

# Nội dung

## Chữ ký phụ thuộc tài liệu

- **Chữ ký số là gì?**

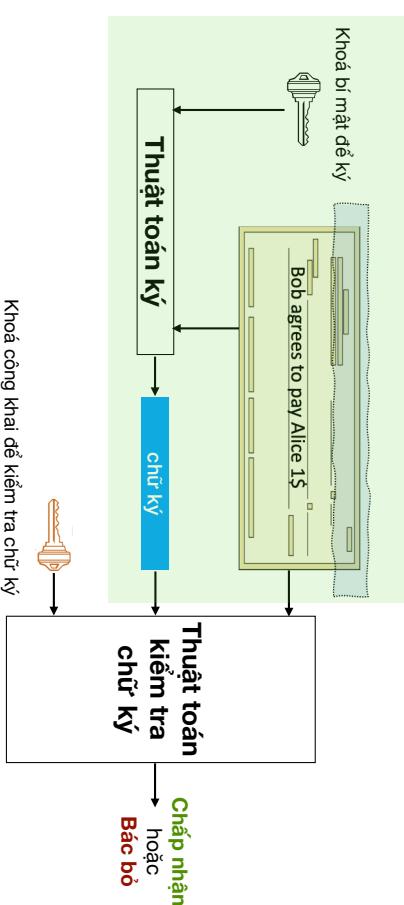
- Ứng dụng

- Sơ đồ chữ ký số RSA

- Sơ đồ chữ ký số ElGamal

- Chuẩn chữ ký số DSA

2

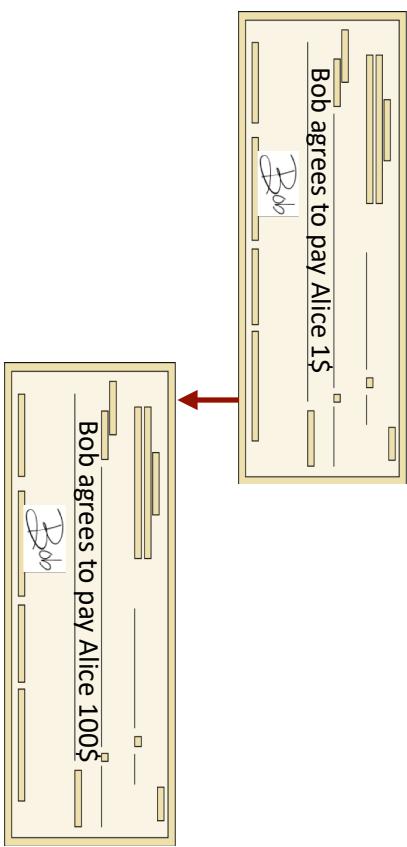


4

## Chữ ký vật lý

### Nhập môn An toàn Thông tin

#### Chữ ký số



3

# Chữ ký số

## Tính an toàn 1

**Định nghĩa.** Một sơ đồ chữ ký số bao gồm ba thuật toán

- $Gen()$  thuật toán ngẫu nhiên output ra cặp khoá ( $pk, sk$ )
- $S(sk, m \in M)$  output ra chữ ký  $\sigma$
- $V(pk, m, \sigma)$  output 'chấp nhận' hoặc 'bá c bỏ'

6

Tấn công chọn bản rõ

- Kẻ tấn công có thể lấy được chữ ký chọn  $q$  thông điệp tùy chọn  $m_1, m_2, \dots, m_q$

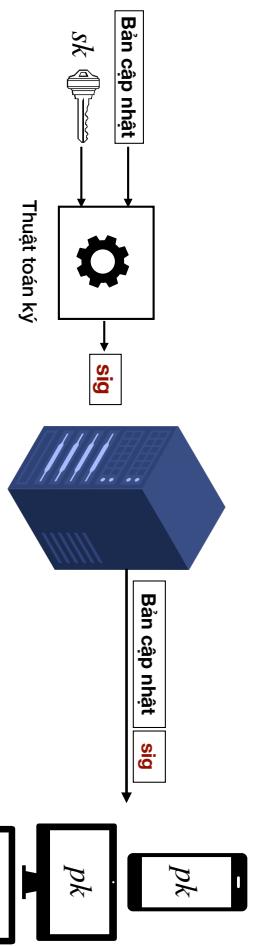
ký hiệu

$$\sigma_i = S(sk, m_i) \quad \text{với } i = 1, \dots, q$$

8

## Ví dụ thực tế

Khách hàng



Kiểm tra  $sig$ ,  
cài đặt nếu hợp lệ

## Tính đúng đắn

- Với mọi cặp  $(pk, sk)$  sinh bởi thuật toán  $Gen()$ ,
- và với mọi thông điệp  $m \in M$ , ta có

$$V(pk, m, S(sk, m)) = \text{'chấp nhận'}$$

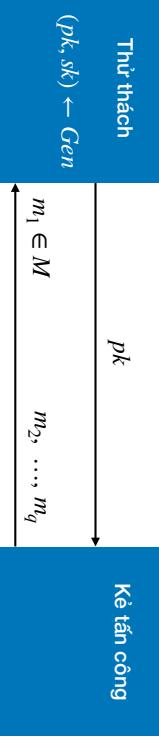
5

- Khả năng của kẻ tấn công là

7

# Chữ ký an toàn

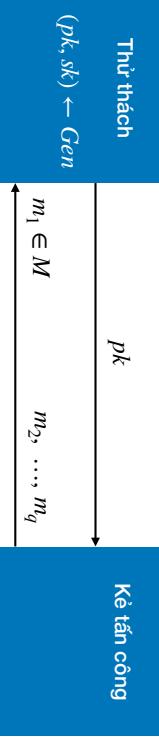
## Nội dung



Kẻ tấn công **thắng** nếu  $V(pk, m, \sigma) = \text{'chấp nhận'}$  và  $m \notin \{m_1, \dots, m_q\}$

10

- Chữ ký số là gì?
- **Ứng dụng**
- Sơ đồ chữ ký số RSA
- Sơ đồ chữ ký số ElGamal
- Chuẩn chữ ký số DSA



Kẻ tấn công **thắng** nếu  $V(pk, m, \sigma) = \text{'chấp nhận'}$  và  $m \notin \{m_1, \dots, m_q\}$

11

# Tính an toàn

- Mục đích của kẻ tấn công

## Giả mạo thông điệp

- Đưa ra được cặp thông điệp/chữ ký hợp lệ  $(m, \sigma)$  mà

$$m \notin \{m_1, \dots, m_q\}$$

- Sơ đồ chữ ký là **an toàn** khi kẻ tấn công không tạo được chữ ký hợp lệ cho thông điệp mới.

# Chữ ký an toàn

- Mục đích của kẻ tấn công

## Giả mạo thông điệp

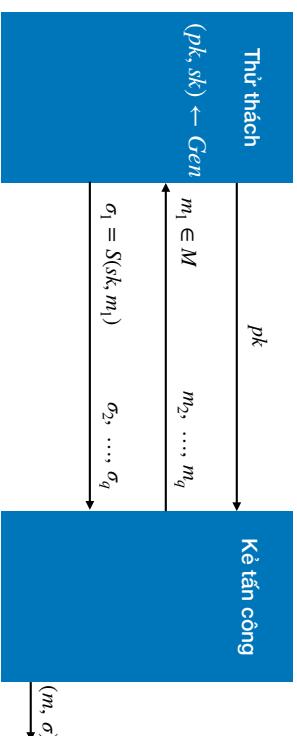
- Đưa ra được cặp thông điệp/chữ ký hợp lệ  $(m, \sigma)$  mà

$$m \notin \{m_1, \dots, m_q\}$$

- Sơ đồ chữ ký là **an toàn** khi kẻ tấn công không tạo được chữ ký hợp lệ cho thông điệp mới.

- Hệ chữ ký là **an toàn** nếu với **mọi** kẻ tấn công  $A$ , xác suất  $A$  thắng là “nhỏ không đáng kể”

9



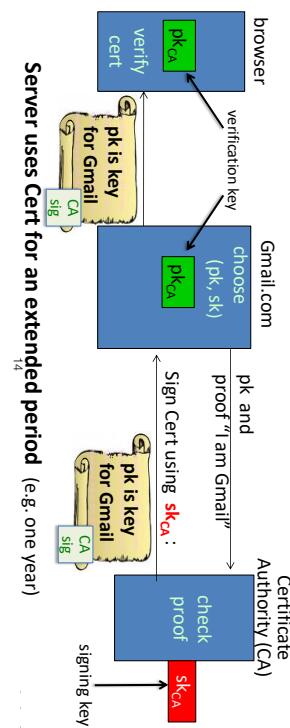
Kẻ tấn công **thắng** nếu  $V(pk, m, \sigma) = \text{'chấp nhận'}$  và  $m \notin \{m_1, \dots, m_q\}$

12

11

# Chứng chỉ số

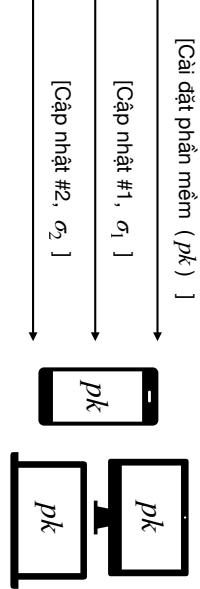
- Vấn đề:** trình duyệt cần khóa công khai của máy chủ để thiết lập khóa phiên
- Giải pháp:** máy chủ yêu cầu bên thứ ba tin cậy (CA) xác thực và ký lên khóa công khai  $pk$



## Ký trên phần mềm

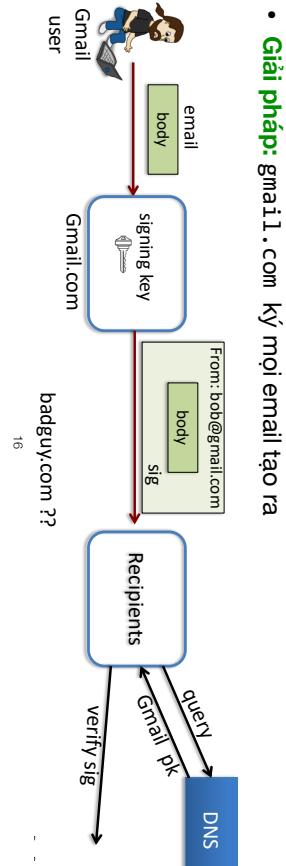
- Công ty bán phần mềm BK ký lên phần mềm

- Khách hàng có khóa công khai  $pk$  của BK. Họ sẽ cài đặt phần mềm nếu chữ ký là hợp lệ.



# Ký email: DKIM (domain key identified mail)

- Vấn đề:** email giả khẳng định gửi từ [someuser@gmai1.com](mailto:someuser@gmai1.com) nhưng thực tế, mail gửi từ [badguy.com](mailto:badguy.com)  
⇒ Làm [gmail.com](mailto:gmail.com) giống như một nguồn gửi email giả



## Chứng chỉ số

The screenshot shows the following certificate information:

- Serial Number:** 581474488373390497
- Version:** 3
- Signature Algorithm:** SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
- Parameters:** none
- Not Valid Before:** Wednesday, July 31, 2013 4:59:24 AM Pacific Daylight Time
- Not Valid After:** Thursday, July 31, 2014 4:59:24 AM Pacific Daylight Time
- Public Key Info:**
  - Algorithm: Elliptic Curve Public Key (1.2.840.10045.2.1)
  - Parameters: Elliptic Curve secp256r1 (1.2.840.10045.1.7)
  - Public Key: 65 bytes: 04 71 8C DD E0 0A C9 76 ...
  - Key Size: 256 bits
  - Key Usage: Encrypt, Verify, Derive
  - Signature: 256 bytes: 8A 38 F5 E7 F6 59 ...
- Details:**
  - Subject Name: mail.google.com
  - State/Province: California
  - Locality: Mountain View
  - Organization: Google Inc.
  - Common Name: mail.google.com
  - Issuer Name: Google Inc.
  - Organization: Google Inc.
  - Common Name: Google Internet Authority C2

# Ba cách tiếp cận cho toàn vẹn thông điệp

## Phương pháp tổng quát

1. **Hàm băm kháng xung đột:** cần không gian công khai chỉ đọc
2. **Mã xác thực thông điệp:** với mỗi khách hàng, người bán phải tính một MAC mới của phần mềm  
⇒ phải quản lý một khoá bí mật dùng lâu dài (để sinh khoá MAC cho mỗi khách hàng)
3. **Chữ ký số:** người bán phải quản lý khoá bí mật dùng lâu dài
  - Chữ ký kèm với phần mềm
  - Phần mềm có thể download ở nơi không tin cậy

18

- Ý tưởng được Diffie & Hellman đưa ra năm 1976
- Xây dựng lược đồ chữ ký từ hệ mã khoá công khai đơn định ( $E, D$ )

$$\sigma = S(sk, m) = D(sk, m)$$

$$V(pk, m, \sigma) = \begin{cases} 1 & \text{nếu } E(pk, \sigma) = m \\ 0 & \text{ngược lại} \end{cases}$$

20

# Khi nào sử dụng chữ ký số

Nếu **một** phía ký và **một** phía kiểm tra : **dùng MAC**

- Phải tương tác để có khoá chia sẻ
- Bên nhận có thể sửa đổi dữ liệu và ký lại nó trước khi chuyển dữ liệu tới bên thứ ba

Nếu **một** bên ký và **nhiều** bên kiểm tra: **dùng chữ ký số**

- Bên nhận không thể nào sửa dữ liệu nhận được trước khi chuyển dữ liệu tới bên thứ ba
- Không chối bỏ được

# Nội dung

- Chữ ký số là gì?
- Ứng dụng

### • **Sơ đồ chữ ký số RSA**

- Sơ đồ chữ ký số ElGamal
- Chuẩn chữ ký số DSA

17

19

# Tấn công 1

## Ví dụ: Sinh khoá

- Chọn  $p = 3$  và  $q = 11$
- $n = p \cdot q = 33$

- $\phi(n) = (3 - 1)(11 - 1) = 20$
- Chọn  $e = 3$

- $d = e^{-1} = 7 \pmod{20}$
- Output ( $pk = 3, sk = 7$ )

22

- Có thể tạo ra chữ ký của thông điệp cụ thể
  - Ví dụ, dễ tính căn bậc  $e$  của thông điệp  $m = 1$  hoặc
    - căn bậc ba của thông điệp  $m = 8$

24

## Ví dụ: Ký và kiểm tra

- Hàm sinh khoá  $Gen()$ :

- Chọn  $n = pq$  ( $p, q$  nguyên tố ngẫu nhiên  $\lambda$ -bit)

- Chọn  $e, d$  thỏa mãn  $ed = 1 \pmod{\phi(n)}$

-  $pk = (n, e)$  và  $sk = (n, d)$

• Hàm ký  $S(sk, m) = m^d \pmod{n}$

• Hàm kiểm tra chữ ký  $V(pk, m, \sigma) = 1 \Leftrightarrow \sigma^e = m \pmod{n}$

21

### Kiểm tra chữ ký

$V(pk = e = 3, m = 4, \sigma = 16)$ :

Tạo chữ ký  
 $S(sk = d = 7, m = 4)$ :

$$\begin{aligned} & \bullet \sigma = m^d \pmod{n} \\ & = 4^7 = 16 \pmod{33} \\ & \bullet \text{Do } m = m' \text{ nên 'chấp nhận'} \end{aligned}$$

23

# Bài tập

## Sơ đồ Băm và Ký

- $Gen(): [...]$
- $S(sk, m) = H(m)^d \mod n$
- $V(pk, m, \sigma) = 1 \Leftrightarrow \sigma^e = m \mod n$

Hãy chứng minh hệ chữ ký Textbook RSA

là không an toàn bằng cách chỉ ra rằng: từ chữ ký của thông điệp  $m$  ta có thể tạo ra chữ ký cho thông điệp  $m^2$ .

- **Hỏi:** Có dễ tạo chữ ký cho thông điệp
- **Trả lời:** Tùy thuộc vào hàm băm  $H$

26

## Tấn công 2

## Tấn công 3

- Có thể kết hợp hai chữ ký để thu được chữ ký thứ ba
  - Giả sử  $\sigma_1, \sigma_2$  là chữ ký hợp lệ của thông điệp  $m_1, m_2$
  - Khi đó  $\sigma = [\sigma_1 \cdot \sigma_2 \mod n]$  là chữ ký hợp lệ của thông điệp  $m = m_1 \cdot m_2$  bởi vì
$$(\sigma_1 \cdot \sigma_2)^e = \sigma_1^e \cdot \sigma_2^e = m_1 \cdot m_2$$

25

27

# Sơ đồ Băm và Ký với RSA

- Nếu giả sử RSA là đúng, và H được mô hình như một hàm ngẫu nhiên (ánh xạ lên  $\mathbb{Z}_n^*$ ), thì sơ đồ băm và ký với RSA là **an toàn**

• Trên thực tế, H được sửa đổi từ hàm băm mật mã quen thuộc

- Phải đảm bảo miền giá trị của H là đủ lớn!
- Một lựa chọn “tốt” cho H là:

$$H(m) = n \text{ byte đầu tiên của} \\ SHA256(1\|m)\parallel SHA256(2\|m)\parallel \dots \parallel SHA256(11\|m)$$

30

# Trực giác cho tính an toàn

- Quay lại với các cách tấn công trước...

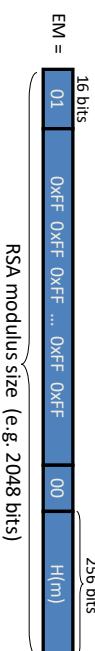
1. Không dễ tính căn bậc  $e$  của  $H(1), \dots$

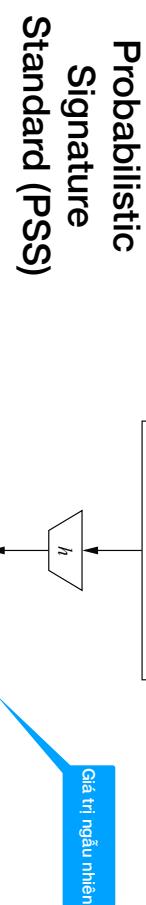
2. Chọn  $\sigma$  nhưng làm thế nào tìm được  $m$  để  $H(m) = \sigma^e \pmod{n}$ ?

$\Rightarrow$  Hàm H nên là hàm một chiều

3.  $H(m_1) \cdot H(m_2) = \sigma_1^e \cdot \sigma_2^e = (\sigma_1 \cdot \sigma_2)^e \neq H(m_1 \cdot m_2)$

# Chữ ký PKCS1 v1.5

- Hoán vị cửa sổ RSA :  $pk = (n, e), sk = (n, d)$
  - $S(sk, m \in M)$  :
- EM = 
- RSA modulus size (e.g. 2048 bits)
- output  $\sigma = (EM)^d \pmod{n}$
- $V(pk, m \in M, \sigma)$ : kiểm tra  $\sigma^e \pmod{n}$  có dạng đúng như ở trên



29

# Hệ chữ ký số ElGamal

## Textbook ElGamal: Hàm ký

- $S(sk = d, m)$  :

1. Chọn khóa tạm thời  $k_E \in \{1, 2, \dots, p - 2\}$  thoả mãn  $\gcd(k_E, p - 1) = 1$  (để có  $k_E^{-1} \bmod p - 1$ )
2. Tính
$$r = g^{k_E} \bmod p,$$
$$s = \frac{(m - d \cdot r)}{k_E} \bmod p - 1$$

3. Output chữ ký  $\sigma = (r, s)$

<sup>36</sup>

- Đẳng thức
$$E(D(m)) = m$$
không đúng cho ElGamal vì ElGamal là hệ mã xác suất.
- Chữ ký ElGamal rất khác so với hệ mật mã ElGamal.

<sup>34</sup>

## Nội dung

### Textbook ElGamal: Sinh khoá

- Chữ ký số là gì?
- Ứng dụng
- Sơ đồ chữ ký số RSA
- **Sơ đồ chữ ký số ElGamal**
  - Chuẩn chữ ký số DSA

<sup>33</sup>

<sup>35</sup>

# ElGamal: Tính đúng đắn

## Ví dụ: Kiểm tra chữ ký

- $t = (g^d)^r \cdot r^s \pmod{p} = (g^d)^r \cdot (g^{k_E})^s \pmod{p}$   
 $= g^{dr + s \cdot k_E} \pmod{p}$
- Do định lý Fermat nhỏ, điều kiện  $g^m = t \pmod{p}$  tương đương với  
 $m = (d \cdot r + s \cdot k_E) \pmod{p-1}$
- và tương đương với điều kiện

$$s = \frac{m - d \cdot r}{k_E} \pmod{p-1}$$



- Kiểm tra**  $V(pk = g^d = 7, m = 26, \sigma = (3, 26))$ :
- $t = (g^d)^r \cdot r^s = 7^3 \cdot 3^{26} = 22 \pmod{29}$
- $g^m = 2^{26} = 22 \pmod{29}$
- Do  $t = g^m \pmod{29}$  nên '**chấp nhận**'

38

40

# Textbook ElGamal: Kiểm tra chữ ký

## Ví dụ: Sinh khoá và chữ ký

### Sinh khoá $Gen()$

- $V(pk = g^d, m, \sigma = (r, s))$ :
- 1. Tính giá trị  
 $t = (g^d)^r \cdot r^s \pmod{p}$
- 2. if  $t = g^m \pmod{p}$  return '**chấp nhận**' else '**bác bỏ**'

### Tạo chữ ký $S(sk = 12, m = 26)$ :

- chọn  $p = 29$
- chọn  $g = 2$
- chọn  $sk = d = 12$ 
  - $s = (m - d \cdot r) \cdot k_E^{-1} \pmod{p-1}$   
 $= -10 \cdot 17 \pmod{28}$   
 $= 26 \pmod{28}$
- Output chữ ký  $(3, 26)$

37

39

## Bài tập

- Biết rằng tham số và khoá công khai của Bob là:

- $p = 29, g = 2, g^d = 7$

- Giả sử Bob đã ký hai thông điệp với cùng khoá tạm  $k_E$ :

- $[m_1, (r, s_1)] = [26, (3, 26)]$

- $[m_2, (r, s_2)] = [13, (3, 1)]$

- Hãy tính khoá bí mật  $s_k$  của Bob.

42

Giả mạo chữ ký cho thông điệp “ngẫu nhiên”	
<b>Tạo chữ ký và thông điệp</b>	<b>Kiểm tra chữ ký</b>
<ul style="list-style-type: none"><li>Chọn hai số <math>i, j</math> thoả mãn <math>\gcd(j, p - 1) = 1</math></li><li>Tính chữ ký <math>r = g^{i \cdot (g^d)^j} \mod p</math> <math>s = -r \cdot j^{-1} \mod p - 1</math></li><li>Tính thông điệp <math>m = s \cdot i \mod p - 1</math></li></ul>	<ul style="list-style-type: none"><li>Tính <math>t = (g^d)^r \cdot r^s \mod p</math></li><li>bởi vì <math>t = g^m \mod p</math> nên chữ ký là hợp lệ</li></ul>

- Kiểm tra chữ ký

- $t = (g^d)^r \cdot r^s \mod p$

- Với Textbook ElGamal, liệu bạn có thể tạo ra chữ ký hợp lệ của một thông điệp “ngẫu nhiên” (tương tự như với Textbook RSA)?

## Không an toàn khi sử dụng lại $k_E$

Nếu ta ký hai thông điệp  $m_1$  và  $m_2$  cùng sử dụng khoá tạm  $k_E$ , khi đó

$$s_1 = \frac{m_1 - dr}{k_E} \mod p - 1 \quad \text{và} \quad s_2 = \frac{m_2 - dr}{k_E} \mod p - 1$$

Kè tốn công Oscar sẽ tính được  $k_E = \frac{m_1 - m_2}{s_1 - s_2} \mod p - 1$

và tính được khoá bí mật

$$d = \frac{m_1 - s_1 k_E}{r} \mod p - 1$$

## Bài tập

41

43

## Nội dung

- Chữ ký số là gì?
- Ứng dụng
- Sơ đồ chữ ký số RSA
- Sơ đồ chữ ký số ElGamal

- Chuẩn chữ ký số DSA

46

## DSA: Sinh khoá

- Sinh số nguyên tố  $p$  với  $2^{1023} < p < 2^{1024}$
- Tìm một ước nguyên tố của  $q$  của  $p - 1$  với  $2^{159} < q < 2^{160}$
- Tìm một phần tử sinh  $g$  với cấp  $\text{ord}(g) = q$ ; tức là  $g$  sinh nhóm con với  $q$  phần tử
- Chọn số ngẫu nhiên  $d$  với  $0 < d < q$
- Tính  $\beta = g^d$
- Output  $pk = (p, q, g, \beta)$  và  $sk = d$

48

## Băm và ký với ElGamal

## The Digital Signature Algorithm (DSA)

- Giống RSA, sơ đồ Băm và Ký không những tăng tính hiệu quả mà còn tăng độ an toàn.
- Nó giúp chống lại tấn công giả mạo chữ ký cho thông điệp “ngẫu nhiên”
- Trong sơ đồ này, phương trình ký trở thành

$$s = \frac{(H(m) - d \cdot r)}{k_E} \pmod{p-1}$$

- Chuẩn chữ ký số của Mỹ
- Được xuất bởi Viện tiêu chuẩn quốc gia (NIST)
- **Ưu điểm:**

- Độ dài chữ ký chỉ 320 bit
- Một số phương pháp tấn công sơ đồ chữ ký ElGamal không áp dụng được cho sơ đồ này

45

47

## DSA: Kiểm tra chữ ký

- Tính  $w = s^{-1} \bmod q$
- Tính  $u_1 = w \cdot H(m) \bmod q$
- Tính  $u_2 = w \cdot r \bmod q$
- Tính  $v = (g^{u_1} \cdot (g^d)^{u_2} \bmod p) \bmod q$
- Hàm kiểm tra  $V(pk, m, (r, s))$  như sau:  
`if v = r mod q return 'chấp nhận' else 'báć bở'`

50

### Sinh khoá

- 
- |   |  |
|---|--|
| • Chọn $p = 59$                             | • Chọn $khoá tạm thời k_E = 10$                          |
| • Chọn $q = 29$                             | • $r = (3^{10} \bmod 59) \bmod 29$<br>= 20 mod 29        |
| • Chọn $g = 3$                              | • Khoá bí mật $sk = d = 7$                               |
| • Khoá công khai<br>$pk = g^d = 4 \bmod 59$ | • $s = (26 + 7 \cdot 20) \cdot 3 \bmod 29$<br>= 5 mod 29 |
- 

### Ký thông điệp $H(m) = 26$

- |  |   |
|--|---|
| • Chọn khoá tạm thời $k_E = 10$                          | • $r = (3^{10} \bmod 59) \bmod 29$<br>= 20 mod 29 |
| • $s = (26 + 7 \cdot 20) \cdot 3 \bmod 29$<br>= 5 mod 29 |   |

52

## DSA: tham số và mức an toàn

$p$	$q$	Chữ ký	Kích thước mã băm	Mức an toàn
1024	160	320	160	80
2048	224	448	224	112
3072	256	512	256	128

49

## Ví dụ: DSA sinh khoá và ký

### Ký thông điệp $H(m) = 26$

- |   |  |
|---|--|
| • Chọn $p = 59$                             | • Chọn $khoá tạm thời k_E = 10$                          |
| • Chọn $q = 29$                             | • $r = (3^{10} \bmod 59) \bmod 29$<br>= 20 mod 29        |
| • Chọn $g = 3$                              | • Khoá bí mật $sk = d = 7$                               |
| • Khoá công khai<br>$pk = g^d = 4 \bmod 59$ | • $s = (26 + 7 \cdot 20) \cdot 3 \bmod 29$<br>= 5 mod 29 |

52

# Tính toán

## Sinh số nguyên tố cho DSA

- **Bài toán:**
  1. Tìm số nguyên tố  $q$  với  $2^{159} < q < 2^{160}$  dùng thuật toán Miller – Rabin
  2. **for**  $i = 1$  to 4096

- Làm thế nào để tìm một nhóm vòng  $\mathbb{Z}_p^*$  kích thước 1024 bit, và
  - có nhóm con nguyên tố kích thước  $2^{160}$
- **Phương pháp:**
  - Sinh số nguyên tố  $q$  kích thước 160 bit và xây dựng số  $p$  từ nó
  - **if**  $p$  là số nguyên tố: **return**  $(p, q)$       // Dùng thuật toán Miller – Rabin
  - 3. Quay lại bước 1

54

56

## Ví dụ: Kiểm tra chữ ký

**Kiểm tra  $V(pk = 4, H(m) = 26, (r = 20, s = 5))$ :**

- $w = 5^{-1} = 5 \pmod{29}$
- $u_1 = 6 \cdot 26 = 11 \pmod{29}$
- $u_2 = 6 \cdot 20 = 4 \pmod{29}$
- $v = (3^{11} \cdot 4^4 \pmod{59}) \pmod{29} = 20$
- Do  $v = r \pmod{29}$  nên chữ ký là '**hợp lệ**'

53

## Sinh số nguyên tố cho DSA

**Output:**

- hai số nguyên tố  $(p, q)$   
với  $2^{1023} < p < 2^{1024}$  và  $2^{159} < q < 2^{160}$   
sao cho  $p - 1$  là bội của  $q$

55

