CHƯƠNG 2:

CƠ SỞ LÝ THUYẾT SỐ HỌC

Chương 2:
Cơ sở lý thuyết số học

2.1. Lý thuyết thông tin

Những khái niệm mở đầu của lý thuyết thông tin được đưa ra lần đầu tiên vào năm 1948 bởi Claude Elwood Shannon (một nhà khoa học được coi là cha đẻ của lý thuyết thông tin).

Kỹ thuật lộn xộn và rườm rà (Confusion and Diffusion)

Theo Shannon, có hai kỹ thuật cơ bản để che dấu sự dư thừa thông tin trong thông báo gốc, đó là:

sự lộn xộn và sự rườm rà

Chương 2:
Cơ sở lý thuyết số học

Thông thường các hệ mã hiện đại thường kết hợp cả hai kỹ thuật thay thế và hoán vị để tạo ra các thuật toán mã hóa có độ an toàn cao hơn

Chương 2:
Cơ sở lý thuyết số học

2.1.1. Entropy

- **Lý thuyết thông tin** định nghĩa khối lượng thông tin trong một thông báo là số bit nhỏ nhất cần thiết để mã hóa tất cả những nghĩa của thông báo đó.

  Ví dụ: trường **ngay_thang** trong một cơ sở dữ liệu chứa không quá 3 bit thông tin, bởi vì thông tin ngày có thể mã hóa với 3 bit dữ liệu:

  000 = Sunday
  001 = Monday
  010 = Tuesday
  011 = Wednesday
  100 = Thursday
  101 = Friday
  110 = Saturday
  111 is unused

Chương 2:
Cơ sở lý thuyết số học

2.2. Lý thuyết độ phức tạp

- Lý thuyết độ phức tạp cung cấp một phương pháp để phân tích độ phức tạp tính toán của thuật toán và các kỹ thuật mã hóa khác nhau. Nó so sánh các thuật toán mã hóa, kỹ thuật và phát hiện ra độ an toàn của các thuật toán đó.
- Lý thuyết thông tin đã cho chúng ta biết rằng một thuật toán mã hóa có thể bị bại lộ.
- Còn lý thuyết độ phức tạp cho biết khả năng bị thám mã của một hệ mật mã
- Độ phức tạp thời gian của thuật toán là một hàm của kích thước dữ liệu input của thuật toán đó. Thuật toán có độ phức tạp thời gian f(n) đối với mọi n và kích thước input n, nghĩa là số bước thực hiện của thuật toán lớn hơn f(n) bước.

Chương 2:
Cơ sở lý thuyết số học

2.2.1. Độ an toàn tính toán

Định nghĩa:

Một hệ mật được gọi là an toàn về mặt tính toán nếu có một thuật toán tốt nhất để phá nó thì cần ít nhất N phép toán, với N là một số rất lớn nào đó.

Chương 2:
Cơ sở lý thuyết số học

2.2.2. Độ an toàn không điều kiện

Một hệ mật được coi là an toàn không điều kiện khi nó không thể bị phá ngay cả với khả năng tính toán không hạn chế.

Rõ ràng là độ an toàn không điều kiện không thể nghiên cứu theo quan điểm độ phức tạp tính toán vì thời gian tính toán là không hạn chế. Vì vậy, ở đây lý thuyết xác suất sẽ được đề cập để nghiên cứu về “an toàn không điều kiện”.

Chương 2:
Cơ sở lý thuyết số học

2.3. Số nguyên tố, Đồng dư và Thặng dư

a. Số nguyên tố

Định nghĩa 1 (Số nguyên tố) Một số nguyên tố $p \geq 2$ được gọi là số nguyên tố nếu nó chỉ chia hết cho 1 và p. Ngược lại là hợp số.

Các số nguyên tố từ 2 đến 100:

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

Số 2 là số nguyên tố nhỏ nhất và cũng là số nguyên tố chẵn duy nhất.

Chương 2:
Cơ sở lý thuyết số học

2.3. Số nguyên tố, Đồng dư và Thặng dư

Bảng số nguyên tố - sàng Eratosthene

Sàn Eratosthenes là một giải thuật cổ xưa để lập bảng tất cả các số nguyên tố nhỏ hơn một số n cho trước

Giải thuật dựa trên tính chất: mọi hợp số n đều có ước nguyên tố không vượt quá căn của chính nó (sqrt(n))

Giải thuật đầu tiên xóa số 1 ra khỏi tập các số nguyên tố. Số tiếp theo số 1 là số 2, là số nguyên tố. Bắt đầu từ số 2 xóa tất cả các bội của 2 ra khỏi bảng. Số đầu tiên không bị xóa sau số 2 (số 3) là số nguyên tố. Tiếp theo lại xóa các bội của 3 … Giải thuật tiếp tục cho đến khi gặp số nguyên tố lớn hơn hoặc bằng sqrt(n) thì dừng lại. Tất cả các số chưa bị xóa là số nguyên tố.

Chương 2:
Cơ sở lý thuyết số học

2.3. Số nguyên tố, Đồng dư và Thặng dư

b. Modulo số học – đồng dư

Định nghĩa 2 (Modulo số học – đồng dư): Nếu a và b là hai số nguyên, khi đó a được gọi là đồng dư với b theo modulo n, ký hiệu:

$$a \equiv b \pmod{n}$$

nếu (a-b) chia hết n, và n được gọi là modulus của đồng dư.

Ví dụ: (i) $24 \equiv 9 \pmod 5$ vì $24 - 9 = 3 \times 5$

(ii) $-11 \equiv 17 \pmod 7$ vì $-11 - 17 = -4 \times 7$

(iii) $42 \equiv 6 \pmod 9$ vì $42 - 6 = 4 \times 9$

(iv) $-42 \equiv 3 \pmod 9$

Chương 2:
Cơ sở lý thuyết số học

2.3. Số nguyên tố, Đồng dư và Thặng dư

Tìm giá trị dư của các số sau:

-13 mod 5

-18 mod 7

-49 mod 8

-123 mod 16

-213 mod 13

Chương 2:
Cơ sở lý thuyết số học

Tính chất của modulo số học

- Modulo số học cũng giống như số học bình thường, bao gồm các phép giao hoán, kết hợp, phân phối. Mặt khác giảm mỗi giá trị trung gian trong suốt quá trình tính toán.

(a+b) mod n = ((a mod n) + (b mod n)) mod n

(a-b) mod n = ((a mod n) - (b mod n)) mod n

(axb) mod n = ((a mod n) x (b mod n)) mod n

(ax(b+c)) mod n = (((axb) mod n) + ((axc) mod n)) mod n

- Các phép tính trong các hệ mã mật hầu hết đều thực hiện đối với một modulo N nào đó

Chương 2:
Cơ sở lý thuyết số học

3. Vành Z_N

- Tập các số nguyên Z_N= {0, 1, …, N-1} trong đó N là một số tự nhiên dương với 2 phép toán cộng (+) và nhân (.) được định nghĩa như sau:

Phép cộng:

$\forall a, b \in Z_N$: a+b = (a+b) mod N

Phép nhân:

$\forall a, b \in Z_N$: a.b = (a*b) mod N

- Theo tính chất của modulo số học chúng ta dễ dàng nhận thấy Z_N là một vành giao hoán và kết hợp. Hầu hết các phép tính toán trong các hệ mã mật đều được thực hiện trên một vành Z_N nào đó.

Chương 2:
Cơ sở lý thuyết số học

3. Vành Z_N

- Trên vành Z_N

  số 0 là phần tử trung hòa vì: a + 0 = 0 + a = a, $\forall a \in Z_N$

  số 1 được gọi là phần tử đơn vị vì a.1 = 1.a = a, $\forall a \in Z_N$

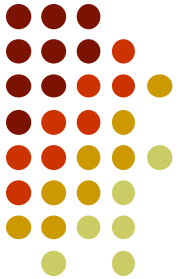
- Ví dụ N=9

  Z_9 = {0, 1, 2, 3, 4, 5, 6, 7, 8}

  6 + 8 = 14 ≡ 5 (mod 9)

  6 x 8 = 48 ≡ 3 (mod 9)

Chương 2:
Cơ sở lý thuyết số học



4. Phần tử nghịch đảo trên vành Z_N

Định nghĩa 5 (nghịch đảo) Cho a ∈ Z_N, số nghịch đảo theo modulo n là một số nguyên x ∈ Z_N, nếu a.x ≡ 1 (mod n). Nếu tồn tại x như vậy, thì nó là duy nhất và a được gọi là khả nghịch, nghịch đảo của a được ký hiệu là a^{-1}

Tính chất a ∈ Z_N, a là khả nghịch khi và chỉ khi

gcd(a, n) = 1

Ví dụ: Các phần tử khả nghịch trong Z_9 là 1, 2, 4, 5, 7 và 8 chẳng hạn:

4^{-1} = 7 vì 4.7 ≡ 1 mod 9

Ví dụ 2: Tìm các phần tử khả nghịch của Z_{26}

Chương 2:
Cơ sở lý thuyết số học

Tìm phần tử nghịch đảo của a

1. A = 3 trong Z_7
2. A = 8 trong Z_8
3. A = 6 trong Z_{13}
4. A = 23 trong Z_{40}
5. A = 19 trong Z_{88}
6. A = 17 trong Z_{88}

Chương 2:
Cơ sở lý thuyết số học

Một số thuật toán cơ sở hay sử dụng trong mã hóa

Thuật toán Thuật toán Euclide, tính ước số chung lớn nhất của hai số

INPUT: Hai số nguyên không âm a và b sao cho $a \geq b$.

OUTPUT: Ước số chung lớn nhất của a và b.

1. Trong khi $b \neq 0$, thực hiện

   1.1 Đặt $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$

2. Kết quả(a)

Chương 2:
Cơ sở lý thuyết số học

Ví dụ (Euclidean algorithm) Tính gcd(4864, 3458) = 38:

$$4864 = 1.3458 + 1406$$

$$3458 = 2.1406 + 646$$

$$1406 = 2.646 + 114$$

$$646 = 5.114 + 76$$

$$114 = 1.76 + 38$$

$$76 = 2.38 + 0$$

Chương 2:
Cơ sở lý thuyết số học

Thuật toán Euclidean có thể được mở rộng để không chỉ tính được ước số chung d của hai số nguyên a và b, mà còn có thể tính được hai số nguyên x, y thỏa mãn ax + by = d

Thuật toán Euclidean mở rộng (tìm USCLN hoặc tìm x, y thỏa mãn ax + by = d):

INPUT: Hai số nguyên không âm a và b với $a \geq b$

OUTPUT: d = gcd(a, b) và hai số x, y thỏa mãn ax+by=d

1. Nếu b = 0, đặt d←a, x←1, y←0, Kết quả (d, x, y)
2. Đặt $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$
3. Trong khi còn b>0, thực hiện:
   - 3.1 $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - q.b$, $x \leftarrow x_2 - q.x_1$, $y \leftarrow y_2 - q.y_1$
   - 3.2 a←b, b←r, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, $y_1 \leftarrow y$
4. Đặt d←a, $x \leftarrow x_2$, $y \leftarrow y_2$. Kết quả (d, x, y)

Chương 2:
Cơ sở lý thuy

1. Nếu b = 0, đặt d←a, x←1, y←0, Kết quả (d, x, y)
2. Đặt x_2←1, x_1←0, y_2←0, y_1←1
3. Trong khi còn b>0, thực hiện:
   3.1 q← ⌊a/b⌋ , r←a-q.b, x ←x_2-q. x_1, y ←y_2-q. y_1
   3.2 a←b, b←r, x_2← x_1, x_1 ← x, y_2←y_1, y_1←y
4. Đặt d←a, x←x_2, y←y_2. Kết quả (d, x, y)

<u>Ví dụ</u> Bảng dưới đây mô Euclidean mở rộng với đầu vào là a=4864, b = 3458 nhận được kết quả gcd(4864, 3458)=38 và (4864)(?) + (3458)(?) = 38

q	r	x	y	a	b	x_2	x_1	y_2	y_1
-	-	-	-	4864	3458	1	0	0	1
1	1406	1	-1	3458	1406	0	1	1	-1
2	646	-2	3	1406	646	1	-2	-1	3
2	114	5	-7	646	114	-2	5	3	-7
5	76	-27	38	114	76	5	-27	-7	38
1	38	32	-45	76	38	-27	32	38	-45
2	0	-91	128	38	0	32	-91	-45	128

Chương 2:
Cơ sở lý thuyết số học

Thuật toán Tính phần tử nghịch đảo trên Z_n

INPUT: a ∈ Z_N

OUTPUT: a^{-1} mod n, nếu tồn tại

1. Sử dụng *thuật toán Euclidean mở rộng,* tìm x và y để ***ax + ny = d***, trong đó d = gcd(a, n)
2. Nếu d>1, thì a^{-1} mod n không tồn tại. Ngược lại kết quả là **x**

Chương 2:
Cơ sở lý thuyết số học

2.4. Một số giải thuật về modulo

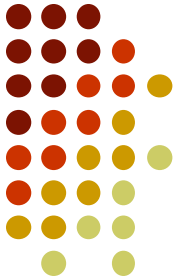
- Giải thuật lũy thừa nhanh
- Giải thuật Lehman
- Phần dư trung hoa

Chương 2:
Cơ sở lý thuyết số học

2.4.1 Giải thuật lũy thừa nhanh

Thuật toán do Chivers đưa ra vào năm 1984, thuật toán tìm a^x mod n có độ phức tạp tính toán không quá $log_2(x+1)$ bước

Chương 2:
Cơ sở lý thuyết số học



2.4.1 Giải thuật lũy thừa nhanh

Thuật toán do Chivers đưa ra vào năm 1984, thuật toán tìm a^x mod n có độ phức tạp tính toán không quá $log_2(m+1)$ bước.

- Input: a, x, N
- Output: a^x mod N

```
long modexp(long a, long x, long n)
{
        long r=1;
        while (x>0){
                if (x%2==1)  /*x is odd?*/
                        r=(r*a)%n;
                a=(a*a)%n
                x/=2;
        }
        return r;
}
```

Chương 2:
Cơ sở lý thuyết số học

Mô tả giải thuật lũy thừa nhanh

Input: a=31, x=101, n=1024

Lặp: (đầu tiên gán r=1)

- x lẻ: r=(r*a) mod n = 31, a=(a*a) mod n = 961, x=x/2=50
- x chẵn: a=(a*a) mod n = 987, x=x/2=25
- x lẻ: r=(r*a) mod n = 159, a=(a*a) mod n = 769, x=x/2=12
- x chẵn: a=(a*a) mod n = 513, x=x/2=6
- x chẵn: a=(a*a) mod n = 1, x=x/2=3
- x lẻ: r=(r*a) mod n = 159, a=(a*a) mod n = 1, x=x/2=1
- x lẻ: r=(r*a) mod n = 159, a=(a*a) mod n = 1, x=x/2=0
- x = 0, Stop

Output: a^x mod n = r = 159

Chương 2:
Cơ sở lý thuyết số học

Hãy tự vận dụng lũy thừa nhanh để

- Tìm 17^{98} mod 77, nghĩa là:
- A=17, x = 98, n = 77

Chương 2:
Cơ sở lý thuyết số học

2.4.2 Giải thuật Lehman

Thuật toán đoán số nguyên dương N là số nguyên tố dựa trên bài toán số nguyên tố của Lehman. Sự chính xác của phép đoán tỷ lệ số lượng phép thử.

Chương 2:
Cơ sở lý thuyết số học

2.4.2 Giải thuật Lehman

Chọn số lần thử và thực hiện chu trình:

- Với mỗi a khác nhau (1<a<N-1)
- Tính r = $a^{(N-1)/2}$ mod N
- Nếu r ≠ 1 và r ≠ N-1 thì N không là số nguyên tố và dừng chu trình

Kết thúc chu trình: Nếu mọi r đều bằng 1 hoặc N-1 thì N có thể là số nguyên tố.

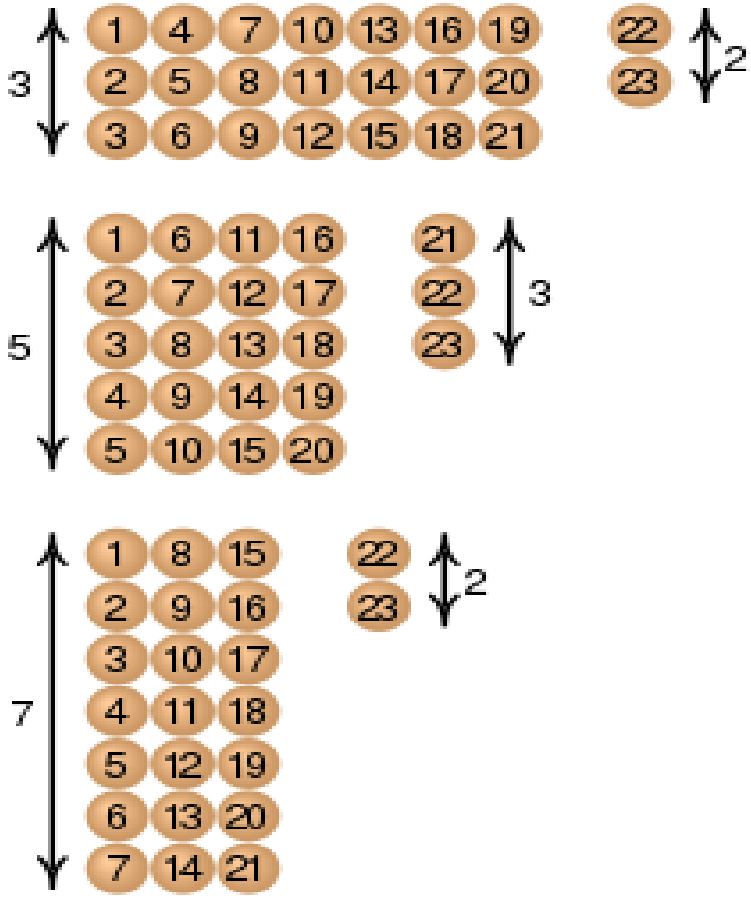
Chương 2:
Cơ sở lý thuyết số học

2.4.3. Phần dư Trung Hoa

- Định lý số dư Trung Quốc là tên người phương Tây đặt cho định lý này. Người Trung Quốc gọi nó là **bài toán Hàn Tín điểm binh.**
- Hàn Tín là một danh tướng thời Hán Sở, từng được phong tước vương thời Hán Cao Tổ Lưu Bang đang dựng nghiệp
- Sử ký Tư Mã Thiên viết rằng Hàn Tín là tướng trói gà không nổi, nhưng rất có tài quân sự. Tục truyền rằng khi Hàn Tín điểm quân số, ông cho quân lính xếp hàng 3, hàng 5, hàng 7 rồi báo cáo số dư. Từ đó ông tính chính xác quân số đến từng người.

Chương 2:
Cơ sở lý thuyết số học

2.4.3. Phần dư Trung Hoa



Chương 2:
Cơ sở lý thuyết số học

2.4.3. Phần dư Trung Hoa

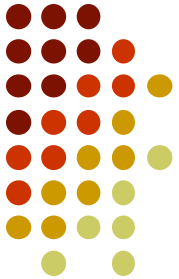
- Bản chất của bài toán Hàn Tín điểm binh là việc giải hệ phương trình đồng dư bậc nhất.

$$\begin{cases} x \equiv a_1 \ (mod\ m_1) \\ x \equiv a_2 \ (mod\ m_2) \\ \quad\quad \dots \\ x \equiv a_3 \ (mod\ m_3) \end{cases}$$

Trong đó $m_1, m_2, m_3 \dots m_k$ đôi một nguyên tố cùng nhau.

Trong bài toán Hàn Tín k=3, m_1=3, m_2=5, m_3=7

Chương 2:
Cơ sở lý thuyết số học



2.4.3. Phần dư Trung Hoa

Hệ phương trình đồng dư nói trên có nghiệm duy nhất theo modun

$$M = m_1.m_2.m_3 \ldots m_k$$

là

$$x \equiv a_1.M_1.y_1 + a_2.M_2.y_2 + \ldots + a_k.M_k.y_k \pmod{M}$$

trong đó

$$M_1 = M/m_1, M_2 = M/m_2, \ldots, M_k = M/m_k$$

$$y_1 = (M_1)^{-1} \pmod{m_1}, y_2 = (M_2)^{-1} \pmod{m_2}, \ldots, y_k = (M_k)^{-1} \pmod{m_k}$$

Biết rằng: $(M_1)^{-1} \pmod{m_1}$ *là nghịch đảo theo modulo của* m_1

với $y_1 = (M_1)^{-1} \pmod{m_1} \Leftrightarrow y_1 M_1 = 1 \pmod{m_1}$

Chương 2:
Cơ sở lý thuyết số học

Ví dụ:

$$\begin{cases} x \equiv 2 \ (mod\ 3) \\ x \equiv 3 \ (mod\ 5) \\ x \equiv 5 \ (mod\ 7) \end{cases}$$

ta có

$M = 3.5.7 = 105; M_1 = 5.7 = 35, M_2 = 3.7 = 21, M_3 = 3.5 = 15.$

$y_1 = 35^{-1} \pmod 3 = 2^{-1} \pmod 3 = 2;$

$y_2 = 21^{-1} \pmod 5 = 1^{-1} \pmod 5 = 1;$

$y_3 = 15^{-1} \pmod 7 = 1^{-1} \pmod 7 = 1.$

Từ đó

$x \equiv 2.35.2 + 3.21.1 + 5.15.1 \pmod{105}$

$x \equiv 140 + 63 + 75 \pmod{105} \equiv 278 \pmod{105}$

$x \equiv 68 \pmod{105}.$

Như vậy x có dạng $x = 68 + k.105$, k là số nguyên (hoặc số tự nhiên thích hợp nếu tìm nghiệm tự nhiên)

Chương 2:
Cơ sở lý thuyết số học

Thuật toán **lũy thừa nhanh**, **Lehman** và **phần dư Trung Hoa** thường được sử dụng cho:

+ Mã hóa Khóa công khai

+ Chữ ký số