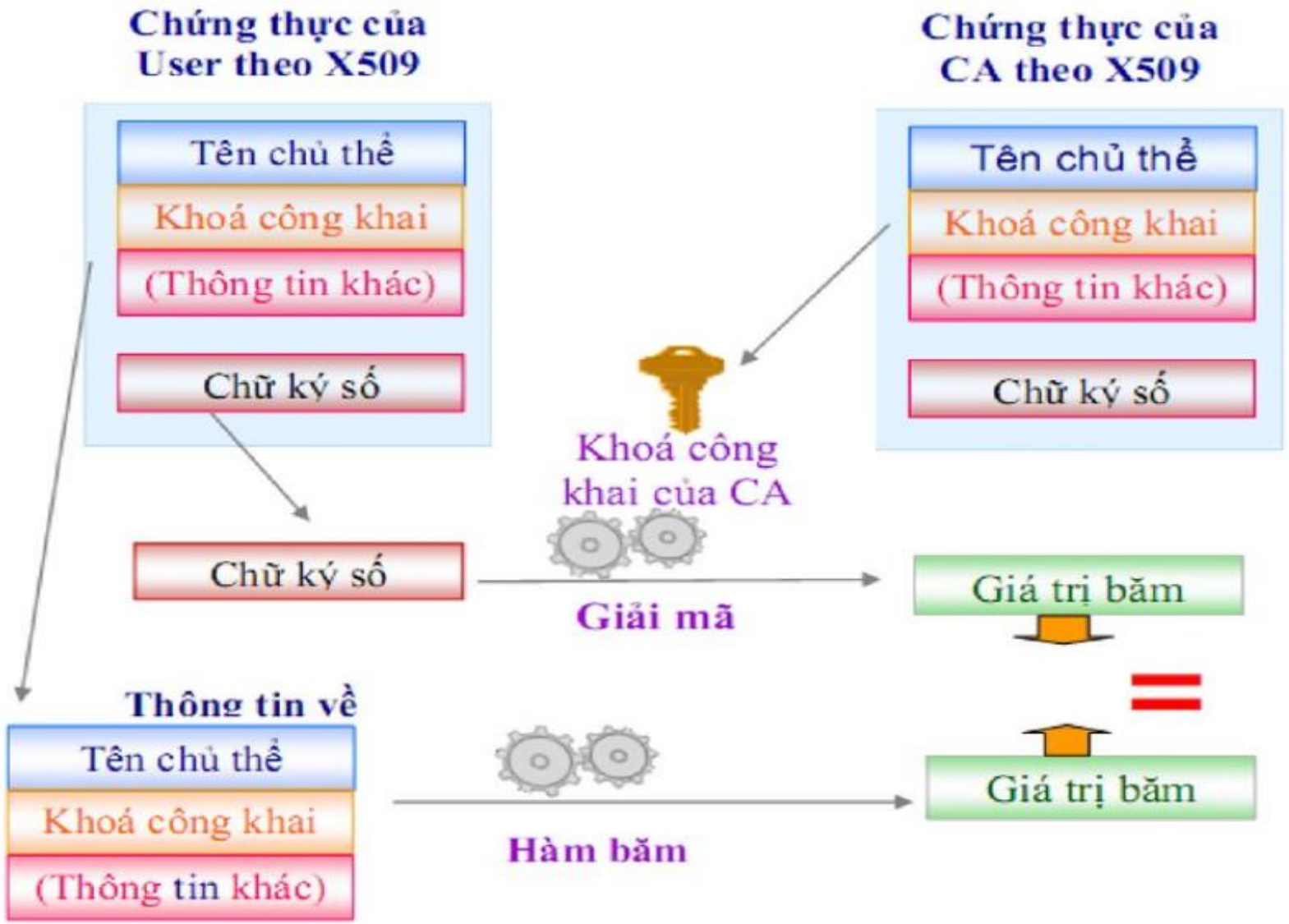
Chứng thực số

- Phân loại chứng thư số:
  - Chứng thư số cho cá nhân: Là chứng thư số được cấp cho các chức danh nhà nước, người có thẩm quyền của cơ quan, tổ chức theo quy định của pháp luật về quản lý và sử dụng con dấu, cấp cho cán bộ, công chức, viên chức trong các cơ quan nhà nước có nhu cầu giao dịch điện tử
  - Chứng thư số cho cơ quan, tổ chức: Là chứng thư số được cấp cho các cơ quan nhà nước và được giao cho người có thẩm quyền của cơ quan theo quy định của pháp luật về quản lý và sử dụng con dấu để sử dụng để ký số trên văn bản điện tử thay cho con dấu của cơ quan.
  - Chứng thư số cho thiết bị, dịch vụ, phần mềm: Là chứng thư số cấp cho các thiết bị, dịch vụ và phần mềm thuộc sở hữu, quản lý của cơ quan nhà nước

Chứng thực số: sơ đồ tạo



Chứng thực số: sơ đồ kiểm tra



The Big Picture

	Secret Key Setting	Public Key Setting
Secrecy / Confidentiality	Stream ciphers Block ciphers + encryption modes	Public key encryption: RSA, El Gamal, etc.
Authenticity / Integrity	Message Authentication Code	Digital Signatures: RSA, DSA, etc.