Mật mã & Ứng dụng

Trần Đức Khánh
Bộ môn HTTT – Viện CNTT&TT
ĐH BKHN

Chủ đề

- Hệ mật mã cổ điển
- Hệ mật mã khóa bí mật (đối xứng)
- Hệ mật mã khóa công khai (bất đối xứng)
- Hàm băm, chữ ký số
- Quản lý khóa, giao thức mật mã,…

Tại sao Hệ mật mã khóa công khai

- Hệ mật mã khóa đối xứng không đáp ứng được 2 mục tiêu an toàn
  - Xác thực
    - Alice và Bob trao đổi thông tin bí mật
    - Alice cần phải biết thông tin chắc chắn đến từ Bob, và ngược lại
  - Chống phủ nhận
    - Alice và Bob trao đổi thông tin bí mật
    - Nếu Alice đã gửi thông tin nào đó cho Bob thì Alice không thể chối bỏ thông tin đó là của mình

Tại sao Hệ mật mã khóa công khai

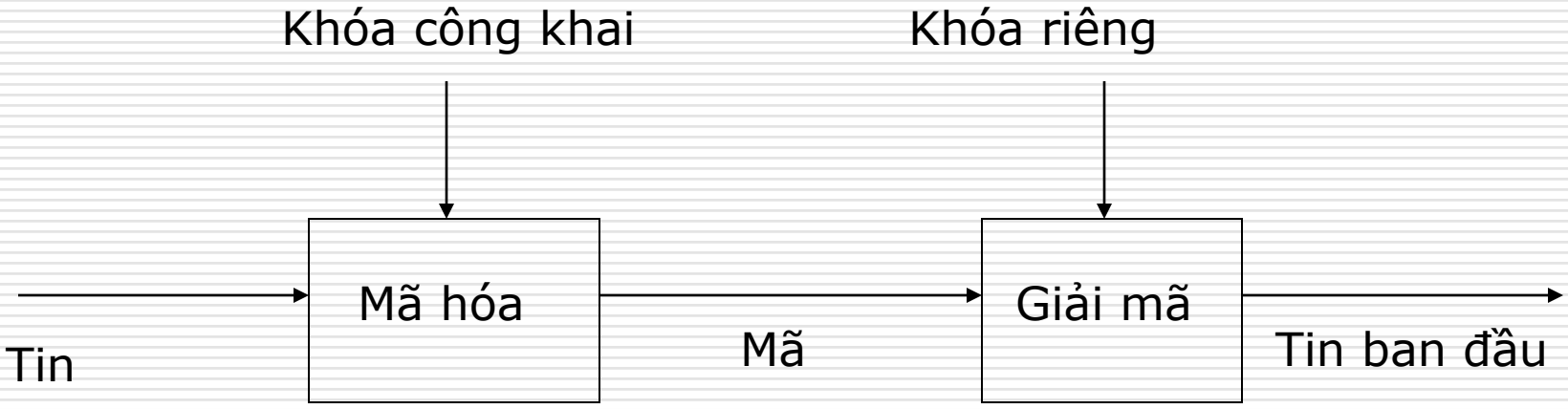
- Quản lý khóa đối xứng là một vấn đề nan giải
  - Trong các hệ khóa đối xứng, mỗi cặp người dùng phải có khóa riêng
  - *N* người dùng cần *N * (N-1)/2* khóa
  - Việc quản lý khóa trở nên phức tạp khi số lượng người dùng tăng

Hệ mật mã khóa công khai

- Mỗi người dùng có 1 khóa riêng và 1 khóa công khai
  - Khóa riêng bí mật
  - Khóa công khai có thể chia xẻ
- Quản lý khóa
  - N người dùng cần N khóa công khai được xác thực
  - Hạ tầng khóa công khai PKI

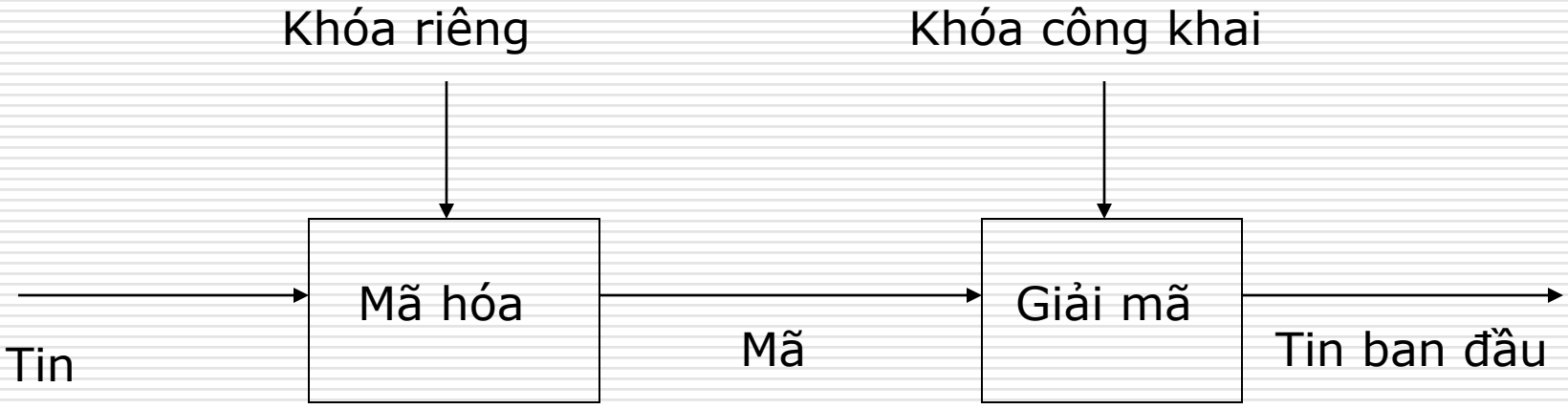
Hệ mật mã khóa công khai

- Mã hóa dùng khóa công khai k
  - $C = E(k,M)$
- Giải mã dùng khóa riêng K
  - $M = D(K,C)$



Hệ mật mã khóa công khai

- Mã hóa dùng khóa riêng K
  - $C = E(K,M)$
- Giải mã dùng khóa công khai k
  - $M = D(k,C)$



Khóa bí mật vs. Khóa công khai

	Khóa bí mật	Khóa công khai
Số khóa	1	2
Bảo vệ khóa	Khóa được giữ bí mật	1 khóa bí mật 1 khóa công khai
Ứng dụng	Bí mật và toàn vẹn dữ liệu	Trao đổi khóa Xác thực
Tốc độ	Nhanh	Chậm

Hệ mật mã khóa công khai

- Lý thuyết nền tảng
  - Độ phức tạp
  - Số học đồng dư (Modular Arithmetic)
- Các hệ Mật mã khóa công khai
  - RSA
  - MerkleHellman
  - ElGamal
  - Rabin
  - Đường cong êlip (Elliptic Curve)
  - …

Độ phức tạp

- Độ phức tạp tính toán (thời gian)
  - Vấn đề "dễ": lớp P
  - Vấn đề "khó": lớp NP
- Giải quyết các vấn đề P
  - Số trường hợp phải xét đến là một hàm đa thức
- Giải quyết các vấn đề NP
  - Số trường hợp phải xét đến là hàm lũy thừa

Các hệ mật mã khóa công khai dựa trên độ khó/phức tạp của giải thuật bẻ khóa

Số học đồng dư

- Số học đồng dư
  - a mod n
  - a op b mod n
    - op = +, -, *, /, ^
- Ví dụ:
  - 40 mod 6 = 4
  - 5 + 2 mod 6 = 1
  - 9 – 4 mod 3 = 2
  - 5 * 3 mod 6 = 3
  - 4/2 mod 3 = 2
  - 2^4 mod 6 = 4

Số học đồng dư

- a mod n
  - Số dư của a chia n
- a + b mod n
  - Số dư của a + b chia n
- a - b mod n
  - Số dư của a - b chia n
- a * b mod n
  - Số dư của a * b chia n
- a ^ b mod n
  - Thủ tục bình phương
- a / b mod n
  - Giải thuật Euclide mở rộng

Thủ tục bình phương

- Dựa vào tính chất
  - a*b mod n = ((a mod n)*(b mod n)) mod n
- Tính a^25
  - a^25 = a^(11001)
  - a^(11001) = a^(10000+1000+1)
  - a^(10000+1000+1) = a^10000 * a^1000 * a^1
  - a^10000 * a^1000 * a^1 = a^16 * a^8 * a^1
- Độ phức tạp (O(logb*(logs)^2))
- Hiệu quả hơn phương pháp tính lũy thừa bằng phép nhân đồng dư (O(b*(logs)^2))

Thủ tục bình phương

ModExp1(a,b, s)

- Vào:
  - 3 số nguyên dương a,b,s sao cho a < s
  - bn−1 ⋯b1b0 là biểu diễn nhị phân của b, n = [logb]
- Ra: a^b mod s

```
p[0] = a mod s
for i = 1 to n−1
    p[i] = p[i−1]^2 mod s
r = 1
for i = 0 to n−1
    if b[i] = 1 then r = r*p[i] mod s
return r
```

Bài tập

- Tính 6^73 mod 100
  - 73 = 2^0 + 2^3 + 2^6
  - 6^73 = 6 * 6^(2^3)*6^(2^6)
  - 6 = 6 mod 100
  - 6^(2^3) = 16 mod 100
  - 6^(2^6) = -4 mod 100
  - 6^73 = 6 * (16) * (-4) = 16 mod 100

Giải thuật Euclide mở rộng

- Giải thuật Euclide
  - Tính ƯSCLN(a,b)
  - Dựa trên tính chất
    - Nếu a > b thì ƯSCLN(a,b) = ƯSCLN(a mod b,b)
- Giải thuật Euclide mở rộng
  - Tính 2 số x, y sao cho
    - a*x + b*y = ƯSCLN(a,b)
  - Giải quyết bài toán tìm x sao cho
    - a*x = 1 mod s

Giải thuật Euclide mở rộng

Extended-Euclid(a,b)

- Vào: 2 số nguyên dương a,b
- Ra: 3 số nguyên x,y,d sao cho
  d = ƯSCLN(a,b) và ax+by = d

1. Nếu b = 0 thì trả về (1,0,a)
2. Tìm q, r sao cho a = b*q+r
3. (x’,y’,d) = Extended-Euclid(b, r)
4. Trả về (y’,x’−q*y’,d)

Bài tập

- Dùng giải thuật Euclide mở rộng để tìm ƯSCLN(120,23)

a	b	q	r	x	y	d
120	23	5	5	-9	47	1
23	5	4	3	2	-9	1
5	3	1	2	-1	2	1
3	2	1	1	1	-1	1
2	1	2	0	0	1	1
1	0	_	_	1	0	1

Bài tập

- Dùng giải thuật Euclide mở rộng để tìm tìm x sao cho 51*x mod 100 = 1
  - Nếu a*x mod n = 1 thì tồn tại k trong đó a*x = 1 + n*k
  - Ta có a*x – n*k = 1
  - Đặt y = -k, ta được a*x + b*y = 1
  - Tìm x,y bằng giải thuật Euclide mở rộng
    - x = -49, y = 25

Hệ Mật mã khóa công khai RSA

- RSA
  - 1978 Rivest, Shamir và Adlerman phát minh ra hệ mật mã RSA
  - Hệ mật mã khóa công khai phổ biến và đa năng nhất trong thực tế
  - Sử dụng các kết quả trong số học đồng dư
  - Dựa trên độ phức tạp của bài toán
    - *phân tích số nguyên ra thừa số nguyên tố*

RSA – Tạo khóa

- Chọn ngẫu nhiên 2 số nguyên tố p, q
  - n = p * q
- Chọn e sao cho
  - 1 < e < (p-1) * (q-1)
  - ƯSCLN(e, (p-1) * (q-1)) = 1
- Chọn d sao cho
  - 1 < d < (p-1) * (q-1)
  - e*d = 1 mod ((p-1) * (q-1))
- Khóa công khai
  - (n,e)
- Khóa riêng
  - (p,q,d)

RSA – Tạo khóa

- Ví dụ
  - p = 11, q = 23
  - n = 11*23 = 253
  - (p-1)*(q-1) = 10*22=220
  - ƯSCLN(e,220) = 1
    - giá trị nhỏ nhất e = 3
  - áp dụng giải thuật Euclide mở rộng
    - d = 147

RSA – Mã hóa

- Mã hóa sử dụng khóa công khai
  - Tin m
  - Khóa công khai (n,e)
  - Mã
    - c = m^e mod n

RSA – Mã hóa

- Ví dụ
  - p = 11, q = 23
  - n = 11*23 = 253
  - (p-1)*(q-1) = 10*22=220
  - e = 3
  - d = 147
  - Tin m = 165
  - Mã
    - c = 165^3 mod 253 = 110

RSA – Giải mã

- Tin m
- Khóa công khai (n,e)
- Khóa riêng (p,q,d)
- Mã c = m^e mod n
- Giải mã
  - m = c^d mod n

RSA – Giải mã

- Ví dụ
  - p = 11, q = 23
  - n = 11*23 = 253
  - (p-1)*(q-1) = 10*22=220
  - e = 3
  - d = 147
  - Mã
    - c = 165^3 mod 253 = 110
  - Tin
    - m = 110^147 mod 253 = 165

RSA – Định lý RSA

Nếu

- (n,e) là khóa công khai
- (p,q,d) là khóa riêng
- 0 <= m < n

thì

$$(m^e)^d \bmod n = m$$

RSA – Định lý Euler & Fermat

Nếu

- ef(n) là số “số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n”
- x và n là hai số nguyên tố cùng nhau

thì

$$x^{ef(n)} = 1 \bmod n$$

RSA- Độ an toàn

- RSA và bài toán phân tích thừa số nguyên tố
  - Khóa công khai (n,e)
  - Khóa riêng (p,q,d) được giữ bí mật
  - Độ an toàn của RSA dựa trên độ khó/phức tạp của bài toán tính (p,q,d) từ (n,e)
    - p,q là 2 số nguyên tố,
    - n = p*q
    - e,d được tính từ p,q
  - Do đó bài toán trên qui về bài toán PTTSNT(n)

RSA- Độ an toàn

- Lựa chọn p,q
  - Đảm bảo rằng bài toán PTTSNT(n) thực sự khó
  - Tránh tình trạng p,q rơi vào những trường hợp đặc biệt mà bài toán trên trở nên dễ dàng
    - Ví dụ: p-1 có các thừa số nguyên tố nhỏ
  - p,q phải có độ dài tối thiểu là 512 bít
  - p,q xấp xỉ nhau

RSA- Độ an toàn

- Lựa chọn e
  - e nhỏ nhất có thể
  - e không nhỏ quá để tránh bị tấn công theo dạng “low exponent”
- Lựa chọn d
  - d không nhỏ quá ($d < n/4$) để tránh tấn công dạng “low decryption”

RSA – Hiệu năng

- Nhân, chia, số dư phép chia
- Tính lũy thừa modulo
  - m^e mod n
  - c^d mod n
- Tốc độ rất chậm so với DES

Các Mật mã khóa công khai khác

- MerkleHellman
- ElGamal
- Rabin
- Đường cong êlip (Elliptic Curve)
- …

RSA – Bài tập

- Cho p = 7, q = 11. Giả sử Alice dùng khóa công khai (n,e) = (77,17).

  Tìm khóa riêng.

  Biết rằng các ký tự từ A đến Z được biểu diễn bằng các số nguyên từ 00 đến 25. Dấu cách được biểu diễn bằng số 26.

  Bob muốn gửi cho Alice Tin "HELLO WORLD" sử dụng hệ mật mã RSA.

  Tính Mã tương ứng.

  Giải Mã.

- Đáp án
  - (p,q,d) = (7,11,53)
  - Tin
    - H E L L O W O R L D
    - 07 04 11 11 14 26 22 14 17 11 03
  - Mã
    - 28 16 44 44 42 38 22 42 19 44 75

Bài tập

- Chứng minh Định lý Euler & Fermat
- Chứng minh Định lý RSA