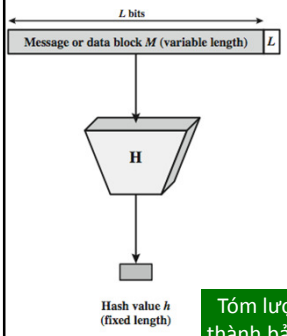
MẬT MÃ ỨNG DỤNG TRONG ATTT

Bài 04. Hàm băm và mật mã khóa công khai

1. Hàm băm
2. Tấn công từ điển
3. Một số thuật toán mật mã khóa công khai điển hình

1. Hàm băm
2. Tấn công từ điển
3. Một số thuật toán mật mã khóa công khai điển hình

Giới thiệu về hàm băm



- Giá trị băm "đại diện" cho một thông báo (văn bản) rất dài
  - Có thể gọi là "bản tóm lược" của thông báo (*message digest*)
- Một bản tóm lược thông báo như là một `` dấu vân tay số - digital fingerprint'' của tài liệu gốc

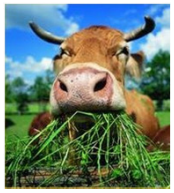
Tóm lược thông báo có độ dài tùy ý thành bản tóm lược có độ dài cố định

$$h = H(M)$$

4

Tính chất của hàm băm

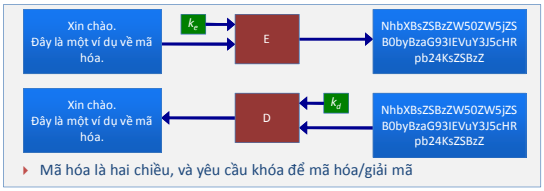
- Hàm nghiền
  - Hàm băm như hàm "nghiền" hay "tóm lược"



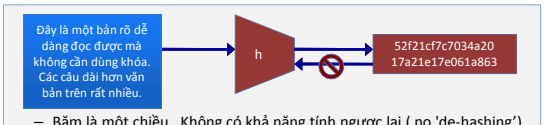
5

Tính chất của hàm băm

- Băm và mã hóa



- Mã hóa là hai chiều, và yêu cầu khóa để mã hóa/giải mã



- Băm là một chiều. Không có khả năng tính ngược lại (no 'de-hashing')

6

Tính chất của hàm băm

- Có độ dài cố định
- Kháng tiền ảnh:
- Kháng tiền ảnh thứ hai:
- Kháng va chạm:

7

1. Hàm băm
2. **Tấn công từ điển**
3. Một số thuật toán mật mã khóa công khai điển hình

Tấn công từ điển

9

Tấn công từ điển

Dictionary Attack

- Most people use real words as passwords
- Try all dictionary words before trying a brute force attack
- Makes the attack much faster

10

Tấn công từ điển

Password	Hash 0xe3bca98abcd
mimoza	0x938ff302c906
violet210	0xf2357adef39c
luckyday	0x03aa8c0ff391
mysecret	0xff0cea390de9
vietninja	0x930000b8ca8
p@$$w0rd	0xe3bca98abcd
khongbiet	0xac0bb81ca83
.....	.....

Precomputed Hash Table

11

Tấn công từ điển

Password	Salt	Hash
mimoza	0x7381a0f10c3	0x938ff3a2c906
violet210	0xa0c110f139d	0xf23e7adef39c
luckyday	0x30ea0fd1d2f	0x03aa8c01f391
p@$$w0rd	0x31ffac10ca0	0xff0cea3d0de9
p@$$w0rd	0xffa0cc103e1	0x930e00b8ca8
p@$$w0rd	0x00a10fc13d	0xe3bc098abcd
khongbiet	0xd103c3f13f1	0xac0bb80ca83
.....		.....

Sử dụng Salt chống lại Precomputed Hash Table

12

Tấn công từ điển

- Sử dụng salt ngăn chặn được việc dùng Precomputed Hash Table nhưng không ngăn chặn được việc sử dụng từ điển
- Để chống lại tấn công từ điển cần sử dụng mật khẩu không có trong từ điển!

13

1. Hàm băm
2. Tấn công từ điển
3. **Một số thuật toán mật mã khóa công khai điển hình**

Hàm băm và ứng dụng

- Cơ sở toán học
- Thuật toán Diffie-Hellman
- Thuật toán El-Gamal
- Thuật toán RSA

15

Hàm băm và ứng dụng

- Cơ sở toán học
- Thuật toán Diffie-Hellman
- Thuật toán El-Gamal
- Thuật toán RSA

16

Nhóm

Nhóm (G, *) là một tập hợp G, cùng với phép toán hai ngôi * thỏa mãn:

1. Tính đóng
   $a,b \in G \Rightarrow a*b \in G$
2. Tính kết hợp
   $(a*b)*c = a*(b*c) \quad \forall a,b,c \in G$
3. Tồn tại phần tử trung hòa
   $\exists e \in G: \quad a*e = e*a = a \quad \forall a \in G$
4. Tồn tại phần tử nghịch đảo
   $\forall a \in G \quad \exists b \in G: \quad a*b = b*a = e$

Ví dụ: (Z, +) là một nhóm

17

Nhóm hữu hạn

- Nhóm hữu hạn là nhóm có số phần tử hữu hạn

  |G| = q
- Nhóm cộng Z_n

  G = {0, 1, 2, ..., n-1}
- Nhóm nhân Z^*_n

18

Phần tử sinh của nhóm cyclic

- Nhóm cyclic là nhóm mà trong đó tồn tại phần tử **g**, sao cho khi áp dụng liên tiếp phép toán * lên phần tử **g** thì thu được tất cả các phần tử khác của nhóm.

- **Ví dụ 1**: $Z_5 = \{\{0, 1, 2, 3, 4\}, +\}$

$2+2 = 4 \pmod 5$
$2+2+2 = 1 \pmod 5$
$2+2+2+2 = 3 \pmod 5$
$2+2+2+2+2 = 0 \pmod 5$
$2+2+2+2+2+2 = 2 \pmod 5$

19

Phần tử sinh của nhóm cyclic

- **Ví dụ 2**: $Z^*_5 = \{\{1, 2, 3, 4\}, \times\}$

$3 \times 3 = 4 \pmod 5$
$3 \times 3 \times 3 = 2 \pmod 5$
$3 \times 3 \times 3 \times 3 = 1 \pmod 5$
$3 \text{ ^1} = 3 \pmod 5$

- Nếu n = 2, 4, p^k, $2p^k$ (p là số nguyên tố lẻ) thì Z^*_n là nhóm cyclic.

- Phần tử **g** được gọi là **phần tử sinh** hay **căn nguyên thủy**.

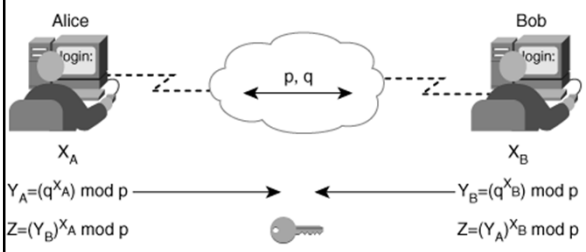
20

Hàm băm và ứng dụng

- Cơ sở toán học
- Thuật toán Diffie-Hellman
- Thuật toán El-Gamal
- Thuật toán RSA

21

Thuật toán Diffie-Hellman



By exchanging numbers (p,q) in the clear, two entities can determine a new unique number (z) known only to them.

22

Thuật toán Diffie-Hellman

	Alice	Bob
Step 1	Alice chooses a number, A Keeps it secret. A=3	Bob chooses a number, B Keeps it secret. B=6
Step 2	Alice puts 3 through $7^A \pmod{11}$ $7^3 \pmod{11}=343 \pmod{11}=2$	Bob puts 6 through $7^B \pmod{11}$ $7^6 \pmod{11}=117649 \pmod{11}=4$
Step 3	Alice calls result α Sends 2 to Bob	Bob calls result β Sends 4 to Alice
Step 4	Alice puts β through $\beta^A \pmod{11}$ $4^3 \bmod(11)=64 \pmod{11}=9$	Bob puts α through $\alpha^B \pmod{11}$ $2^6 \bmod(11)=64 \pmod{11}=9$

23

Hàm băm và ứng dụng

- Cơ sở toán học
- Thuật toán Diffie-Hellman
- Thuật toán El-Gamal
- Thuật toán RSA

24

Thuật toán mã hóa ElGamal

Thuật toán mã hóa ElGamal

Là thuật toán mật mã khóa công khai

25

Thuật toán mã hóa ElGamal

❑**Sinh cặp khóa cho Alice:**

- Chọn số nguyên tố **p**, phần tử sinh **g** của $\mathbf{Z^*_p}$
- Chọn ngẫu nhiên $\mathbf{x \in [1, p-1]}$
- Tính $\mathbf{h = g^x}$
- Khóa bí mật là $\mathbf{KS_A = (p, g, x)}$
- Khóa công khai là $\mathbf{KP_A = (p, g, h)}$

❑**Ví dụ:**

$$G = Z_{29}^*; \quad q = 28; \quad g = 8$$

$$x = 15; \quad h = g^x = 8^{15} = 21 (\mathrm{mod}\, 29)$$

$$KS_A = (29, 8, 15); \quad KP_A = (29, 8, 21)$$

26

Thuật toán mã hóa ElGamal

❑**Mã hóa (thông điệp m gửi cho Alice)**

- Biết khóa công khai là $\mathbf{KP_A = (p, g, h)}$
- Chọn ngẫu nhiên $\mathbf{y \in [1, p-1]}$
- Tính khóa chung $\mathbf{s = h^y}$
- Bản mã: $\mathbf{c = (c_1, c_2) = (g^y, m \cdot s)}$

❑**Ví dụ:**

$$KP_A = (29, 8, 21); \quad m = 10;$$

$$y = 7; \quad s = h^y = 21^7 = 12$$

$$c_1 = g^y = 8^7 = 17; \quad c_2 = ms = 10 \cdot 12 = 4$$

$$c = (c_1, c_2) = (17, 4)$$

27

Thuật toán mã hóa ElGamal

❑**Giải mã (bởi Alice)**

- Bản mã $\mathbf{c = (c_1, c_2)}$
- Dùng khóa bí mật là $\mathbf{KS_A = (p, g, x)}$
- Tính khóa chung $\mathbf{s = c_1^x}$
- Bản rõ: $\mathbf{m = c_2 \cdot s^{-1}}$

❑**Ví dụ:**

$$KS_A = (29, 8, 15); \quad c = (17, 4);$$

$$s = c_1^x = 17^{15} = 12; \qquad s^{-1} = 17;$$

$$m = c_2 s^{-1} = 4 \cdot 17 = 10 (\mathrm{mod}\, 29)$$

28

Lược đồ kí số ElGamal

Lược đồ kí số ElGamal

Tuy cùng tên với thuật toán mã hóa ElGamal nhưng bản chất thuật toán rất khác biệt.

29

Lược đồ kí số ElGamal

❑**Sinh cặp khóa cho Alice:**

- Chọn số nguyên tố **p**, phần tử sinh **g** của $\mathbf{Z^*_p}$
- Chọn ngẫu nhiên $\mathbf{x \in [1, p-1]}$
- Tính $\mathbf{h = g^x}$
- Khóa bí mật là $\mathbf{KS_A = (p, g, x)}$
- Khóa công khai là $\mathbf{KP_A = (p, g, h)}$

❑**Ví dụ:**

$$G = Z_{29}^*; \quad q = 28; \quad g = 8$$

$$x = 15; \quad h = g^x = 8^{15} = 21 (\mathrm{mod}\, 29)$$

$$KS_A = (29, 8, 15); \quad KP_A = (29, 8, 21)$$

30

Lược đồ kí số ElGamal

❑**Thực hiện kí số (bởi Alice)**

Thông điệp **m**, sử dụng KS_A = **(p, g, x)**

1. Sinh ngẫu nhiên: **1<k <p-1; gcd(k,p-1)=1**
2. Tính **r=g^k (mod p)**
3. Tính **s = (m-xr)k^-1 (mod p-1)**
4. Nếu **s=0** thì trở lại bước 1
5. Chữ kí số lên thông điệp **m** là **(r,s)**

❑**Ví dụ:**

m=10; KS_A**=(29,8,15)**

k= 11; r = g^k = 8^11=3 (mod p)

k^-1=23; s= (m-xr)k^-1 =(10 – 15*3)*23=7

sign(10) = (3,7)

31

Lược đồ kí số ElGamal

❑**Kiểm tra chữ kí (bởi bất kì ai)**

Thông điệp **m**, sử dụng KP_A = **(p, g, h)**

1. Kiểm tra: **0< r <p; 0< s <p-1**
2. Kiểm tra: **g^m == h^r·r^s (mod p)**

❑**Cơ chế:** $s = (m - xr)k^{-1} \pmod{p-1}$

$$\Rightarrow \quad m = xr + sk \pmod{p-1}$$

$$\Rightarrow \quad g^m = g^{xr+sk} = g^{xr} g^{sk} = h^r r^s \pmod{p}$$

❑**Ví dụ:**

$m = 10; \quad sign(10) = (3,7); \quad KP_A = (29,8,21)$

$g^m = 8^{10} = 4 \pmod{29}$

$h^r r^s = 21^3 \cdot 3^7 = 4 \pmod{29}$

32

Hàm băm và ứng dụng

- Cơ sở toán học
- Thuật toán Diffie-Hellman
- Thuật toán El-Gamal
- Thuật toán RSA

33

Thuật toán mã hóa RSA

Thuật toán mã hóa RSA

34

Thuật toán mã hóa RSA

❑**Sinh cặp khóa cho Alice:**

- Chọn 2 số nguyên tố **p, q**
- Tính **n = pq**, **φ = (p-1)(q-1)**
- Chọn số mũ công khai **e**: gcd**(e, φ)=1**
- Tính số mũ bí mật **d**: **ed=1 (mod φ)**

❑**Ví dụ:**

$p = 41, \quad q = 43, \quad n = 1763, \quad \varphi = 40 \cdot 42 = 1680$

$e = 11, \quad d = 11^{-1} = 611 \pmod{1680}$

$KS_A = (1763, 611); \quad KP_A = (1763, 11)$

35

Thuật toán mã hóa RSA

❑**Mã hóa và giải mã**

- Mã hóa: **c = m^e (mod n)**
- Giải mã **m = c^d (mod n)**

❑**Cơ chế:**

m = c^d = m^ed = m^kφ+1 = m (mod n)

❑**Ví dụ:**

$m = 100; \quad KS_A = (1763, 611); \quad KP_A = (1763, 11)$

$c = m^e = 100^{11} = 182 \pmod{1763}$

$m = c^d = 182^{611} = 100 \pmod{1763}$

36

Thuật toán kí số RSA

Thuật toán kí số RSA

Thuật toán kí số hoàn toàn tương tự thuật toán mã hóa. Trong đó, khóa bí mật được dùng để kí, khóa công khai được dùng để kiểm tra chữ kí

37

Thuật toán kí số RSA

❑**Sinh cặp khóa cho Alice:**

- Chọn 2 số nguyên tố **p, q**
- Tính **n = pq**, **φ = (p-1)(q-1)**
- Chọn số mũ công khai **e**: **(e, φ)=1**
- Tính số mũ bí mật **d**: **ed=1 (mod φ)**

❑**Ví dụ:**

$p=41,\quad q=43,\quad n=1763,\quad \varphi=30\cdot 42=1680$

$e=11,\quad d=11^{-1}=611\left(\mathrm{mod}1680\right)$

$KS_A=(1763,611);\quad KP_A=(1763,11)$

38

Thuật toán kí số RSA

❑**Kí số và kiểm tra chữ kí**

- Kí số: **sign(m) = s = m^d (mod n)**
- Kiểm tra: **s^e == m (mod n)**

❑**Ví dụ:**

$m=100;\quad KS_A=(1763,611);\quad KP_A=(1763,11)$

$sign(m)=s=m^d=100^{611}=1658\left(\mathrm{mod}1763\right)$

$s^e=1658^{11}=100=m\left(\mathrm{mod}1763\right)$

39

1. Hàm băm
2. Tấn công từ điển
3. Một số thuật toán mật mã khóa công khai điển hình