Chữ ký số và hàm băm

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

Số: 141 /ĐHSPHN-SĐH
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 khoá 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-BGDĐT 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 khoá 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 ch

5. Thời gian nộp kinh p

Trường Đại học Sư phạ
biên lai tài chính cho học v

- Đợt 1, ngày 6/3/201
- 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 kí theo khóa học.***

Có gì chưa rõ, học viên liên hệ với Phòng Sau đại học, Trường ĐSHP 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 /ĐHSPHN-SĐH
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 khoá 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-BGDĐT 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 khoá 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**

- 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 kí theo khóa học.***

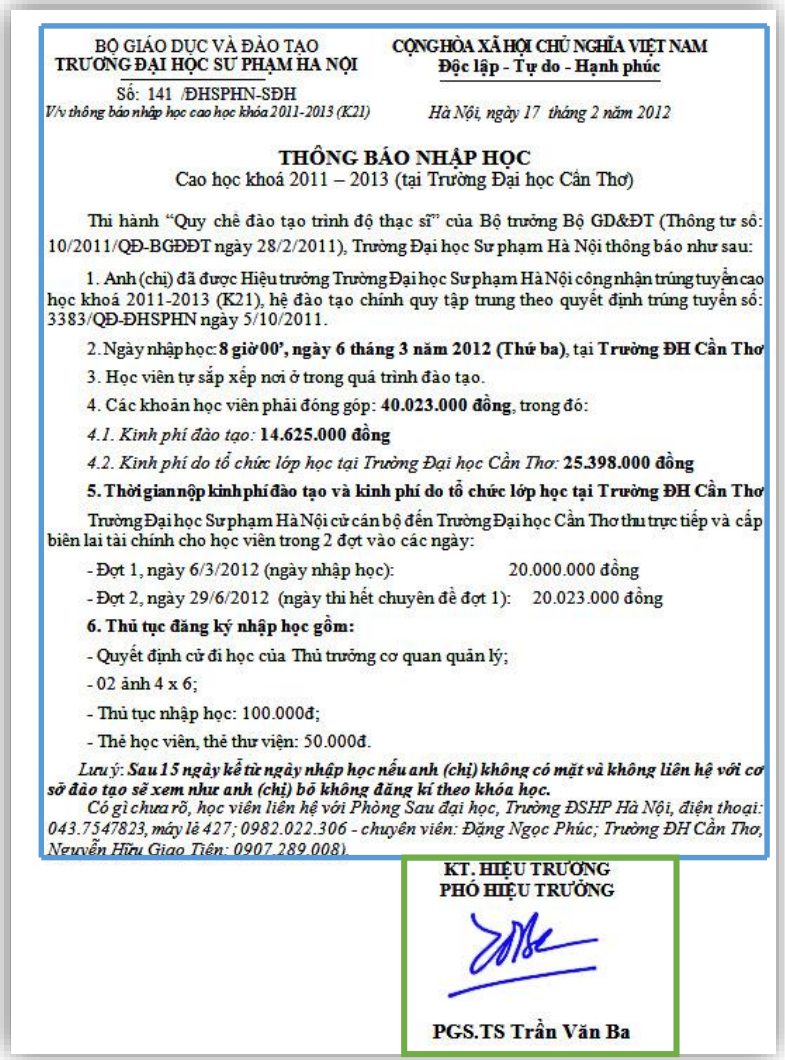
Có gì chưa rõ, học viên liên hệ với Phòng Sau đại học, Trường ĐSHP Hà Nội, điện thoại: 043.7547823, máy lẻ 427; 0982.022.306 - chuyên viên: Đặng Ngọc Phúc; Trường ĐH Cần Thơ, Nguyễn Hữu Giao Tiên: 0907.289.008).

KT. HIỆU TRƯỞNG
PHÓ HIỆU TRƯỞNG

PGS.TS Trần Văn Ba

Văn bản nào có giá trị pháp lý?

Chữ ký viết tay



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

Số: 141 /ĐHSPHN-SĐH
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 khoá 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-BGDĐT 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 khoá 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 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 kí theo khóa học.***

Có gì chưa rõ, học viên liên hệ với Phòng Sau đại học, Trường ĐSHP 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

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 ?

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


PDF
Adobe
Contract
Jim McEwan
Mar 16, 2008
Document Read & Approved

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
- 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

hQlmaw9dfDAWEPmj9h8
7onwe1jd03nDFo

Chữ ký

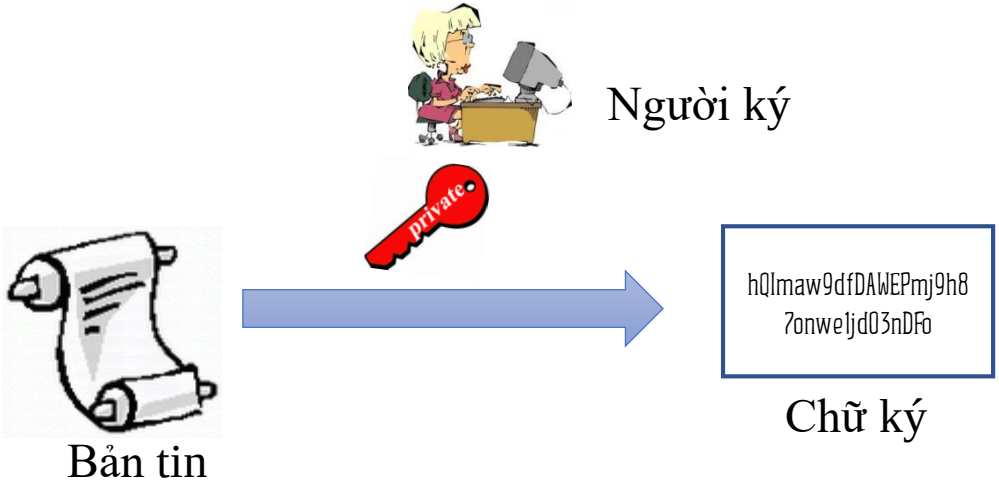
12khmlik0jh72nu8om

- ✓ *khó thay đổi*
- ✓ *khó dùng lại*

⇒ *Xác thực nội dung bản tin được ký*

Tính chất 2

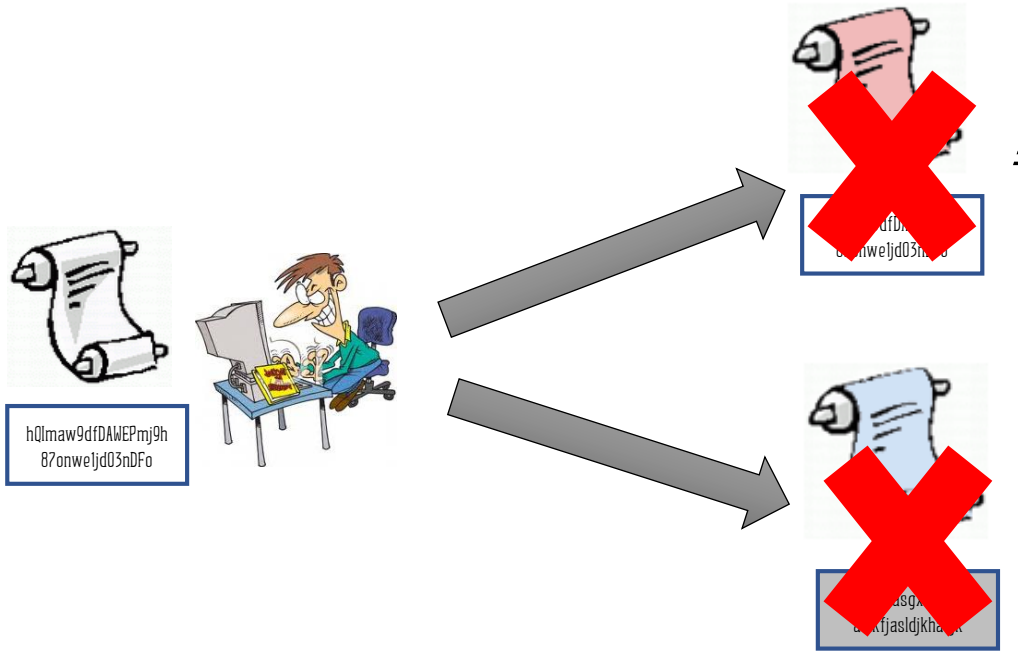
- Sử dụng thông tin mà chỉ có người ký mới có



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

Tính chất 3

- Gần như không thể giả mạo chữ ký



⇒ *Xác thực nội dung bản tin được ký*

⇒ *Xác minh người tạo ra 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

Người ký A

(m)

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

$S_A(m) = s$

(s)

hQlmaw9dfDAWEPmj9
h87onwe1jd03n

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

hQlmaw9dfDAWEPmj9
h87onwe1jd03n

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

hQlmaw9dfDAWEPmj9
h87onwe1jd03n

$V_A(m, s)$

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

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

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
- $V_A(m, s) = true$ nếu và chỉ nếu $S_A(m, s) = s$

Nhắc lại về mật mã khóa công khai

Chủ thể A

Khóa bí mật pr_A

Khóa công khai pb_A

E: Thuật toán mã hóa/giải mã

Tính đối hợp

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

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

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

pb_A : Khóa công khai của A

Chữ ký số dựa trên mật mã khóa công khai

Alice

Bob

Xin chao, toi la Alice. Duoi day la …

$s = E_{private\_key}(m)$

*s#F&G”E

Xin chao, toi la Alice. Duoi day la …

*s#F&G”E

Xin chao, toi la Alice. Duoi day la …

…….
…….
…….

…….
…….
…….

$m' = D_{public\_key}(s)$

Vấn đề

- Tốc độ chậm
- Kích thước chữ ký lớn
- Vấn đề với bản tin quá dài

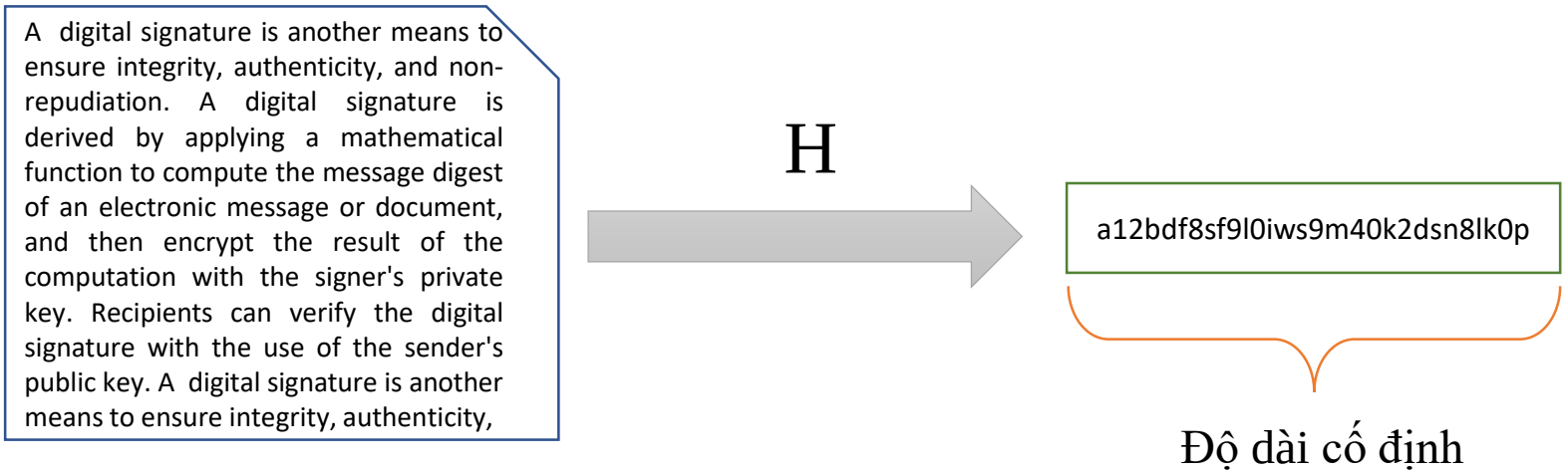
  ⇒ chia thành nhiều bản tin nhỏ và ký trên từng bản tin nhỏ

  ⇒ tấn 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)*



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
```

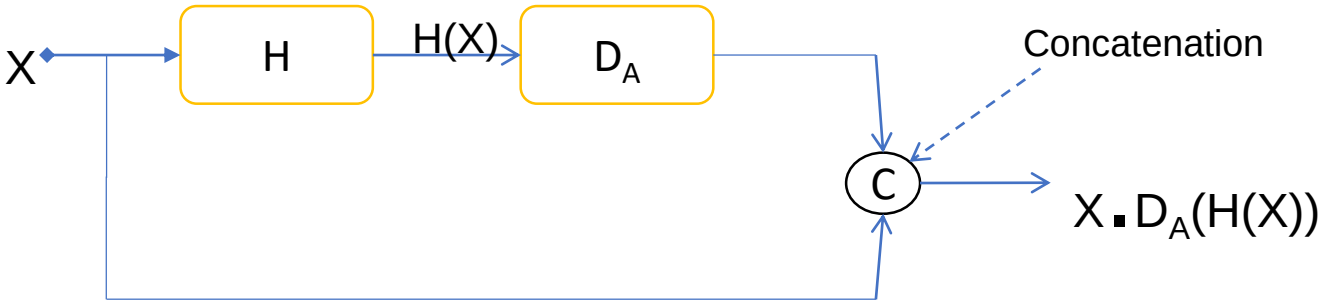
Tính chất

- *Tính một chiều:*
  - Biết giá trị hàm băm ⇒ gần như không thể suy ngược giá trị bản tin
- *Tính không trùng lặp:*
  - Với bản tin X cho trước ⇒ 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*

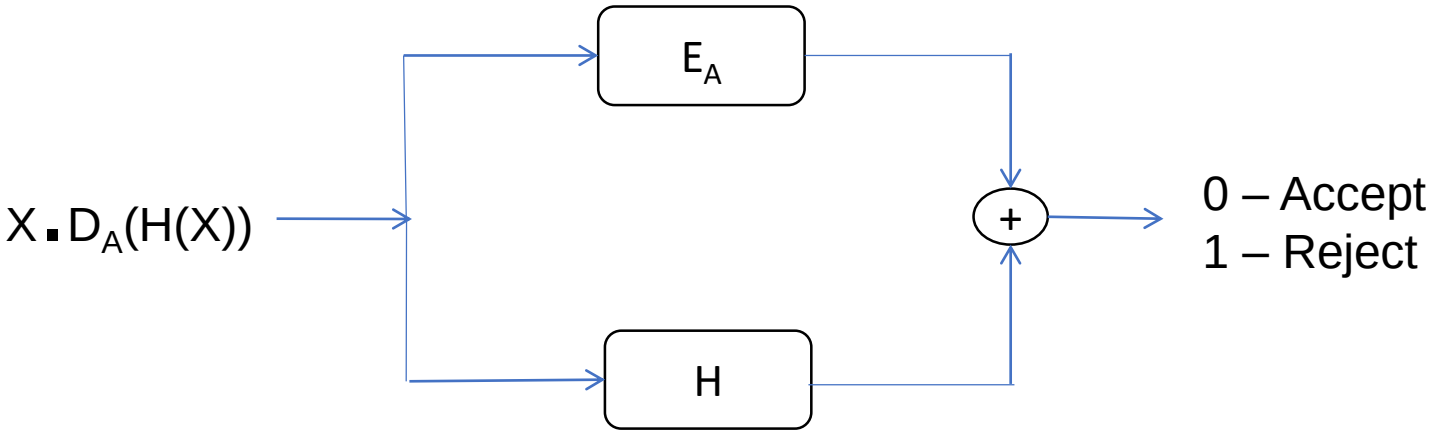
Chữ ký số với hàm băm

- Ý tưởng chính
  - Ký trên giá trị hàm băm
- Sinh chữ ký
  - $s = E_{pr_A}(H(m))$
- Xác minh chữ ký
  - $D_{pb_A}\ eq\ H(m) = \begin{cases} true, & if\ D_{pb_A}(s) = H(m) \\ true, & if\ D_{pb_A}(s) \neq H(m) \end{cases}$

Chữ ký số với hàm băm



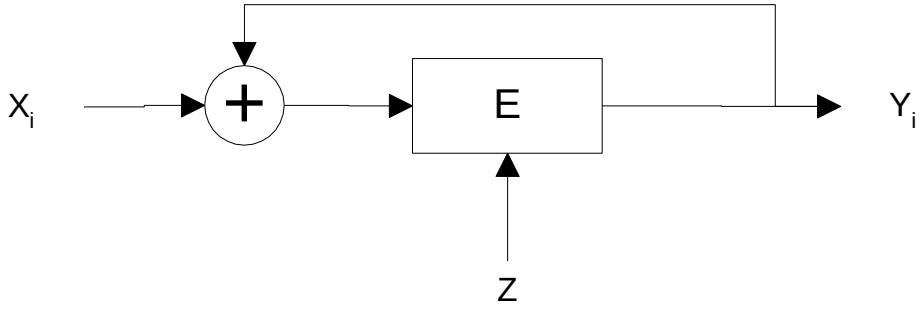
Signature Generator



Signature Verifier

Một số phương pháp tạo hàm băm

- Sử dụng SKC
  - Ví dụ: Dùng SKC với chế độ CBC
- Sử dụng đồng dư (modulo arithmetic operations)
- Một số hàm băm thông dụng
  - MD4, MD5, SHA



$X = X_1 X_2 X_3 \dots X_n$

$Y_i = E_z(X_i \oplus Y_{i-1})$

$H(X) = Y_n$

Tính đụng độ của hàm băm

- Việc tránh đụng độ hoàn toàn là không thể (theo lý thuyết)
  - Nguyên lý Dirichlet: bỏ n+1 con thỏ vào n rọ → ít nhất 2 con thỏ chung 1 roj
  - Nếu thử vét cạn |Y|+1 bản tin → tìm được 2 bản tin có cùng giá trị băm (H:X→Y)
- Thực tế
  - Để đảm bảo tính an toàn cho hàm băm thì cần chọn |Y| đủ lớn sao cho việc vét cạn là không thể
    - Nhược điểm: |Y| quá lớn sẽ làm tăng kích thước chữ ký, chậm quá trình tạo chữ ký
  - Tuy nhiên, vẫn khó tránh khỏi đụng độ

Tấn công theo kiểu nghịch lý ngày sinh

- Giá trị băm là 64 bits có đủ an toàn?
  - Không gian tìm kiếm là 2^{64} → tương đối lớn để có thể thực hiện duyệt toàn bộ
  - Tuy nhiên, có thể tấn công theo nghịch lý ngày sinh
    - Thực tế, kẻ tấn công chỉ cần tạo 2^{32} gói tin và có thể tấn công với xác suất thành công khá cao

Tấn công theo kiểu nghịch lý ngày sinh

- Mục tiêu: Với hàm băm H, tìm x, x' sao cho $H(x) = H(x')$
- Thuật toán:
  - Tạo tập S gồm q giá trị ngẫu nhiên thuộc X
  - Với mỗi $x \in S$, tính $h_x = H(x)$
  - Nếu $h_x = hx$, với $x' \neq x$ → thành công trong tìm ra đụng độ (x, x')
- Xác suất thành công trung bình

  $\varepsilon = 1 - \exp(^{q(q-1)}/_{2|Y|})$
  - Giả sử Y có 2^m phần tử, chọn $\mathbf{q \approx 2^{m/2}}$ → ε xấp xỉ 0.5

Nghịch lý ngày sinh

- Cho một nhóm người → số người nhỏ nhất của nhóm đó, sao cho
  - Xác suất để có 2 người trong nhóm có cùng ngày sinh là 50%

Là 23

- → tại sao lại gọi là nghịch lý?
- Chứng minh
  - 1 - (1- 1/365)(1-2/365)…(1-22/365) = 1-0.493 = 0.507

Nghịch lý ngày sinh

- Cho 1 hàm băm có kích thước đầu ra là M. Lấy 1 tập ngẫu nhiên các bản rõ với độ dài q thì xác suất để tồn tại 2 bản rõ có cùng giá trị băm là: $1 - e^{\frac{-q(q-1)}{2M}}$
- Chứng minh
  - Xác suất để tất bản rõ có giá trị băm khác nhau là:
    - $1 \times \frac{M-1}{M} \times \cdots \times \frac{M-(q-1)}{M} = \left(1 - \frac{1}{M}\right) \ldots (1 - \frac{q-1}{M})$
  - Xác suất để tồn tại 2 bản rõ có cùng gía trị băm là:
    - $1 - \left(1 - \frac{1}{M}\right) \ldots \left(1 - \frac{q-1}{M}\right) \approx 1 - e^{\left(-\frac{1}{M}\right) \times \left(-\frac{2}{M}\right) \times \cdots \times \left(-\frac{q-1}{M}\right)} = 1 - e^{-\frac{q(q-1)}{2M}}$

Nghịch lý ngày sinh

- Cho 1 hàm băm có kích thước đầu ra là M. Lấy 1 tập ngẫu nhiên các bản rõ với độ dài q thì xác suất để tồn tại 2 bản rõ có cùng giá trị băm là: $1 - e^{\frac{-q(q-1)}{2M}}$
  - Với $q \approx \sqrt{2Mln\frac{1}{1-\varepsilon}}$, xác suất xấp xỉ $1 - \varepsilon$
  - Với$q \approx 1.17\sqrt{M}$, xác suất xấp xỉ 0.5

MAC: mã xác thực bản tin

- Hàm băm được công khai, khoá được giữ bí mật giữa người gửi và người nhận
  - Người gửi tính mac1 = MAC(M, H, K), và gửi cùng bản tin M
  - Người nhận tính mac2 = MAC(M, H, K) và kiểm tra xem mac1 = mac2 ?
    - Nếu đúng → gói tin được xác thực
    - Nếu không → gói tin không được xác thực → Không nhận/huỷ gói tin
- Không thể tính được MAC nếu không biết khoá bí mật giữa người gửi và người nhận
  - Cơ chế này vừa đảm bảo tính toàn vẹn và tính xác thực người gửi