KSTP.Ebook

Hoàng Thu Phương - Khoa ATTT

Chương 3. Mật mã khoá công khai

Nội dung chính

1. Giới thiệu
2. Một số kiến thức toán học
3. Một số hệ mật khoá công khai

1. Giới thiệu

- Trong hệ mật khóa đối xứng thì khóa phải được chia sẻ giữa hai bên trên một kênh an toàn trước khi gửi một bản mã bất kì. Trên thực tế điều này rất khó đảm bảo.
- Ý tưởng về một hệ mật khoá công khai được Diffie và Hellman đưa ra vào năm 1976
- Rivesrt, Shamir và Adleman hiện thực hóa ý tưởng trên vào năm 1977, họ đã tạo nên hệ mật nổi tiếng RSA..

1. Giới thiệu

- Đặc điểm của hệ mật KCK:
  - Mỗi bên có một khoá công khai và một khoá bí mật.
  - Bên gửi dùng khoá công khai của bên nhận để mã hoá.
  - Bên nhận dùng khoá bí mật của mình để giải mã.

1. Giới thiệu

- Hệ mật RSA:
  - Độ bảo mật của hệ RSA dựa trên độ khó của việc phân tích ra thừa số nguyên lớn
- Hệ mật xếp ba lô Merkle - Hellman:
  - Hệ này và các hệ liên quan dựa trên tính khó giải của bài toán tổng các tập con (bài toán này là bài toán NP đầy đủ).

1. Giới thiệu

- Hệ mật McEliece:
  - Hệ này dựa trên lý thuyết mã đại số và vẫn còn được coi là an toàn. Hệ mật McEliece dựa trên bài toán giải mã cho các mã tuyến tính (cũng là một bài toán NP đầy đủ)
- Hệ mật ElGamal:
  - Hệ mật ElGamal dựa trên tính khó giải của bài toán logarithm rời rạc trên các trường hữu hạn

1. Giới thiệu

- Hệ mật Chor-Rivest:
  - Hệ mật Chor-Rivest cũng được xem như mọt hệ mật xếp ba lô. Tuy nhiên nó vẫn được coi là an toàn
- Hệ mật trên các đường cong Elliptic:
  - Các hệ mật này là biến tướng của các hệ mật khác (chẳng hạn như hệ mật ElGamal), chúng làm việc trên các đường cong Elliptic chứ không phải là trên các trường hữu hạn. Hệ mật này đảm bảo độ mật với số khoá nhỏ hơn các hệ mật khoá công khai khác.

1. Giới thiệu

- Một chú ý quan trọng là một hệ mật khoá công khai không bao giờ có thể đảm bảo được độ mật tuyệt đối (an toàn vô điều kiện).
- Ta chỉ nghiên cứu độ mật về mặt tính toán của các hệ mật này.

1. Giới thiệu

- Một số khái niệm trong hệ mật KCK:
  - **Đặc tính một chiều:** Hàm mã khoá công khai e_k của Bob phải là một hàm dễ tính toán. Song việc tìm hàm ngược (hàm giải mã) rất khó khăn (đối với bất kỳ ai không phải là Bob)
    - Ví dụ: Giả sử n là tích của hai số nguyên tố lớn p và q, giả sử b là một số nguyên dương. Khi đó hàm $f(x) = x^b \bmod n$ là một hàm một chiều.
  - **Hàm cửa sập một chiều:** thông tin bí mật cho phép Bob dễ dàng tìm hàm của e_k.

2. Một số kiến thức toán học

- Cấu trúc đại số
- Số học modulo

2. Một số kiến thức toán học

- **Cấu trúc đại số:**
  - **Định nghĩa nhóm.** Tập hợp G đó với phép toán **.** đã cho được gọi là **nhóm**, nếu nó thỏa mãn các tính chất sau với mọi phần tử a, b, c thuộc G:
    - Tính kết hợp (a.b).c = a.(b.c)
    - Có đơn vị e: e.a = a.e = a
    - Có nghịch đảo a-1: a.a-1 = e
    - Nếu có thêm tính giao hoán a.b = b.a, thì gọi là nhóm Aben hay nhóm giao hoán.

2. Một số kiến thức toán học

- **Định nghĩa nhóm xyclic.**
  - Định nghĩa lũy thừa như là việc áp dụng lặp phép toán:
    Ví dụ: $a^3 = a.a.a$
  - Và đơn vị $e=a^0$
  - Một nhóm được gọi là xyclic nếu mọi phần tử đều là lũy thừa của một phần tử cố định nào đó. Chẳng hạn $b = a^k$ đối với a cố định và mỗi b trong nhóm. Khi đó a được gọi là phần tử sinh của nhóm.

2. Một số kiến thức toán học

- **Vành:** Cho một tập R các "số" với hai phép toán được gọi là cộng và nhân. Ở đây "số" được hiểu là phần tử của tập hợp và hai phép toán trên xác định trên tập hợp đó. Tập với hai phép toán trên được gọi là **vành,** nếu hai phép toán thoả mãn các tính chất sau:
  - Với phép cộng, R là nhóm Aben
  - Với phép nhân, có:
    - tính đóng và
    - tính kết hợp
    - tính phân phối đối với phép cộng $a(b+c) = ab + ac$
  - Nếu phép nhân có tính giao hoán thì tạo thành **vành giao hoán.**
  - Nếu phép nhân có nghịch đảo và không có thương 0 (tức là không có hai phần khác 0 mà tích của chúng lại bằng 0), thì nó tạo thành **miền nguyên**

2. Một số kiến thức toán học

- **Trường** là một tập hợp F với hai phép toán cộng và nhân, thoả mãn tính chất sau:
  - Với phép cộng F là nhóm Aben
  - Với phép nhân F trừ phần tử 0 là nhóm Aben.
  - F là một vành

  Có thể nói là có các phép toán cộng, trừ, nhân, chia số khác 0. Phép trừ được coi như là cộng với số đối của phép cộng và phép chia là nhân với số đối của phép nhân:

$$a - b = a + (-b)$$

$$a / b = a.b^{-1}$$

- **Ví dụ:** Dễ dàng thấy, với phép cộng và nhân thông thường:
  - Tập số nguyên Z là nhóm Aben với phép cộng
  - Tập số nguyên Z là vành giao hoán.
  - Tập số hữu tỉ Q là trường.
  - Tập số thực R là trường.
  - Tập số phức C là trường với phép cộng và nhân hai số phức.

2. Một số kiến thức toán học

- Số học modulo
  - Cho số tự nhiên n và số nguyên a. Ta định nghĩa: a mod n là phần dư dương khi chia a cho n.
  - Định nghĩa quan hệ tương đương trên tập số nguyên $a \equiv b \bmod n$ khi và chỉ khi a và b có phần dư như nhau khi chia cho n.

2. Một số kiến thức toán học

- Ví dụ: 100 mod 11 = 1; 34 mod 11 = 1, nên 100 ≡ 34 mod 11
- Số b được gọi là đại diện của a, nếu a ≡ b mod n (a = qn + b) và 0 <= b < n.
- Ví dụ: -12 mod 7 ≡ -5 mod 7 ≡ 2 mod 7 ≡ 9 mod 7. Ở đây 2 là đại diện của –12, -5, 2 và 9.
- Trong Modulo 7 ta có các lớp tương đương viết trên các hàng như sau:
- Các phần tử cùng cột là có quan hệ đồng dư với nhau.
- Tập các đại diện của các số nguyên theo Modulo n gồm n phần tử ký hiệu như sau:

$$Z_n = \{ 0, 1, 2, 3, \ldots, n-1 \}.$$

```
...
-21 -20 -19 -18 -17 -16 -15
-14 -13 -12 -11 -10  -9  -8
-7  -6  -5  -4  -3  -2  -1
 0   1   2   3   4   5   6
 7   8   9  10  11  12  13
14  15  16  17  18  19  20
21  22  23  24  25  26  27
28  29  30  31  32  33  34
...
```

2. Một số kiến thức toán học

- **Ước số**
  - Số b không âm được gọi là ước số của a, nếu có số m sao cho: a = mb trong đó a, b, m đều nguyên.
  - Tức là a chia hết cho b, ký hiệu là b|a
  - Ví dụ: 1, 2, 3, 4, 6, 8, 12, 24 là các ước số của 24

2. Một số kiến thức toán học

- **Các phép toán số học trên Modulo**
  - Cho trước một số n. Ta muốn thực hiện các phép toán theo Modulo của n. Ta có thể thực hiện các phép toán trên các số nguyên như các phép cộng, nhân các số nguyên thông thường sau đó rút gọn lại bằng phép lấy Modulo hoặc cũng có thể vừa tính toán, kết hợp với rút gọn tại bất cứ thời điểm nào:

$$(a+b) \bmod n = [a \bmod n + b \bmod n] \bmod n \quad (*)$$

$$(a.b) \bmod n = [a \bmod n \,.\, b \bmod n] \bmod n \quad (**)$$

  - Như vậy khi thực hiện các phép toán ta có thể thay các số bằng các số tương đương theo Modulo n đó hoặc đơn giản hơn có thể thực hiện các phép toán trên các đại diện của nó: $Z_n = \{ 0, 1, 2, 3, \ldots, n-1 \}$.

2. Một số kiến thức toán học

- Zn với các phép toán theo Modulo tạo thành vành giao hoán có đơn vị. Các tính chất kết hợp, giao hoán và nghịch đảo được suy ra từ các tính chất tương ứng của các số nguyên.
- Các chú ý về tính chất rút gọn:
  - Nếu $(a+b)\equiv(a+c) \bmod n$, thì $b\equiv c \bmod n$
  - Nhưng $(ab)\equiv(ac) \bmod n$, thì $b\equiv c \bmod n$ chỉ khi nếu a là nguyên tố cùng nhau với n
- Ví dụ: Tính $(11*19 + 10^{17}) \bmod 7 = ?$

2. Một số kiến thức toán học

Ví dụ. Áp dụng các tính chất của modulo:

$(11*19 + 10^{17}) \bmod 7 =$

$((11*19) \bmod 7 + 10^{17} \bmod 7) \bmod 7 =$

$((11 \bmod 7 * 19 \bmod 7) \bmod 7 + (10 \bmod 7)^{17} \bmod 7) \bmod 7 =$

$((4.(-2)) \bmod 7 + (((3^2)^2)^2)^2 * 3 \bmod 7) \bmod 7 =$

$((-1) \bmod 7 + ((2^2)^2)^2 * 3 \bmod 7) \bmod 7 =$

$(-1 + 5) \bmod 7 =$

4

2. Một số kiến thức toán học

- Ví dụ: bảng modulo 8 với phép cộng

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

2. Một số kiến thức toán học

- **Ước số chung lớn nhất.**
  - *Bài toán:* Cho hai số nguyên dương a và b. Bài toán tìm ước chung lớn nhất của hai số nguyên dương là bài toán chung của lý thuyết số. Ta ký hiệu GCD(a,b) là ước số chung dương lớn nhất của a và b, tức là số nguyên dương vừa là ước của a vừa là ước của b và là số nguyên dương lớn nhất có tính chất đó.
  - **Ví dụ**: GCD(60,24) = 12 ; GCD (6, 15) = 3;
    GCD(8, 21) = 1.

2. Một số kiến thức toán học

- **Nguyên tố cùng nhau**: Ta thấy 1 bao giờ cũng là ước số chung của hai số nguyên dương bất kỳ. Nếu GCD(a, b) = 1, thì a, b được gọi là hai số nguyên tố cùng nhau:
  - **Ví dụ:** GCD(8,15) = 1, tức là 8 v à 15 là hai số nguyên tố cùng nhau

2. Một số kiến thức toán học

- **Tìm ước chung lớn nhất**. Bây giờ chúng ta xét bài toán tìm ước số chung lớn nhất của hai số nguyên dương cho trước. Dễ dàng chứng minh được tính chất sau:

$$GCD(a,b) = GCD(b, a \bmod b)$$

- Như vậy để tìm ước số chung của một cặp số cho trước, ta đưa về bài toán tìm ước chung của cặp số gồm số nhỏ hơn trong hai số đó và phần dư của số lớn khi chia cho số nhỏ hơn. Thuật toán Ơcơlít tạo nên vòng lặp, ở mỗi bước ta áp dụng tính chất trên cho đến khi phần dư đó còn khác 0.

2. Một số kiến thức toán học

- **Thuật toán Ơcơlit tìm GCD(a, b)**

  A=a, B=b

  while B>0

  R = A mod B

  A = B, B = R

  return A

2. Một số kiến thức toán học

- **Ví dụ**: GCD(1970,1066)

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	

gcd(1970, 1066) = 2

2. Một số kiến thức toán học

- **Trường Galoa**
  - Ta muốn đi tìm một trường số có hữu hạn các phần tử, tức là một tập hữu hạn các phần tử mà ở đó có thể cộng trừ, nhân, chia mà không vượt ra ngoài phạm vi tập hữu hạn các phần tử đó. Trường Galoa thuộc loại đó và đóng vai trò quan trọng trong lý thuyết mã.
  - Có thể chứng minh được rằng số các phần tử của trường hữu hạn bất kỳ bằng lũy thừa của p^m của sô nguyên tố p nào đó, ta ký hiệu trường Galoa đó là $GL(p^m)$. Thông thường ta sử dụng các trường: GL(p) và $GL(2^m)$.Sau đây chúng ta sẽ xây dựng các trường Galoa đó.

2. Một số kiến thức toán học

- **Trường Galoa** GL(p), với p là số nguyên tố.
  - GL(p) gồm tập {0,1, … , p-1}.
  - Với các phép toán cộng và nhân Modulo, như ta đã biết GL(p) tạo thành một vành giao hoán. Vì p là số nguyên tố nên mọi số khác 0 nhỏ hơn p đều nguyên tố cùng nhau với p.
  - GL(p) tạo thành trường vì mọi a thuộc {1, … , p-1} đều có phần tử nghịch đảo a^{-1}: $a \cdot a^{-1} = 1$. Thực vậy vì a và p nguyên tố cùng nhau nên theo thuật toán tìm nghịch đảo dưới đây ta sẽ tìm được nghịch đảo của a.
  - Như vậy trên GL(p) ta có thể thực hiện các phép toán cộng, trừ, nhân, chia.

2. Một số kiến thức toán học

Ví dụ phép nhân trên GL(7)

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplication modulo 7

2. Một số kiến thức toán học

- **Tìm số nghịch đảo:** Bây giờ ta xét bài toán: nếu GCD(m, b) = 1, thì tìm nghịch đảo của b theo Modulo m. Ta mở rộng thuật toán Ơcơlit vừa tìm ước chung lớn nhất của m và b, vừa tính nghịch đảo trong trường hợp GCD(m, b) = 1.
- **Thuật toán Euclid mở rộng:**

EXTENDED EUCLID(*m*, *b*)

1. (A1, A2, A3)=(1, 0, *m*);
(B1, B2, B3)=(0, 1, *b*)

2. **if** B3 = 0
return A3 = gcd(*m*, *b*); no inverse

3. **if** B3 = 1
return B3 = gcd(*m*, *b*); B2 = *b*–1 mod *m*

4. Q = A3 div B3

5. (T1,T2,T3)=(A1 – Q*B1,A2 – Q*B2, A3 – Q*B3)

6. (A1, A2, A3)=(B1, B2, B3)

7. (B1, B2, B3)=(T1, T2, T3)

8. **goto** 2

2. Một số kiến thức toán học

- Chứng minh tính đúng đắn của thuật toán Ơcơlit mở rộng.
- Áp dụng thuật toán mở rộng với các đầu vào:
  - b = 550; m = 1759
  - b = 4864; m = 3458

2. Một số kiến thức toán học

Q	A1	A2	A3	B1	B2	B3
–	1	0	1759	0	1	550
3	0	1	550	1	-3	109
5	1	-3	109	-5	16	5
21	-5	16	5	106	-339	4
1	106	-339	4	-111	355	1

$\Rightarrow$ GCD(1759, 550) = 1 và 550^{-1} mod 1759 = 355

2. Một số kiến thức toán học

- **Số học đa thức**
  - Ta xét tập các đa thức Pn có bậc nhỏ hơn hoặc bằng n:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

  - Trên tập các đa thức đó ta có thể có một số cách khác nhau thực hiện các phép toán cộng và nhân đa thức

2. Một số kiến thức toán học

- Phép toán đa thức thông thường
  - Cộng trừ các hệ số tương ứng
  - Nhân mọi hệ số với cùng một số.
    - Ví dụ: $f(x) = x^3 + x^2 + 2$ và $g(x) = x^2 - x + 1$

$$f(x) + g(x) = x^3 + 2x^2 - x + 3$$

$$f(x) - g(x) = x^3 + x + 1$$

$$f(x) \,.\, g(x) = x^5 + 3x^2 - 2x + 2$$

2. Một số kiến thức toán học

- Phép toán đa thức với Modulo hệ số
  - Cho số nguyên tố p tùy ý
  - Tính các hệ số theo Modulo p. Khi đó tập các hệ số được lấy từ trường GL(p). Còn phép nhân đa thức có thể nhận được kết quả là đa thức bậc lớn hơn n.
  - Ta thường quan tâm đến Mod 2, tức là mọi hệ số là 0 hoặc 1
    - Ví dụ: $f(x) = x^3 + x^2$ và $g(x) = x^2 + x + 1$

      $\Rightarrow f(x) + g(x) = x3 + x + 1$

      $\Rightarrow f(x) \,.\, g(x) = x5 + x2$

2. Một số kiến thức toán học

- **Phép toán đa thức với Modulo đa thức**
  - Cho đa thức g(x) bậc n và các hệ số của các đa thức xét trong mục này lấy trong trường Galoa GF(p) với p là số nguyên tố. Viết đa thức f(x) dưới dạng:

$$f(x) = q(x)\, g(x) + r(x)$$

trong đó r(x) là phần dư khi chia f(x) cho g(x). Rõ ràng bậc của r(x) sẽ nhỏ hơn bậc của g(x).Ta viết:

$$r(x) = f(x) \bmod g(x)$$

2. Một số kiến thức toán học

- Nếu không có phần dư, tức là $r(x) = 0$, ta nói g(x) là ước của f(x) hay g(x) chia hết f(x) hay f(x) chia hết cho g(x).
- Trong trường hợp g(x) không có ước ngoài 1 và chính nó, thì ta nói g(x) là đa thức nguyên tố hoặc không rút gọn được. Ví dụ $g(x) = x^3 + x + 1$ là đa thức nguyên tố.
- Việc tìm ước chung lớn nhất của hai đa thức được trình bày trong thuật toán tương tự như Ơcolit như sau:

2. Một số kiến thức toán học

- **Tìm đa thức ước chung lớn nhất GCD(a(x), b(x))**
  - $c(x) = \text{GCD}(a(x), b(x))$ nếu $c(x)$ là đa thức bậc lớn nhất mà chia hết cả $a(x), b(x)$
  - Có thể điều chỉnh thuật toán Euclid's Algorithm để tìm nó:

    EUCLID[$a(x), b(x)$]

    1. $A(x) = a(x)$; $B(x) = b(x)$

    2. if $B(x) = 0$ **return** $A(x) = \text{gcd}[a(x), b(x)]$

    3. $R(x) = A(x) \bmod B(x)$

    4. $A(x) \leftarrow B(x)$

    5. $B(x) \leftarrow R(x)$

    6. goto 2

2. Một số kiến thức toán học

- **Phép toán đa thức với Modulo đa thức.**
  - Cho g(x) là đa thức nguyên tố bậc n. Khi đó tập các đa thức bậc nhỏ hơn bằng n với các phép toán cộng và nhân đa thức theo Modulo của đa thức nguyên tố g(x) tạo thành trường hữu hạn, gọi là **trường Galoa** và ký hiệu là $GL(p^n)$.
  - Sau đây ta xét trường $GF(2^n)$, tức là xét tập các đa thức với các hệ số Modulo 2 và bậc nhỏ hơn bằng n và phép toán nhân có thể rút gọn theo Modulo của đa thức g(x) nguyên tố bậc n

2. Một số kiến thức toán học

Ví dụ GF(2^3)

Polynomial Arithmetic Modulo ($x^3 + x + 1$)

+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000 0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001 1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010 x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011 $x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100 x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101 x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110 x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111 x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000 0	0	0	0	0	0	0	0	0
001 1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010 x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011 $x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100 x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101 x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110 x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111 x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

2. Một số kiến thức toán học

- **Ví dụ:** Trong $GF(2^3)$ ta có (x^2+1) tương ứng dãy bít 101_2 và (x^2+x+1) tương ứng với dãy 111_2
- Tổng hai đa thức trên là
  - $(x^2+1) + (x^2+x+1) = x$
  - $101 \text{ XOR } 111 = 010_2$
- Tích của hai đa thức là
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1) = x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011.101 = (101)<<1 \text{ XOR } (101)<<0 = 1010 \text{ XOR } 101 = 1111_2$

2. Một số kiến thức toán học

- Phép rút gọn theo Modulo là:
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = (x^3+x^2+x+1) - (x^3+x+1)$
    $= x^2$
  - $1111 \bmod 1011 = 1111 \text{ XOR } 1011 = 0100_2$
- Như vậy trường Galoa GL(2^n) bao gồm 2^n phần tử. Muốn trường Galoa có số phần tử lớn tuỳ ý, ta chỉ việc tăng và lấy n thích hợp.
- Đặc biệt việc tính toán các phép toán cộng trừ, nhân, chia trên đó rất nhanh và hiệu quả trên các thao tác của các thiết bị phần cứng $\Rightarrow$ trường Galoa đóng vai trò quan trọng trong lý thuyết mã

2. Một số kiến thức toán học

- **Giới thiệu lý thuyết số**
  - **Các số nguyên tố**
    - Như chúng ta đã biết số nguyên tố là các số nguyên dương chỉ có ước số là 1 và chính nó. Chúng không thể được viết dưới dạng tích của các số khác.
    - Các số nguyên tố là trung tâm của lý thuyết số. Số các số nguyên tố là vô hạn.
      - *Ví dụ:* Danh sách các số nguyên tố nhỏ hơn 200:

        2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

2. Một số kiến thức toán học

- Một trong những bài toán cơ bản của số học là phân tích ra thừa số nguyên tố số a, tức là viết nó dưới dạng tích của các số nguyên tố.
- Lưu ý rằng phân tích là bài toán khó hơn rất nhiều so với bài toán nhân các số để nhận được tích.
- Ta có kết luận: mọi số nguyên dương đều có phân tích duy nhất thành tích các lũy thừa của các số nguyên tố
  - **Ví dụ:** $51=3x17$; $3600=2^4\times3^2\times5^2$

2. Một số kiến thức toán học

- **Các số nguyên tố cùng nhau và GCD**
  - Hai số nguyên dương a và b không có ước chung nào ngoài 1, được gọi là nguyên tố cùng nhau.
    - **Ví dụ:** 8 và 15 là nguyên tố cùng nhau, vì ước của 8 là 1, 2, 4, 8, còn ước của 15 là 1, 3, 5, 15. Chỉ có 1 là ước chung của 8 và 15.
  - Ngược lại có thể xác định ước chung lớn nhất bằng cách trong các phân tích ra thừa số của chúng, tìm các thừa số nguyên tố chung và lấy bậc lũy thừa nhỏ nhất trong hai phân tích của hai số đó.
    - **Ví dụ.** Ta có phân tích: $300=2^2 \times 3^1 \times 5^2$ và $18=2^1 \times 3^2$. Vậy $GCD(18,300)=2^1 \times 3^1 \times 5^0=6$

2. Một số kiến thức toán học

- **Định lý Ferma (Định lý Ferma nhỏ)**

$$a^{p-1} \bmod p = 1$$

trong đó plà số nguyên tố và a là số nguyên bất kỳ khác bội của p: GCD(a, p) = 1.

  - Hay với mọi số nguyên tố p và số nguyên a không là bội của p, ta luôn có

$$a^p = a \bmod p$$

  - Công thức trên luôn đúng, nếu p là số nguyên tố, còn a là số nguyên dương nhỏ hơn p.

2. Một số kiến thức toán học

- **Ví dụ:** Vì 5 và 7 là các số nguyên tố. 2 và 3 không là bội tương ứng của 7 và 5, nên theo định lý Ferma ta có:

  $2^{7-1} \bmod 7 = 1 \; (= 2^6 \bmod 7 = 64 \bmod 7 = 1)$

  $3^{5-1} \bmod 5 = 1 \; (= 3^4 \bmod 5 = 81 \bmod 5 = 1)$

- Kết quả trên được dùng trong khoá công khai. Nó cũng được sử dụng để kiểm tra tính nguyên tố của một số nguyên p nào đó. (?)

2. Một số kiến thức toán học

- **Hàm Ole**
  - Cho n là một số nguyên dương. Khi thực hiện phép tính đồng dư n của mọi số nguyên khác ta nhận được tập đầy đủ các phần dư có thể có là:

    $$0, 1, 2, \ldots, n-1$$

  - Từ tập trên ta tìm tập rút gọn $\Phi(n)$ bao gồm các số nguyên tố cùng nhau với n và quan tâm đến số lượng các phần tử như vậy đối với số nguyên dương n cho trước.

2. Một số kiến thức toán học

- Các tính chất của hàm Φ(n):
  - Dễ dàng thấy, nếu p là số nguyên tố Φ(p) = p-1
  - Nếu (m, n) = 1, thì: Φ(m.n) = Φ(m).Φ(n)
  - Nếu $n = p_1^{e1} \dots p_k^{ek}$ là phân tích ra thừa số nguyên tố của n thì:

$$\Phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right)$$

2. Một số kiến thức toán học

- Ví dụ:
  - Tính Φ(37); Φ(25); Φ(18); Φ(21)?

Φ(37) = 37 – 1 = 36

Φ(25) = Φ(5^2) = 20

Φ(18) = Φ(2). Φ(9) = 1. Φ(3^2) = 6

Φ(21) = Φ(3). Φ(7) = 2.6 = 12

2. Một số kiến thức toán học

- **Định lý Ole:** Định lý Ole là tổng quát hoá của Định lý Ferma

$$a^{\Phi(n)} \bmod n = 1$$

với mọi cặp số nguyên dương nguyên tố cùng nhau a và n: gcd(a,n)=1.

  - *Ví dụ:*
    - a = 3; n = 10; Φ(10)=4; Vì vậy $3^4 = 81 = 1 \bmod 10$
    - *a* = 2; *n* =11; Φ(11)=10; Do đó $2^{10} = 1024 = 1 \bmod 11$

2. Một số kiến thức toán học

- **Kiểm tra tính nguyên tố**
  - Giả sử cần phải tìm một số nguyên tố rất lớn. Lấy ngẫu nhiên một số đủ lớn, ta cần phải kiểm tra xem số đó có phải là số nguyên tố không?
    - Cách 1: Thử bằng phép chia
    - Cách 2: sử dụng các phép kiểm tra tính nguyên tố thống kê dựa trên các tính chất:
      - Mà mọi số nguyên tố phải thỏa mãn
      - Nhưng có một số số không nguyên tố, gọi là giả nguyên tố cũng thoả mãn tính chất đó

2. Một số kiến thức toán học

- Cụ thể là phép kiểm tra dựa trên Định lý Ferma như sau:
  - Nếu số n cần kiểm tra tính nguyên tố là số nguyên tố, thì nó sẽ thoã mãn định lý Ferma đối với mọi số a nhỏ hơn nó $a^{n-1} \bmod n = 1$.
  - Như vậy, lấy ngẫu nhiên số a và kiểm tra xem nó có tính chất trên không. Nếu có thì n có thể là số nguyên tố, nếu cần độ tin cậy lớn hơn, thì ta kiểm tra liên tiếp nhiều lần như vậy với các số ngẫu nhiên a được chọn. Sau mỗi lần qua được phép thử, xác suất để n là số nguyên tố lại tăng lên

2. Một số kiến thức toán học

- Chú ý rằng:
  - nếu $b^i \bmod n = 1$, thì:

    $b^{2i} \bmod n = (1)^2 \bmod n = 1$ và
  - nếu $b^i \bmod n = n - 1$, thì:

    $b^{2i} \bmod n = (n - 1)^2 \bmod n = (n^2 - 2n + 1) \bmod n = 1$

2. Một số kiến thức toán học

- Kiểm tra số n có là số nguyên tố không, ta chỉ cần xét n là lẻ, khi đó n-1 là chẵn và biểu diễn nó dạng $(n-1) = 2^k.q$
- Khi đó để tính a^{n-1}, ta tính a^q, sau đó bình phương liên tiếp k lần.

2. Một số kiến thức toán học

- Thuật toán Miller - Rabin:
  - TEST (n) is:

    1. Find integers k, q, $k > 0$, q odd, so that $(n–1)= 2^k.q$
    2. Select a random integer a, $1<a<n–1$
    3. **if** a^q mod $n = 1$ **then** return (“maybe prime");
    4. **for** $j = 0$ **to** $k – 1$ **do**
    5. **if** ($a^{2^{\wedge}j.q}$ mod $n = n$-1)

    then return(" maybe prime ")

    return ("composite")

2. Một số kiến thức toán học

- **Các xem xét về mặt xác suất**
  - Nếu thuật toán Miller Rabin trả về số "composite" thì số đó chắc chắn không là số nguyên tố, vì khi đó số n và số a < n không thoả mãn định lý Fecma, tức là $a^{n-1} \bmod n \neq 1$.
  - Ngược lại số đó có thể là số nguyên tố hoặc giả nguyên tố theo nghĩa nó thoả mãn định lý Fecma với số a < n. Người ta chứng minh được rằng xác suất để số giả nguyên tố đó không là số nguyên tố là là ¼. Suy ra nếu lặp t phép thử với các lựa chọn ngẫu nhiên khác nhau của số a, thì khi đó xác suất để số n sau t phép thử là số nguyên tố là: $1-(1/4)^t$
  - **Ví dụ.** Sau 10 bước, t = 10, mà số đã cho n đều có thể là nguyên tố, thì xác suất để n là số nguyên tố là $1 - (1/4)^{10} > 0.99999$.

2. Một số kiến thức toán học

- **Phân bố nguyên tố.**
  - Định lý về số nguyên tố khẳng định số nguyên tố xuất hiện trung bình sau mỗi khoảng lnn số nguyên (nếu xét các số trong kích thước n).
  - Lưu ý đây chỉ là *trung bình*, vì có lúc các số nguyên rất gần nhau và có lúc lại rất xa nhau.

2. Một số kiến thức toán học

- Trong nhiều trường hợp ta muốn tìm cách để tăng tốc độ tính toán Modulo. Các phép toán trên modulo các số nhỏ tính nhanh nhiều so với các số lớn.
- Chính vì vậy nếu số lớn phân tích được thành tích của các số nhỏ, từng cặp nguyên tố cùng nhau, thì ta sẽ có cách tính hiệu quả nhờ vào định lý Phần dư Trung hoa

2. Một số kiến thức toán học

- Định lí phần dư Trung Hoa

  $n_1, \ldots, n_k$ nguyên tố cùng nhau từng đôi một thì hệ sau có nghiệm duy nhất theo modulo $n = n_1 \ldots n_k$

$$
\begin{aligned}
x &\equiv a_1 \pmod{n_1} \\
x &\equiv a_2 \pmod{n_2} \\
&\ldots\ldots\ldots \\
x &\equiv a_k \pmod{n_k}
\end{aligned}
$$

2. Một số kiến thức toán học

- Có thể triển khai Định lý Trung Hoa theo một số cách như sau:
  - **1. Tính toán theo modulo số lớn:**
    - Để tính A mod M, với M (M= $m_1 m_2 .. m_k$) khá lớn và A là biểu thức số học nào đó. Trước hết ta cần tính tất cả $a_i = A \bmod m_i$. Sau đó sử dụng công thức:

$$A = \left(\sum_{i=1}^{k} a_i c_i \right) \bmod M$$

      Trong đó: $M_i = M/m_i$

$$c_i = M_i \times \left(M_i^{-1} \bmod m_i \right); \quad 1 \le i \le k$$

    - Áp dụng tính ví dụ: **$17^8 \bmod 77$?**

2. Một số kiến thức toán học

- Áp dụng định lý phần dư Trung hoa, ta coi $A = 17^{18}$, $m_1 = 7$, $m_2 = 11$. Khi đó $M_1 = 11$, $M_2 = 7$ và
  - $11^{-1} \bmod 7 = 4^{-1} \bmod 7 = 2$, suy ra $\mathbf{c_1 = 11*2 = 22}$;
  - $7^{-1} \bmod 11 = 8$, suy ra $\mathbf{c_2 = 7*8 = 56}$;
  - $17^8 \bmod 7 = (17 \bmod 7)^8 \bmod 7 = 3^8 \bmod 7 = (3^2)^4 \bmod 7 = \mathbf{a_1 = 2}$;
  - $17^8 \bmod 11 = (17 \bmod 11)^8 \bmod 11 = 6^8 \bmod 11$
    $= (6^2)^4 \bmod 11 = 3^4 \bmod 11 = \mathbf{a_2 = 4}$;
- Vậy $178 \bmod 77 = (2*22 + 4*56) \bmod 77$
  $= 268 \bmod 77 = 37 \bmod 77 = \mathbf{A = 37}$;

2. Một số kiến thức toán học

– 2. Giải hệ phương trình modulo:

- Cho $x = a_i \bmod m_i$, với $GCD(m_i, m_j) = 1$, với mọi i khác j. Khi đó ta cũng áp dụng Định lý phần dư Trung Hoa để tìm x.
- Áp dụng tính ví dụ:
  - Tìm x với:

$$\begin{cases} x \equiv 5 \bmod 7 \\ x \equiv 6 \bmod 11 \end{cases}$$

2. Một số kiến thức toán học

- Áp dụng định lý phần dư Trung hoa, ta tính:
  - $7^{-1} \bmod 11 = 8$ và $11^{-1} \bmod 7 = 2$. Như vậy:
  - $x = (5*2*11 + 6*8*7) \bmod (7*11) = 61 \bmod 77$.

2. Một số kiến thức toán học

- Định lí: nếu $(n_1, n_2) = 1$ thì

$$x \equiv a \pmod{n_1}, \; x \equiv a \pmod{n_2}$$

có nghiệm duy nhất

$$x \equiv a \bmod(n_1 . n_2)$$

2. Một số kiến thức toán học

- **Căn nguyên tố**
  - Từ Định lý Ole ta có $a^{\Phi(n)} \bmod n = 1$, với a và n là nguyên tố cùng nhau. Nếu không có số mũ dương nào nhỏ hơn Φ(n), mà có tính chất như vậy đối với a, thì khi đó ta gọi a là căn nguyên tố của n.
  - **Ví dụ:**
    - **(a)** Xét xem a = 2 có phải là căn nguyên tố của 5 không?
    - **(b)** a = 3 có là căn nguyên tố của 8 không?

2. Một số kiến thức toán học

- (a) Ta có:
  - $2 \bmod 5 = 2$; $2^2 \bmod 5 = 4$; $2^3 \bmod 5 = 3$; $2^4 \bmod 5 = 1$.
  - Rõ ràng $m = 4 = \Phi(5)$ là số mũ dương nhỏ nhất có tính chất $2^m \bmod 5 = 1$, nên 2 là căn nguyên tố của 5.
- (b) Ta có:
  - $3 \bmod 8 = 3$; $3^2 \bmod 8 = 1$; $3^3 \bmod 8 = 3$; $3^4 \bmod 8 = 1$
  - Rõ ràng $m = 2 < 4 = \Phi(8)$ là số mũ dương nhỏ nhất có tính chất $3^m \bmod 8 = 1$, nên 3 không là căn nguyên tố của 8.

2. Một số kiến thức toán học

- **Logarit rời rạc**
  - Bài toán ngược của bài toán lũy thừa là tìm logarit rời rạc của một sô modulo p, tức là tìm số nguyên x sao cho: $a^x = b \bmod p$. Hay còn được viết là $x=\log_a b \bmod p$
  - Nếu a là căn nguyên tố của p và p là số nguyên tố, thì luôn luôn tồn tại logarit rời rạc, ngược lại thì có thể không
  - **Ví dụ:**
    - Tìm $x = \log_2 3 \bmod 13$?
    - Tìm $x = \log_3 4 \bmod 13$?

2. Một số kiến thức toán học

- **Tìm $x = \log_2 3 \bmod 13$? (Hay: $2^x = 3 \bmod 13$)**
  - $2^0 \bmod 13 = 1$;
  - $2^1 \bmod 13 = 2$,
  - $2^2 \bmod 13 = 4$,
  - $2^3 \bmod 13 = 8$,
  - $2^4 \bmod 13 = 3$.
  - **Vậy $\log_2 3 \bmod 13 = 4$.**
- **Tìm $x = \log_3 4 \bmod 13$? (Hay $3^x = 4 \bmod 13$)**
  - Trong trường hợp này không có lời giải, vì
  - $3^0 \bmod 13 = 1$;
  - $3^1 \bmod 13 = 3$;
  - $3^2 \bmod 13 = 9$;
  - $3^3 \bmod 13 = 1 = 3^0 \bmod 13$

2. Một số kiến thức toán học

- Ta nhận thấy, trong khi bài toán lũy thừa là dễ dàng, thì bài toán logarit rời rạc là rất khó. Đây cũng là một cơ sở của mã công khai

2. Một số kiến thức toán học

Định nghĩa nhóm nhân của Z_n:

$$Z_n^* = \{a \in Z_n \mid (a,n) = 1\}$$

Với n nguyên tố thì $Z^*_n = ?$

2. Một số kiến thức toán học

Định lí: n nguyên tố:

- **Định lí Euler:** Nếu $a \in Z_n^*$ thì $a^{\Phi(n)} \equiv 1 \pmod{n}$
- Nếu n là tích của các số nguyên khác nhau, và nếu $r \equiv s \pmod{\Phi(n)}$ thì $a^r \equiv a^s \pmod{n}$

với mọi số nguyên a

2. Một số kiến thức toán học

ĐN thặng dư bậc 2, thặng dư không bậc 2:

$a \in Z_n^*$ là thặng dư bậc 2 modulo n nếu tồn tại $x \in Z_n^*$ sao cho $x^2 \equiv a \pmod{n}$

Nếu không tồn tại x như thế thì a được gọi là thặng dư không bậc 2 modulo n.

- Q_n là tập các thặng dư bậc 2 modulo n
- $\overline{Q_n}$ là tập các thặng dư không bậc 2 modulo n

2. Một số kiến thức toán học

Định lí số các căn bậc 2: Cho $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ trong đó p_i là các số nguyên tố lẻ phân biệt và $e_i \geq 1$. Nếu $a \in Q_n$ thì a có đúng 2^k căn bậc 2 khác nhau theo modulo n.

2. Một số kiến thức toán học

- **Lũy thừa**
  - Trong các bài toán mã hoá công khai, chúng ta sử dụng nhiều phép toán lũy thừa với số mũ lớn. Như vậy cần có thuật toán nhanh hiệu quả đối với phép toán này.
    - Trước hết ta phân tích số mũ theo cơ số 2, xét biểu diễn nhị phân của số mũ
    - Sau đó sử dụng thuật toán bình phương và nhân. Khái niệm được dựa trên phép lặp cơ sở bình phương và nhân để nhận được kết quả mong muốn.

2. Một số kiến thức toán học

- Thuật toán nhân bình phương có lặp để lấy lũy thừa trong Z_n:

VÀO : $a \in Z_n$ và số nguyên k, $(0 \le k < n)$ có biểu diễn nhị phân:

$$k = \sum_{i=0}^{t} k_i 2^i$$

RA : $a^k \bmod n$

(1) Đặt $b \leftarrow 1$. Nếu $k = 0$ thì **return** (b)

(2) Đặt $A \leftarrow a$.

(3) Nếu $k_0 = 1$ thì đặt $b \leftarrow a$.

(4) **For** i **from** 1 **to** t **do**

4.1. Đặt $A \leftarrow A^2 \bmod n$.

4.2. Nếu $k_i = 1$ thì đặt $b \leftarrow A.b \bmod n$

(5) Return (b)

2. Một số kiến thức toán học

- Ví dụ: Tính $5^{596} \bmod 1234 = ?$

k_i

i	0	1	2	3	4	5	6	7	8	9
k_i	0	0	1	0	1	0	1	0	0	1
A	5	25	625	681	1011	369	421	779	947	925
b	1	1	625	625	67	67	1059	1059	1059	1013

$\Rightarrow$ Vậy $5^{596} \bmod 1234 = 1013$

- Tính $9^{68} \bmod 78 = ?$

2. Một số kiến thức toán học

- **ĐN kí hiệu Legendre:** p là một số nguyên tố lẻ, a là một số nguyên. Kí hiệu Legendre được xác định như sau:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \in Q_p \\ -1 & a \in \overline{Q}_p \end{cases}$$

2. Một số kiến thức toán học

Các tính chất của ký hiệu Legendre.

Cho p là một số nguyên tố lẻ và $a, b \in Z$. Khi đó ký hiệu Legendre có các tính chất sau:

(1) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Đặc biệt $\left(\frac{1}{p}\right) = 1$ và $\left(-\frac{1}{p}\right) = (-1)^{(p-1)/2}$ Bởi vậy $-1 \in Q_p$ nếu $p \equiv 1 \pmod 4$ và $-1 \in \overline{Q}_p$ nếu $p \equiv 3 \pmod 4$

(2) $\left(\frac{a.b}{p}\right) \equiv \left(\frac{a}{p}\right).\left(\frac{b}{p}\right)$. Bởi vậy nếu $a \in Z_p^*$ thì $\left(\frac{a^2}{p}\right) = 1$.

(3) Nếu $a \equiv b \pmod{p}$ thì $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2. Một số kiến thức toán học

(4) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. Bởi vậy $\left(\frac{2}{p}\right) = 1$ nếu $p \equiv 1$ hoặc $7 \pmod 8$ và $\left(\frac{2}{p}\right) = -1$ nếu $p \equiv 3$ hoặc $5 \pmod 8$.

(5) Luật thuận nghịch bậc 2:

Giả sử p là một số nguyên tố lẻ khác với q, khi đó:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$$

2. Một số kiến thức toán học

ĐN kí hiệu Jacobi

Cho $n \geq 3$ là một số nguyên lẻ có phân tích

$$n = p_1^{e_1} . p_2^{e_2} \dots p_k^{e_k}$$

Khi đó kí hiệu Jacobi được định nghĩa là:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_k}\right)^{e_k}$$

2. Một số kiến thức toán học

Các tính chất của ký hiệu Jacobi.

Cho $n \geq 3$ là các số nguyên lẻ $a, b \in Z$. Khi đó ký hiệu Jacobi có các tính chất sau:

(1) $\left(\frac{a}{n}\right) = 0,1$ hoặc -1. Hơn nữa $\left(\frac{a}{n}\right) = 0$ nếu và chỉ nếu $\text{UCLN}(a,n) \neq 1$.

(2) $\left(\frac{a.b}{n}\right) \equiv \left(\frac{a}{n}\right).\left(\frac{b}{n}\right)$. Bởi vậy $a \in Z_n^*$ thì $\left(\frac{a^2}{n}\right) = 1$

2. Một số kiến thức toán học

(3) $\left(\frac{a}{m.n}\right) \equiv \left(\frac{a}{m}\right).\left(\frac{a}{n}\right)$.

(4) Nếu $a \equiv b \pmod n$ thì $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(5) $\left(\frac{1}{n}\right) = 1$

(6) $\left(-\frac{1}{n}\right) = (-1)^{(n-1)/2}$. Bởi vậy $\left(-\frac{1}{n}\right) = 1$ nếu $n \equiv 1 \pmod 4$

$\left(-\frac{1}{n}\right) = -1$ nếu $n \equiv 3 \pmod 4$

2. Một số kiến thức toán học

(7) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$. Bởi vậy $\left(\frac{2}{n}\right) = 1$ nếu $n \equiv 1$ hoặc $7 \pmod 8$

$\left(\frac{2}{n}\right) = -1$ nếu $n \equiv 3$ hoặc $5 \pmod 8$

(8) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{(m-1)(n-1)/4}$

2. Một số kiến thức toán học

Từ các tính chất của ký hiệu Jacobi ta thấy rằng **n** lẻ và $a = 2^e a_1$ trong đó a_1 là một số lẻ thì:

$$\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right) = \left(\frac{2}{n}\right)^e \left(\frac{n \bmod a_1}{a_1}\right)(-1)^{(a_1-1)(n-1)/4}$$

Từ công thức này ta có thể xây dựng thuật toán đệ quy sau để tính $\left(\frac{a}{n}\right)$ mà không cần phải phân tích **n** ra các thừa số nguyên tố .

2. Một số kiến thức toán học

- **Thuật toán** (*Tính toán ký hiệu Jacobi (và ký hiệu Legendre)*

VÀO : Số nguyên lẻ $n \geq 3$ số nguyên a, $(0 \leq a \leq n)$

RA : Ký hiệu Jacobi $\left(\frac{a}{n}\right)$ (Sẽ là ký hiệu Legendre khi n là số nguyên tố)

(1) Nếu $a = 0$ thì **return** (0)

(2) Nếu $a = 1$ thì **return** (1)

(3) Viết $a = 2^e a_1$, trong đó a_1 là một số lẻ

(4) Nếu e chẵn thì đặt $s \leftarrow 1$. Ngược lại hãy đặt $s \leftarrow 1$ nếu $n = 1$ hoặc $7 (\text{mod } 8)$

(5) Nếu $n \equiv 3 (\text{mod } 4)$ và $a_1 \equiv 3 (\text{mod } 4)$ thì đặt $s \leftarrow -s$

(6) Đặt $r_1 \leftarrow n \bmod a_1$

(7) Return $(s.\text{JACOBI}(n_1, a_1))$

2. Một số kiến thức toán học

Ví dụ tính toán ký hiệu Jacobi.

Cho $a = 158$ và $n = 235$. Thuật toán trên tính $\left(\frac{158}{235}\right)$ như sau:

$$\left(\frac{158}{235}\right) = \left(\frac{2}{235}\right)\left(\frac{79}{235}\right) = (-1)\left(\frac{235}{79}\right)(-1)^{78 \cdot 234/4} = \left(\frac{77}{79}\right)$$

$$= \left(\frac{77}{79}\right)(-1)^{76 \cdot 78/4} = \left(\frac{2}{77}\right) = -1$$

2. Một số kiến thức toán học

Ví dụ (Các thặng dư bậc 2 và không bậc 2).

$a \in Z_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
$a^2 \bmod n$	1	4	16	4	1	16	16	1	4	16	4	1
$\left(\frac{a}{3}\right)$	1	−1	1	−1	−1	1	−1	1	1	−1	1	−1
$\left(\frac{a}{7}\right)$	1	1	1	−1	1	−1	1	−1	1	−1	−1	−1
$\left(\frac{a}{21}\right)$	1	−1	1	1	−1	−1	−1	−1	1	1	−1	1

Các ký hiệu Jacobi của các phần tử trong Z_{21}^*

- Từ ví dụ ta thấy $Q_{21}=\{1,4,16\}$; thấy rằng $\left(\frac{5}{21}\right)=1$ nhưng $5 \notin Q_{21}$

2. Một số kiến thức toán học

Định nghĩa

Cho $n \geq 3$ là các số nguyên tố lẻ và cho $J_n = \left\{ a \in Z_n^* \middle| \left(\frac{a}{n}\right) = 1 \right\}$ tập các thặng dư giả bậc 2 theo modulo n (Ký hiệu $\hat{Q}_n$) được định nghĩa là tập $J_n - Q_n$.

2. Một số kiến thức toán học

Số Blum n là số có dạng $n = p.q$ trong đó p, q là các số nguyên tố khác nhau thoả mãn:

$$p \equiv 3 \bmod 4$$

$$q \equiv 3 \bmod 4$$

Định lí: n là một số Blum, $a \in Q_n$ khi đó a có đúng 4 căn bậc 2 modulo n và chỉ có duy nhất một căn bậc 2 thuộc Q_n (căn bậc 2 chính a mod n)

3. Một số hệ mật khoá công khai

- 3.1 Hệ mật RSA
- 3.2 Hệ mật Merkle – Hellman
- 3.3 Hệ mật McEliece
- 3.4 Hệ mật ElGamal
- 3.5 Hệ mật Chor- Rivest
- 3.6 Hệ mật trên đường cong Elliptic

3.1 Hệ mật RSA

- RSA là mã công khai được sáng tạo bởi Rivest, Shamir & Adleman ở MIT (Trường Đại học Công nghệ Massachusetts) vào năm 1977.
- RSA là mã công khai được biết đến nhiều nhất và sử dụng rộng rãi nhất hiện nay.
- RSA dựa trên các phép toán lũy thừa trong trường hữu hạn các số nguyên theo modulo nguyên tố. Cụ thể, mã hoá hay giải mã là các phép toán luỹ thừa theo modulo số rất lớn.
- Việc thám mã, tức là tìm khoá riêng khi biết khoá công khai, dựa trên bài toán khó là phân tích một số rất lớn đó ra thừa số nguyên tố. Nếu không có thông tin gì, thì ta phải lần lượt kiểm tra tính chia hết của số đó cho tất cả các số nguyên tố nhỏ hơn căn của nó. Đây là việc làm không khả thi!

3.1 Hệ mật RSA

- Người ta chứng minh được rằng, phép lũy thừa cần $O((\log n)^3)$ phép toán, nên có thể coi lũy thừa là bài toán dễ.
- Cần chú ý rằng ở đây ta sử dụng các số rất lớn khoảng 1024 bit, tức là cỡ 10^{350}.
- Tính an toàn dựa vào độ khó của bài toán phân tích ra thừa số các số lớn. Bài toán phân tích ra thừa số yêu cầu $O(e^{\log n \log\log n})$ phép toán, đây là bài toán khó.

3.1 Hệ mật RSA

- **Khởi tạo khoá RSA**
  - Mỗi người sử dụng tạo một cặp khoá công khai – riêng như sau:
    - Chọn ngẫu nhiên 2 số nguyên tố lớn p và q
    - Tính số làm modulo của hệ thống: N = p.q
  - Ta đã biết $\Phi(N)=(p-1)(q-1)$
  - Và có thể dùng Định lý Trung Hoa để giảm bớt tính toán
  - Chọn ngẫu nhiên khoá mã e
  - Trong đó $1<e<\Phi(N)$, $\gcd(e,\Phi(N))=1$
  - Giải phương trình sau để tìm khoá giải mã d sao cho
  - $e.d=1 \bmod \Phi(N)$ với $0\leq d\leq \Phi(N)$
  - In khoá mã công khai $KU=\{e,N\}$
  - Giữ khoá riêng bí mật $KR=\{d,p,q\}$

3.1 Hệ mật RSA

- **Sử dụng RSA**
  - Để mã hoá mẩu tin, người gủi:
    - Lấy khoá công khai của người nhận KU={e,N}
    - Tính $C=M^e \bmod N$, trong đó $0 \leq M < N$
  - Để giải mã hoá bản mã, người sở hữu nhận:
    - Sử dụng khóa riêng KR={d,p,q}
    - Tính $M=C^d \bmod N$
  - Lưu ý rằng bản tin $M < N$, do đó khi cần chia khối bản rõ.

3.1 Hệ mật RSA

- **Cơ sở của RSA**
  - Theo Định lý Ole
    - $a^{\Phi(n)} \bmod N = 1$ trong đó gcd(a,N)=1
    - Ta có N=p.q
    - $\Phi(N)=(p-1)(q-1)$
    - $e.d=1 \bmod \Phi(N)$
    - $e.d=1+k.\Phi(N)$ đối với một giá trị k nào đó.
  - Suy ra
    - $C^d = (M^e)^d = M^{1+k.\Phi(N)} = M^1.(M^{\Phi(n)})^k$ suy ra
    - $C^d \bmod N = M^1.(1)^k \bmod N = M^1 \bmod N = M \bmod N$

3.1 Hệ mật RSA

- **Ví dụ**
  - Chọn các số nguyên tố: $p=17$ & $q=11$.
  - Tính $n = pq$, $n = 17\times11=187$
  - Tính $\Phi(n)=(p-1)(q-1)=16\times10=160$
  - Chọn e : gcd(e,160)=1; Lấy $e=7$
  - Xác định d: $de=1 \bmod 160$ và $d < 160$
  - Giá trị cần tìm là d=23, vì $23\times7=161= 10\times160+1$
  - In khoá công khai KU={7,187}
  - Giữ khoá riêng bí mật KR={23,17,11}

3.1 Hệ mật RSA

- Ví dụ áp dụng mã RSA trên như sau:
  - Cho mẩu tin M = 88 (vậy 88<187)
  - Mã C = 88^7 mod 187 = 11
  - Giải mã M = 11^{23} mod 187 = 88
  - Có thể dùng định lý phần dư Trung Hoa để giải mã cho nhanh như sau:
    - Tính 11^{23} mod 11 = 0
    - Tính 11^{23}mod 17 = $(-6)^{23}$ mod 17 = $(-6)^{16}(-6)^4$ $(-6)^2$ (-6) mod 17 = c_1= 3
      Vì $(-6)^2$ mod 17 = 2, nên $(-6)^4$ mod 17 = 4, $(-6)^8$ mod 17 = -1,
      $(-6)^{16}$ mod 17 = 1
    - 11^{-1} mod 17 = $(-6)^{-1}$ mod 17 = 14 nên 11(11^{-1} mod 17) = 11(14 mod 17) = c_2 = 154
    - Vậy M = (3.154) mod 187 = 462 mod 187 = 88

3.1 Hệ mật RSA

- **Mã hiệu quả:**
  - Mã sử dụng lũy thừa của khoá công khai e, nếu giá trị của e nhỏ thì tính toán sẽ nhanh, nhưng dễ bị tấn công. Thường chọn e nhỏ hơn hoặc bằng 65537 (2^{16}-1), tức là độ dài khoá công khai là 16 bit. Chẳng hạn trong ví dụ trên ta có thể lựa chọn e = 23 hoặc e = 7.
  - Ta có thể tính mã hoá nhanh, nếu biết n=pq và sử dụng Định lý phần dư Trung Hoa với mẩu tin M theo các Modulo p và q khác nhau. Nếu khoá công khai e cố định thì cần tin tưởng rằng khi chọn n ta luôn có gcd(e,Φ(n)) = 1. Loại bỏ mọi p, q mà làm cho Φ(n) không nguyên tố cùng nhau với e.

3.1 Hệ mật RSA

- **Giải mã hiệu quả:**
  - Có thể sử dụng Định lý phần dư Trung Hoa để tính theo mod p và q, sau đó kết hợp lại để tìm ra bản rõ. Vì ở đây người sử dụng khoá riêng biết được p và q, do đó có thể sử dụng kỹ thuật này.
  - Nếu sử dụng định lý phần dư Trung Hoa để giải mã thì hiệu quả là nhanh gấp 4 lần so với giải mã tính trực tiếp.

3.1 Hệ mật RSA

- **Sinh khoá RSA**
  - Người sử dụng RSA cần phải xác định ngẫu nhiên 2 số nguyên tố rất lớn p, q thông thường khoảng 512 bit.
  - Sau khi chọn được một khoá e hoặc d nguyên tố cùng nhau với Φ(n), dễ dàng tính được khoá kia chính là số nghịch đảo của nó qua thuật toán Euclide mở rộng.

3.1 Hệ mật RSA

- **An toàn của RSA**
  - Trên thực té có nhiều cách tấn công khác nhau đối với mã công khai RSA như sau:
    - Tìm kiếm khoá bằng phương pháp vét cạn, phương pháp này không khả thi với kích thước đủ lớn của các số
    - Tấn công bằng toán học dựa vào độ khó việc tính Φ(n) bằng cách phân tích n thành hai số nguyên tố p và q hoặc tìm cách tính trực tiếp Φ(n).
    - Trong quá trình nghiên cứu việc thám mã người ta đề xuất kiểu tấn công thời gian trong khi giải mã, tức là căn cứ vào tốc độ mã hoá và giải mã các mẩu tin cho trước mà phán đoán các thông tin về khoá.

3.1 Hệ mật RSA

- **Điểm bất động**

  Định lí: Nếu các thông báo được mã bằng hệ mật RSA với cặp khóa công khai (e,n) với n = p.q thì số các thông báo không thể che dấu được là

$$N = (1 + UCLN(e-1, p-1))(1 + UCLN(d-1, q-1))$$

3.2 Hệ mật Merkle – Hellman

- Hệ mật Merkle – Hellman

- Dãy siêu tăng: Dãy số ngdương $(a_1, a_2, \ldots, a_n)$ tmãn

$$a_i > \sum_{j=1}^{i-1} a_j \quad \text{với} \quad \forall i, 2 \le i \le n$$

- Bài toán xếp ba lô:Cho tập các giá trị

và một tổng S. Hãy tính các giá trị b_i để: $M_1, M_2, \ldots, M_n$

$$S = b_1 M_1 + b_2 M_2 + \ldots + b_n M_n \quad \text{với } b_i \in \{0, 1\}$$

3.2 Hệ mật Merkle – Hellman

- TT giải btoán xếp ba lô trong trường hợp dãy siêu tăng:

VÀO: Dãy siêu tăng $M = \{M_1, M_2, \ldots, M_n\}$ và một số nguyên S là tổng của một tập con trong M

RA: $(b_1, b_2, \ldots, b_n)$ trong đó $b_i \in \{0,1\}$ sao cho: $\sum_{i=1}^{n} b_i M_i = S$

(1) $i \leftarrow n$

(2) Chừng nào $i \geq 1$ hãy thực hiện

a. Nếu $S \geq M_i$ thì : $b_i \leftarrow 1$ và $S \leftarrow S - M_i$ ngược lại: $b_i \leftarrow 0$

b. $i \leftarrow i - 1$

(3) Return (b)

3.2 Hệ mật Merkle – Hellman

Chọn một sô nguyên xác định n được xem là một tham sô chung của hệ thông

Mỗi đầu liên lạc phải thực hiện các bước sau:

1. Chọn một dãy siêu tăng $(M_1, M_2, \ldots, M_n)$ và một modulo M sao cho $M > M_1, M_2, \ldots, M_n$.
2. Chọn một số nguyên ngẫu nhiên W, $1 \le W \le M-1$ sao cho $(W, M) = 1$.
3. Chọn một phép hoán vị ngẫu nhiên π của các số nguyên $\{1, 2, \ldots, n\}$
4. Tính $a_i = WM_{\pi(i)} \bmod M$ với $i = 1, 2, \ldots, n$.
5. Khoá công khai là tập các số $(a_1, a_2, \ldots, a_n)$

   Khoá bí mật là $(\pi, M, W(M_1, M_2, \ldots, M_n))$

3.2 Hệ mật Merkle – Hellman

- Mã hoá

Mã hoá: B phải thực hiện các bước sau:

(1) Nhận khoá công khai của A: $(a_1, a_2, \ldots, a_n)$

(2) Biểu thị bản tin m như một chuỗi nhị phân có độ dài n

$m = m_1, m_2, \ldots, m_n$.

(3) Tính số nguyên $c = m_1 a_1 + m_2 a_2 + \cdots + m_n a_n$

(4) Gửi bản mã c cho A.

3. Một số hệ mật khoá công khai (15)

- Giải mã

Để khôi phục bản rõ m từ c, A phải thực hiện các bước sau:

(1) Tính $d = W^{-1} c \bmod M$

(2)Sử dụng thuật giải xếp ba lô trong trường hợp dãy siêu tăng để tìm các số nguyên $r_1, r_2, \ldots, r_n$, $r_i \in \{0,1\}$ sao cho:

$$d = r_1 M_1 + r_2 M_2 + \cdots + r_n M_n$$

(3)Các bit của bản rõ là $m_i = r_{\pi(i)}$, $i = 1,2,\ldots,n$

3.2 Hệ mật Merkle – Hellman

- Chứng minh

Thuật toán trên cho phép A thu được bản rõ vì:

$$d \equiv W^{-1}c \equiv W^{-1}\sum_{i=1}^{n} m_i a_i \equiv \sum_{i=1}^{n} m_i M_{\pi(i)} \bmod M$$

Vì $0 \le d < M$, $d = \sum_{i=1}^{n} m_i M_{\pi(i)} \bmod M$, bởi vậy nghiệm của bài toán xếp ba lô ở bước (2) sẽ cho ta các bit của bản rõ sau khi sử dụng phép hoán vị π

3. Một số hệ mật khoá công khai (1)

3.1 Hệ mật RSA (Ron Rivest, Adi Shamir và Len Adleman)

- Tạo khoá:

(1) Tạo 2 số nguyên tố lớn ngẫu nhiên và khác nhau p và q. p và q có độ lớn xấp xỉ nhau.

(2) Tính $n = p.q$ và $\Phi(n) = (p-1)(q-1)$.

(3) Chọn một số nguyên ngẫu nhiên e, $1 < e < \Phi$, sao cho $(e, \Phi) = 1$.

(4) Sử dụng thuật toán Euclide mở rộng để tính một số nguyên d duy nhất, $1 < d < \Phi$ thoả mãn $ed \equiv 1 (\mathrm{mod} \Phi)$.

(5) Khoá công khai là cặp số (n, e). Khoá riêng bí mật là d.

3. Một số hệ mật khoá công khai (2)

- Mã hoá: Bên mã là B, bên nhận là A

Mã hoá: B phải thực hiện:

(1) Thu nhận khoá công khai (n, e) của A.

(2) Biểu diễn bản tin dưới dạng một số nguyên m trong khoảng $[0, n-1]$

(3) Tính $c = m^e \bmod n$.

(4) Gửi bản mã c cho A.

Giải mã: Khôi phục bản rõ m từ c. A phải thực hiện phép tính sau bằng cách dùng khoá riêng $m = c^d \bmod n$

3. Một số hệ mật khoá công khai (3)

Chú ý: $\lambda = \text{BCNN}\ (p-1, q-1)$

1. Số mũ vạn năng

thay cho $\Phi = (p-1)(q-1)$

2. Điểm bất động

Định lí: Nếu các thông báo được mã bằng hệ mật RSA với cặp khóa công khai (e,n) với $n = p.q$

thì số các thông báo không thể che dấu được là

$$N = (1 + \text{UCLN}(e-1, p-1))(1 + \text{UCLN}(d-1, q-1))$$

3. Một số hệ mật khoá công khai (4)

3.2 Hệ mật Rabin

- Tạo khoá

  + Tạo 2 số nguyên tố lớn, ngẫu nhiên và phân biệt p và q có kích thước xấp xỉ nhau.

  + Tính $n = p.q$

  + Khoá công khai là n, khoá bí mật là các cặp số (p, q).

3. Một số hệ mật khoá công khai (5)

- Mã hoá:
  - + Nhận khoá công khai của A: n.
  - + Biểu thị bản tin dưới dạng một số nguyên m nằm trong dải $[0, n-1]$
  - + Tính $c = m^2 \bmod n$
  - + Gửi bản mã c cho A

3. Một số hệ mật khoá công khai (6)

- Giải mã:

  + A phải thực hiện các bước sau:Tìm 4 căn bậc hai của c mod n là m_1, m_2, m_3 hoặc m_4

  + Thông báo cho người gửi là một trong 4 giá trị m_1, m_2, m_3 hoặc m_4. Bằng một cách nào đó A sẽ quyết định m là giá trị nào.

3. Một số hệ mật khoá công khai (7)

Chú ý: Khi p, q là các số nguyên Blum thì ta có thể tính 4 căn bậc 2 của c mod n như sau:

+ Tìm a,b nguyên thoả mãn: $ap + bq = 1$

+Tính các giá trị sau:

$r = c^{(p+1)/4} \bmod p$ $\quad s = c^{(q+1)/4} \bmod q$

$y = (aps - bqr) \bmod n$ $\quad x = (aps + bqr) \bmod n$

4 giá trị căn bậc 2 của $c \bmod n$ là x, $-x \bmod n$, y và $-y \bmod n$

3. Một số hệ mật khoá công khai (8)

3.3 Hệ mật Elgamal

- Tạo khoá:

  + Tạo 1 số nguyên tố p lớn và một phần tử sinh α của nhóm nhân Z_p^* của các số nguyên mod p.

  + Chọn một số nguyên ngẫu nhiên a, $1 \le a \le p-2$ và tính $\alpha^a \bmod p$

Khoá công khai là bộ 3 số (p, α, α^a), khoá bí mật là a.

3. Một số hệ mật khoá công khai (9)

- Mã hoá:
  + Nhận khoá công khai (p, α, α^a) của A
  + Biểu thị bản tin dưới dạng một số nguyên m trong dải $\{0, 1, \ldots, p-1\}$
  + Chọn số nguyên ngẫu nhiên k, $1 \le k \le p-2$
  + Tính $\gamma = \alpha^k \bmod p$ và $\delta = m(\alpha^a)^k \bmod p$
  + Gửi bản mã $c = (\alpha, \delta)$ cho A

3. Một số hệ mật khoá công khai (10)

- Giải mã:
  + Sử dụng khoá riêng a để tính $\gamma^{p-1-a} \bmod p$
  + Khôi phục bản rõ bằng cách tính $\left(\gamma^{-a}\right)\delta \bmod p$
- Chứng minh:

$$\gamma^{-a}\,\delta \equiv \alpha^{-a\,k}.m\,\alpha^{a\,k} \equiv m \bmod p$$

3. Một số hệ mật khoá công khai (17)

3.5 Hệ mật trên đường cong Elipptic

Một đường cong Elliptic là một phương trình bậc 3 có dạng sau:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

Trong đó a, b, c, d, e là các số thực.

3. Một số hệ mật khoá công khai (18)

Các phép toán cộng và nhân trên các nhóm E.

Giả sử $P=(x_1,y_1)$, $Q=(x_2,y_2)$ là các điểm trong nhóm $E_p(a,b)$, O là điểm vô cực. Các quy tắc đối với phép cộng trên nhóm con $E_p(a,b)$ như sau:

(1) $P+O=O+P=P$.

(2) Nếu $x_2=x_1$ và $y_2=-y_1$ tức là $P=(x_1,y_1)$ và $Q=(x_2,y_2)=(x_1,-y_1)=-P$ thì $P+Q=0$.

(3) Nếu $Q\neq -P$ thì tổng $P+Q=(x_3,y_3)$ được

$$x^3=\lambda^2-x_1-x_2 \bmod p$$
$$y^3=\lambda(x_1-x_3)-y_1 \bmod p$$

Trong đó:

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} & P\neq Q\\ \dfrac{3x_1^2+a}{2y_1} & P=Q\end{cases}$$

3. Một số hệ mật khoá công khai (19)

Mật mã trên đường cong Elliptic.

Trong hệ mật này bản rõ M được mã hóa thành một điểm P_M trong tập hữu hạn các điểm của nhóm $E_p(a,b)$.

Trước hết ta phải chọn một điểm sinh $G \in E_p(a,b)$ sao cho giá trị nhỏ nhất của n đảm bảo $nG = 0$ phải là một số nguyên tố rất lớn. Nhóm $E_p(a,b)$ và điểm sinh G được đưa ra công khai.

Mỗi người dùng chọn một khóa riêng $n_A < n$ và tính khóa công khai P_A như sau: $P_A = n_A G$.

3. Một số hệ mật khoá công khai (20)

Để gửi thông báo P_M cho bên B, A chọn một số nguyên ngẫu nhiên k và tính cặp bản mã P_C bằng cách dùng khóa công khai P_B của B:

$$P_C = \left[(kG), (P_M + kP_B)\right]$$

Sau khi thu cặp điểm P_C, B sẽ nhân điểm đầu tiên (kG) với khóa riêng n_B của mình rồi cộng kết quả với điểm thứ hai trong cặp điểm P_C (Điểm $(P_M + kP_B)$);

$$(P_M + kP_B) - n_B(kG) = (P_M + kn_BG) - n_B(kG) = P_M$$

Đây chính là điểm tương ứng với bản rõ M. Chỉ có B mới có khóa riêng n_B và mới có thể tách $n_B(kG)$ khỏi điểm thứ hai của P_C để thu thông tin về bản rõ P_M.