

# Chữ ký điện tử

BỘ GIÁO DỤC VÀ ĐÀO TẠO  
TRƯỜNG ĐẠI HỌC SƯ PHẠM HÀ NỘI

Số: 141 /DHSPHN-SDH  
V/v thông báo nhập học cao học khóa 2011-2013 (K21)

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 17 tháng 2 năm 2012

### THÔNG BÁO NHẬP HỌC

Cao học khóa 2011 – 2013 (tại Trường Đại học Cần Thơ)

Thi hành “Quy chế đào tạo trình độ thạc sĩ” của Bộ trưởng Bộ GD&ĐT (Thông tư số: 10/2011/QĐ-BGDDT ngày 28/2/2011), Trường Đại học Sư phạm Hà Nội thông báo như sau:

1. Anh (chị) đã được Hiệu trưởng Trường Đại học Sư phạm Hà Nội công nhận trúng tuyển cao học khóa 2011-2013 (K21), hệ đào tạo chính quy tập trung theo quyết định trúng tuyển số: 3383/QĐ-ĐHSPHN ngày 5/10/2011.

2. Ngày nhập học: 8 giờ 00', ngày 6 tháng 3 năm 2012 (Thứ ba), tại Trường ĐH Cần Thơ

3. Học viên tự sắp xếp nơi ở trong quá trình đào tạo.

4. Các khoản học viên phải đóng góp: 40.023.000 đồng, trong đó:

4.1. Kinh phí đào tạo: 14.625.000 đồng

4.2. Kinh phí do tổ chức

5. Thời gian nộp kinh phí

Trường Đại học Sư phạm Hà Nội  
biên lai tài chính cho học viên

- Đợt 1, ngày 6/3/2012

- Đợt 2, ngày 29/6/2012 (ngày thi hết chuyên đề đợt 1): 20.023.000 đồng

6. Thủ tục đăng ký nhập học gồm:

- Quyết định cử đi học của Thủ trưởng cơ quan quản lý;

- 02 ảnh 4 x 6;

- Thủ tục nhập học: 100.000đ;

- Thẻ học viên, thẻ thư viện: 50.000đ.

Lưu ý: Sau 15 ngày kể từ ngày nhập học nếu anh (chị) không có mặt và không liên hệ với cơ sở đào tạo sẽ xem như anh (chị) bỏ không đăng ký theo khóa học.

Có gì chưa rõ, học viên liên hệ với Phòng Sau đại học, Trường ĐHSP Hà Nội, điện thoại: 043.7547823, máy lẻ 427; 0982.022.306 - chuyên viên: Đặng Ngọc Phúc; Trường ĐH Cần Thơ, Nguyễn Hữu Giao Tiên: 0907.289.008).

KT, HIỆU TRƯỞNG  
PHÓ HIỆU TRƯỞNG



PGS.TS Trần Văn Ba

BỘ GIÁO DỤC VÀ ĐÀO TẠO  
TRƯỜNG ĐẠI HỌC SƯ PHẠM HÀ NỘI

Số: 141 /DHSPHN-SDH  
V/v thông báo nhập học cao học khóa 2011-2013 (K21)

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 17 tháng 2 năm 2012

### THÔNG BÁO NHẬP HỌC

Cao học khóa 2011 – 2013 (tại Trường Đại học Cần Thơ)

Thi hành “Quy chế đào tạo trình độ thạc sĩ” của Bộ trưởng Bộ GD&ĐT (Thông tư số: 10/2011/QĐ-BGDDT ngày 28/2/2011), Trường Đại học Sư phạm Hà Nội thông báo như sau:

1. Anh (chị) đã được Hiệu trưởng Trường Đại học Sư phạm Hà Nội công nhận trúng tuyển cao học khóa 2011-2013 (K21), hệ đào tạo chính quy tập trung theo quyết định trúng tuyển số: 3383/QĐ-ĐHSPHN ngày 5/10/2011.

2. Ngày nhập học: 8 giờ 00', ngày 6 tháng 3 năm 2012 (Thứ ba), tại Trường ĐH Cần Thơ

3. Học viên tự sắp xếp nơi ở trong quá trình đào tạo.

4. Các khoản học viên phải đóng góp: 40.023.000 đồng, trong đó:

4.1. Kinh phí đào tạo: 14.625.000 đồng

00 đồng  
ong ĐH Cần Thơ  
u trực tiếp và cấp  
g

- Đợt 2, ngày 29/6/2012 (ngày thi hết chuyên đề đợt 1): 20.023.000 đồng

6. Thủ tục đăng ký nhập học gồm:

- Quyết định cử đi học của Thủ trưởng cơ quan quản lý;

- 02 ảnh 4 x 6;

- Thủ tục nhập học: 100.000đ;

- Thẻ học viên, thẻ thư viện: 50.000đ.

Lưu ý: Sau 15 ngày kể từ ngày nhập học nếu anh (chị) không có mặt và không liên hệ với cơ sở đào tạo sẽ xem như anh (chị) bỏ không đăng ký theo khóa học.

Có gì chưa rõ, học viên liên hệ với Phòng Sau đại học, Trường ĐHSP Hà Nội, điện thoại: 043.7547823, máy lẻ 427; 0982.022.306 - chuyên viên: Đặng Ngọc Phúc; Trường ĐH Cần Thơ, Nguyễn Hữu Giao Tiên: 0907.289.008).

KT, HIỆU TRƯỞNG  
PHÓ HIỆU TRƯỞNG

PGS.TS Trần Văn Ba

# Chữ ký viết tay

BỘ GIÁO DỤC VÀ ĐÀO TẠO TRƯỜNG ĐẠI HỌC SƯ PHẠM HÀ NỘI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 141 /DHSPHN-SĐH V/v thông báo nhập học cao học khóa 2011-2013 (K21)	Hà Nội, ngày 17 tháng 2 năm 2012
<b>THÔNG BÁO NHẬP HỌC</b> Cao học khóa 2011 – 2013 (tại Trường Đại học Cần Thơ)	
Thi hành “Quy chế đào tạo trình độ thạc sĩ” của Bộ trưởng Bộ GD&ĐT (Thông tư số: 10/2011/QĐ-BGĐĐT ngày 28/2/2011), Trường Đại học Sư phạm Hà Nội thông báo như sau:	
1. Anh (chị) đã được Hiệu trưởng Trường Đại học Sư phạm Hà Nội công nhận trúng tuyển cao học khóa 2011-2013 (K21), hệ đào tạo chính quy, tập trung theo quyết định trúng tuyển số: 3383/QĐ-ĐHSPHN ngày 5/10/2011.	
2. Ngày nhập học: 8 giờ 00', ngày 6 tháng 3 năm 2012 (Thứ ba), tại Trường ĐH Cần Thơ	
3. Học viên tự sắp xếp nơi ở trong quá trình đào tạo.	
4. Các khoản học viên phải đóng góp: 40.023.000 đồng, trong đó:	
4.1. Kinh phí đào tạo: 14.625.000 đồng	
4.2. Kinh phí do tổ chức lớp học tại Trường Đại học Cần Thơ: 25.398.000 đồng	
5. Thời gian nộp kinh phí đào tạo và kinh phí do tổ chức lớp học tại Trường ĐH Cần Thơ	
Trường Đại học Sư phạm Hà Nội cử cán bộ đến Trường Đại học Cần Thơ thu trực tiếp và cấp biên lai tài chính cho học viên trong 2 đợt vào các ngày:	
- Đợt 1, ngày 6/3/2012 (ngày nhập học): 20.000.000 đồng	
- Đợt 2, ngày 29/6/2012 (ngày thi hết chung kết đợt 1): 20.023.000 đồng	
6. Thủ tục đăng ký nhập học gồm:	
- Quyết định cử đi học của Thủ trưởng cơ quan quản lý;	
- 02 ảnh 4 x 6;	
- Thủ tục nhập học: 100.000đ;	
- Thẻ học viên, thẻ thư viện: 50.000đ.	
<i>Lưu ý: Sau 15 ngày kể từ ngày nhập học nếu anh (chị) không có mặt và không liên hệ với cơ sở đào tạo sẽ xem như anh (chị) bỏ không đăng ký theo khóa học.</i>	
<i>Có gì chưa rõ, học viên liên hệ với Phòng Sau đại học, Trường ĐHSP Hà Nội, điện thoại: 043.7547823, máy lẻ 427; 0982.022.306 - chuyên viên: Đặng Ngọc Phúc; Trường ĐH Cần Thơ, Nguyễn Hữu Giao Tiên: 0907.289.008.</i>	
KT. HIEU TRƯỞNG PHÓ HIEU TRƯỞNG	
	
PGS.TS Trần Văn Ba	

## 1. Xác minh người tạo ra chữ ký

## 2. Xác thực nội dung được ký



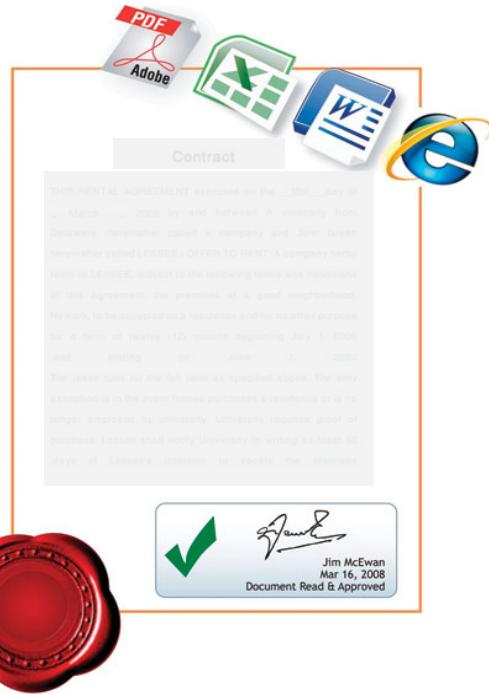
Làm thế nào để định nghĩa một chữ ký cho các văn bản số, với các tính chất tương tự như chữ ký viết tay ?

# Chữ ký số và hàm băm

# Nội dung

- Chữ ký số
  - Yêu cầu
  - Tính chất
  - Mô hình
  - Chữ ký số dựa trên mật mã khóa công khai
- Hàm băm
  - Định nghĩa
  - Tính chất
  - Ứng dụng vào chữ ký số

# Chữ ký số



# Yêu cầu của chữ ký số

- Xác thực nội dung được ký
  - Không thể thay đổi
  - Không thể dùng lại
- Xác minh người tạo ra chữ ký

# Yêu cầu của chữ ký số

- Xác thực nội dung được ký
  - Không thể thay đổi
    - Không thể thay đổi nội dung của bản tin đã được ký
  - Không thể dùng lại
- Xác minh người tạo ra chữ ký

# Yêu cầu của chữ ký số

- Xác thực nội dung được ký
  - Không thể thay đổi
  - Không thể dùng lại
    - Không thể dùng lại chữ ký cho 1 bản tin khác
- Xác minh người tạo ra chữ ký

# Yêu cầu của chữ ký số

- Xác thực nội dung được ký
  - Không thể thay đổi
  - Không thể dùng lại
- Xác minh người tạo ra chữ ký
  - Không thể làm giả
  - Không thể từ chối

# Yêu cầu của chữ ký số

- Xác thực nội dung được ký
  - Không thể thay đổi
  - Không thể dùng lại
- Xác minh người tạo ra chữ ký
  - Không thể làm giả
    - A không thể giả mạo chữ ký của B
  - Không thể từ chối

# Yêu cầu của chữ ký số

- Xác thực nội dung được ký
  - Không thể thay đổi
  - Không thể dùng lại
- Xác minh người tạo ra chữ ký
  - Không thể làm giả
  - Không thể từ chối
    - Nếu A đã ký thì sau đó A không thể chối bỏ là đã ký

# Tính chất 1

- Là một chuỗi ký tự, có nội dung phụ thuộc vào nội dung bản tin được ký

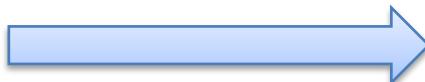


Bản tin



hQImaw9dfDAW  
EPmj9h87onwe1j  
d03nDFo

Chữ ký

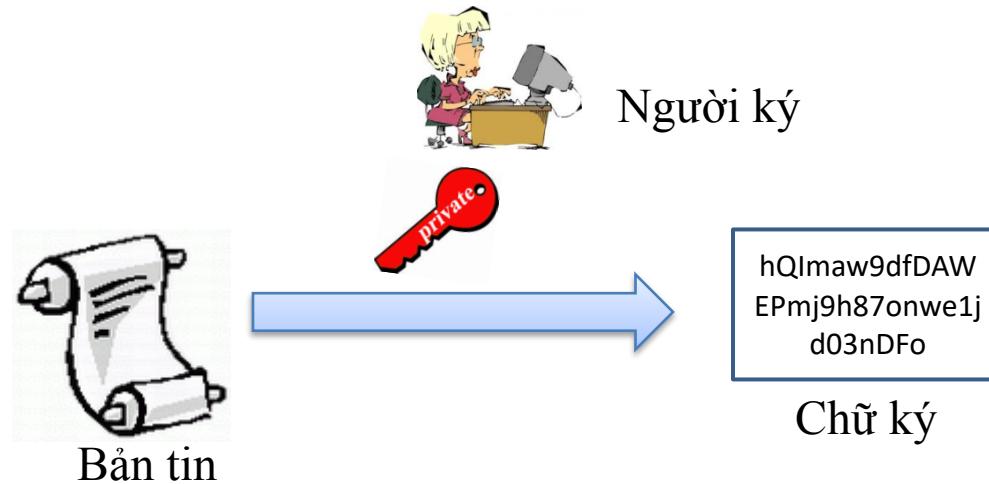


12khmlik0jh72nu  
8om

- ✓ khó thay đổi
  - ✓ khó dùng lại
- ⇒ Xác thực nội dung bản tin được ký

# Tính chất 2

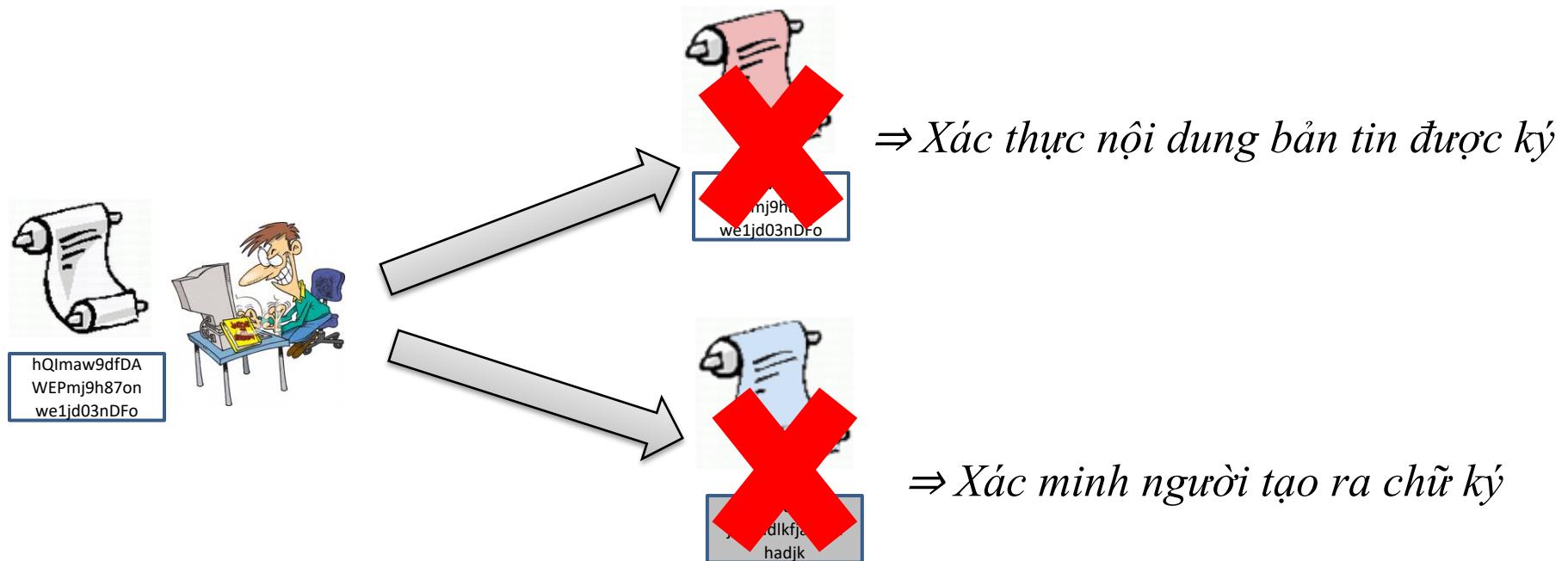
- Sử dụng thông tin mà chỉ có người ký mới có



- ✓ khó giả mạo
  - ✓ khó chối từ
- ⇒ Xác minh người tạo ra chữ ký

# Tính chất 3

- Gần như không thể giả mạo chữ ký



# So sánh chữ ký viết tay và chữ ký số

Chữ ký viết tay	Chữ ký số
Chữ ký cố định	Chữ ký thay đổi theo nội dung được ký
Gắn liền với nội dung được ký	Có thể tách khỏi nội dung được ký

# Mô hình



$S_A$  : Hàm sinh chữ ký

$(m)$

Chào B, tôi là A.  
Dưới đây là  
thông tin cá  
nhân của tôi:

$S_A(m) = s$

Người ký A

$(s)$

hQImaw9dfDA  
WEPmj9h87on  
we1jd03n

Chào B, tôi là A.  
Dưới đây là  
thông tin cá  
nhân của tôi:  
hQImaw9dfDA  
WEPmj9h87on  
we1jd03n

**true:**

- + nội dung không bị thay đổi
- + chữ ký không bị giả mạo

**false:**

Nội dung không bị thay đổi  
hoặc chữ ký không bị giả mạo

$V_A(m, s)$

Chào B, tôi là A.  
Dưới đây là  
thông tin cá  
nhân của tôi:

hQImaw9dfDA  
WEPmj9h87on  
we1jd03n

Chào B, tôi là A.  
Dưới đây là  
thông tin cá  
nhân của tôi:  
hQImaw9dfDA  
WEPmj9h87on  
we1jd03n

Hàm xác nhận chữ ký:  $V_A$



Người xác minh B

# Yêu cầu

- $S_A$  là hàm bí mật ;  $V_A$  là hàm công khai
- $V_A(m, s) = \text{true}$  nếu và chỉ nếu  $S_A(m) = s$

# Nhắc lại về mật mã khóa công khai



Chủ thẻ A



Khóa bí mật  $pr_A$

Khóa công khai  $pb_A$

$E$ : Thuật toán mã hóa/giải mã

*Tính đối hợp*

$$m = E_{pr_A} \left( E_{pb_A} (m) \right) = E_{pb_A} \left( E_{pr_A} (m) \right)$$

# Chữ ký số dựa trên mật mã khóa công khai

- Sinh chữ ký

$$s = E_{pr_A}(m)$$

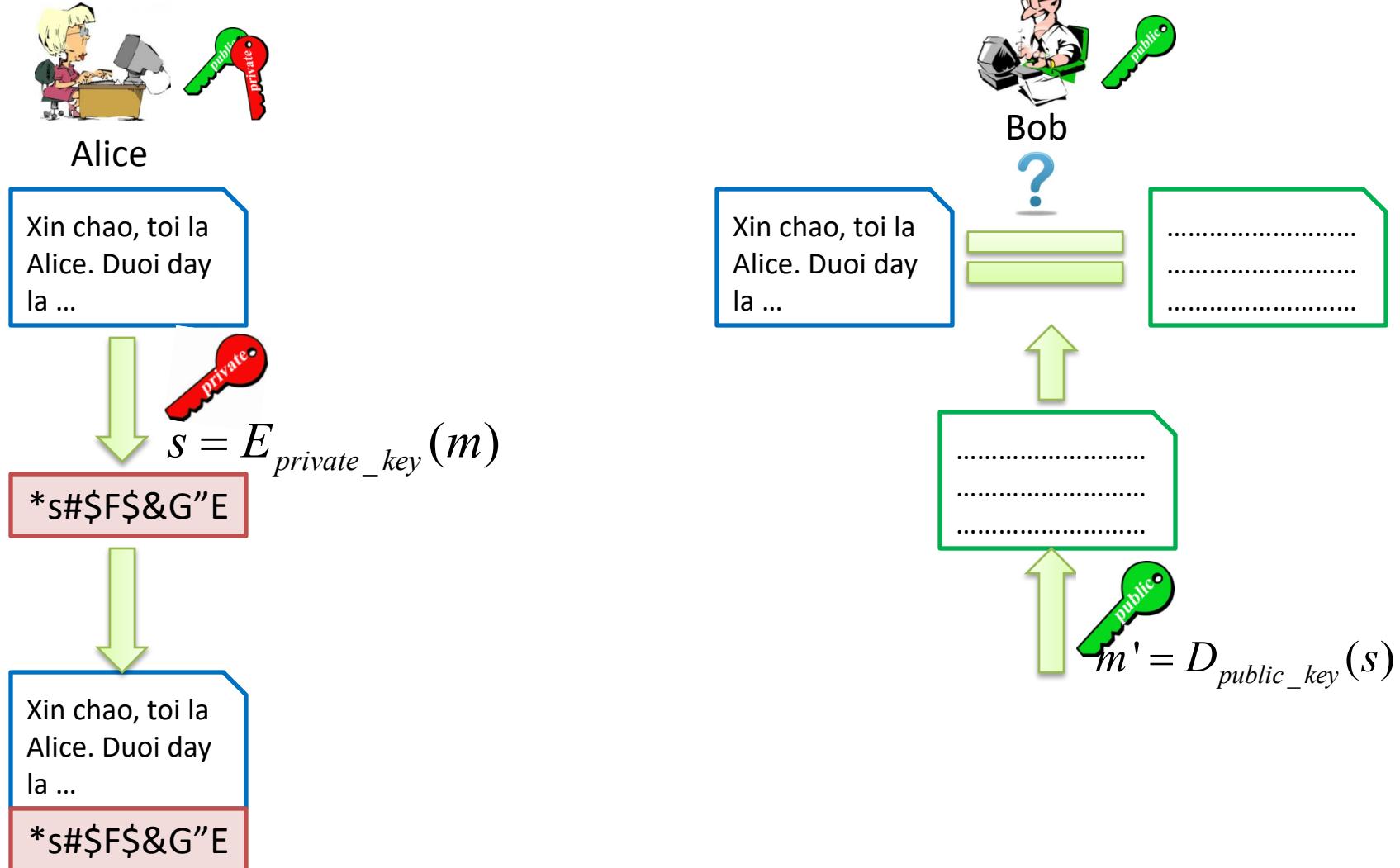
$pr_A$  : Khóa bí mật của A

- Xác minh chữ ký

$$D_{pb_A} \text{ eq } m = \begin{cases} \text{true, if } D_{pb_A}(s) = m \\ \text{false, if } D_{pb_A}(s) \neq m \end{cases}$$

$pb_A$  : Khóa công khai của A

# Chữ ký số dựa trên mật mã khóa công khai



- Tài liệu tham khảo
  - William Stallings, “*Cryptography and network security principles and practices*”, fourth edition, Prentice Hall, 2005
- Bài tập
  - Tìm hiểu các hệ chữ ký khác

# Vấn đề

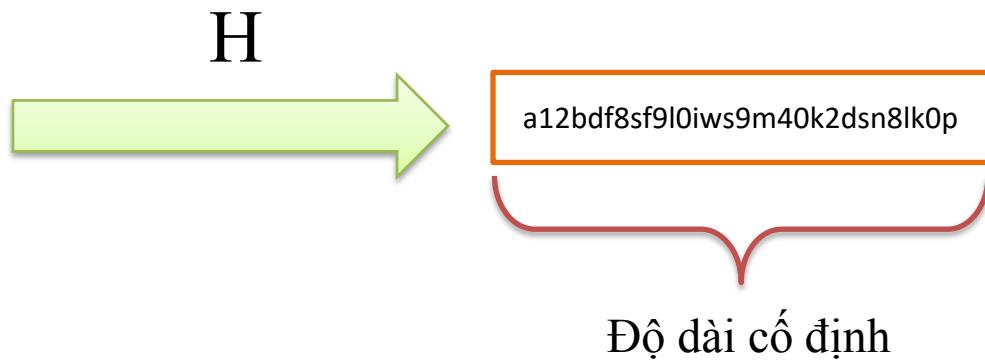
- Tốc độ chậm
- Kích thước chữ ký lớn
- Vấn đề với bản tin quá dài
  - ⇒ chia thành nhiều bản tin nhỏ và ký trên từng bản tin nhỏ
  - ⇒ tần công: thay đổi thứ tự, thêm bớt các bản tin nhỏ

# Hàm băm

# Định nghĩa

- Là hàm biến đổi một chuỗi ký tự có độ dài bất kỳ thành một chuỗi ký tự có độ dài cố định
  - $m$ : bản tin
  - $n = H(m)$  : giá trị băm của  $m$  (*message digest, hash code*)

A digital signature is another means to ensure integrity, authenticity, and non-repudiation. A digital signature is derived by applying a mathematical function to compute the message digest of an electronic message or document, and then encrypt the result of the computation with the signer's private key. Recipients can verify the digital signature with the use of the sender's public key. A digital signature is another means to ensure integrity, authenticity,



# Tính chất

- *Tính kiểm tra lỗi:*
  - Thay đổi 1 bit bất kỳ của bản tin đầu vào sẽ thay đổi hoàn toàn giá trị đầu ra

Message: "A hungry brown fox jumped over a lazy dog"

SHA1 hash code: a8e7038cf5042232ce4a2f582640f2aa5caf12d2

Message: "A hungry brown fox jumped over a lazy dog"

SHA1 hash code: d617ba80a8bc883c1c3870af12a516c4a30f8fda

# Tính chất

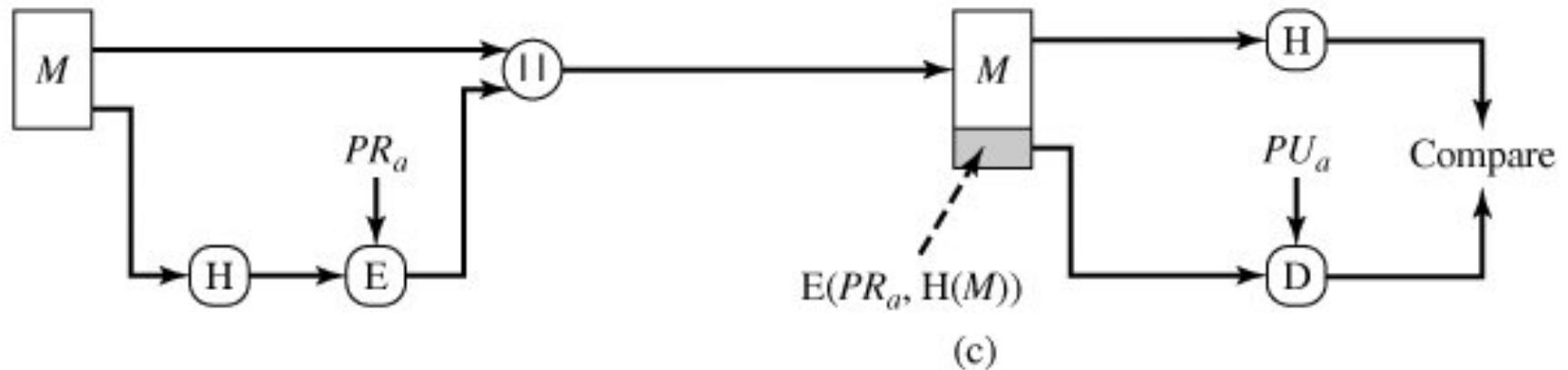
- *Tính một chiều:*
  - Biết giá trị hàm băm  $\Rightarrow$  gần như không thể suy ngược giá trị bản tin
- *Tính không trùng lặp:*
  - Với bản tin X cho trước  $\Rightarrow$  gần như không thể tìm được Y sao cho  $H(x) = H(y)$ 
    - *Tính không trùng lặp yếu*
  - Gần như không thể tìm được  $(X, Y)$  sao cho  $H(x) = H(y)$ 
    - *Tính không trùng lặp mạnh*

# Chữ ký số với hàm băm

- Ý tưởng chính
  - Ký trên giá trị hàm băm
- Sinh chữ ký
- Xác minh chữ ký

$$s = E_{pr_A}(H(m))$$
$$D_{pb_A} \text{ eq } H(m) = \begin{cases} \text{true, if } D_{pb_A}(s) = H(m) \\ \text{false, if } D_{pb_A}(s) \neq H(m) \end{cases}$$

# Chữ ký số với hàm băm



# Bài tập về nhà

- Tìm hiểu trước
  - Cơ chế tạo hàm băm
  - Các tấn công vào hàm băm
    - Nghịch lý ngày sinh
- Tài liệu tham khảo
  - William Stallings, “*Cryptography and network security principles and practices*”, fourth edition, Prentice Hall, 2005.



# Mô hình

- Ký hiệu
  - Tập các bản tin,  $M$
  - Tập các chữ ký,  $S$ : Là các chuỗi  $s \in \{0,1\}^n$
- Hàm sinh chữ ký:  $S_A : M \rightarrow S$ 
  - Với mỗi  $m \in M : S_A(m) = s \in S$
- Hàm xác minh chữ ký:  $V_A : M \times S \rightarrow \{true, false\}$   
$$V_A(m, s) = true \text{ nếu và chỉ nếu } S_A(m) = s$$

# Cơ chế

- Sinh chữ ký
  - Tạo chữ ký  $s = S_A(m)$
  - Gắn chữ ký vào văn bản gốc:  $(m, s)$
- Xác minh chữ ký
  - Lấy hàm xác minh  $V_A$  bằng một cách nào đó
  - Tính  $V_A(m, s)$ 
    - Nếu  $V_A(m, s) = true$  : chữ ký đúng
    - Nếu  $V_A(m, s) = false$  : chữ ký sai