Trần Văn Dũng, Bộ môn Khoa học máy tính.

BÀI TẬP MÔN AN TOÀN VÀ BẢO MẬT THÔNG TIN

BÀI 1: MÃ CỔ ĐIỂN VÀ MÃ DÒNG

1. MÃ CỔ ĐIỂN

1. Mã Vigenere đoạn văn sau: “Khoa cong nghe thong tin”

   với khóa “8,3,19,12”

2. Có bao nhiêu khóa Vigenere độ dài k.

3. Vì sao mã Vigenere có không gian khóa lớn mà lại không an toàn

4. Mã PlayFair thông điệp “Dai hoc Giao thong” bằng khóa “BADINH”

5. Mã khóa tự động thông điệp “Khoa hoc may tinh” bằng khóa “Cau giay”

6. Có bao nhiêu khóa PlayFair độ dài k. Một chữ cái trong mã Playfair có thể được mã hóa bởi bao nhiêu chữ khác nhau.

7. Cho bản rõ p = 10111001 10101110

   và khóa k = 11000110 01100110

   Tìm bản mã bộ đệm một lần và nêu cách giải mã.

8. Cho bản mã p dạng bit độ dài h. Lấy một dãy bit d bất kỳ độ dài h. Chứng tỏ rằng có một dãy bit k độ dài h, sao cho khi thực hiện phép cộng trên từng bit tương ứng ta có:

   $$p \text{ xor } k = d$$

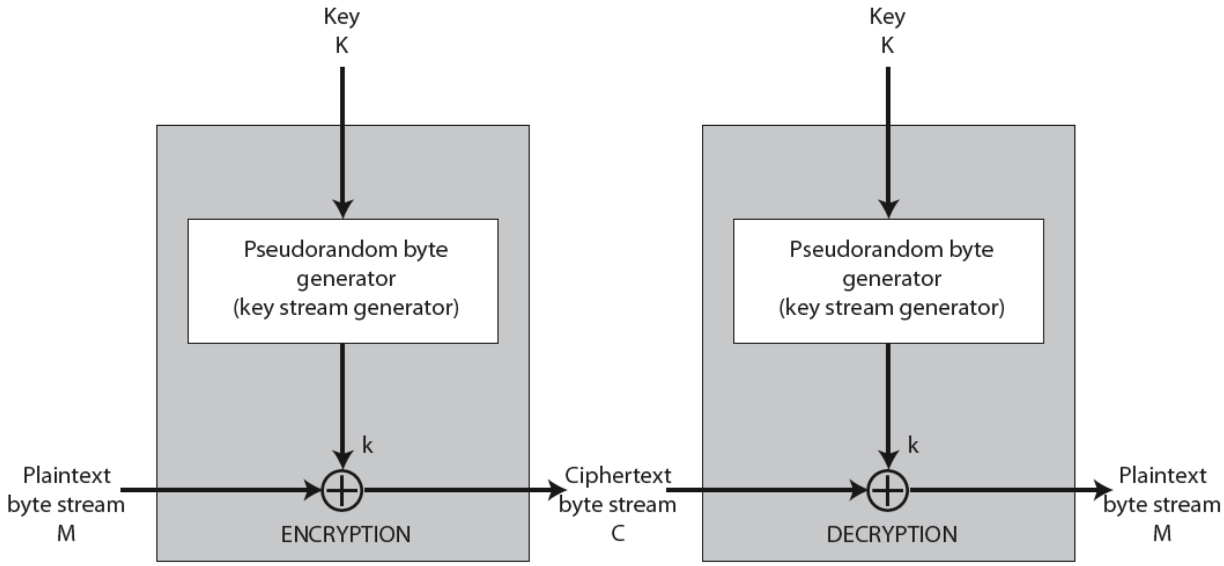
9. Tại sao mã bộ đệm một lần được cho là an toàn tuyệt đối.

10. Mã dịch chuyển dòng thông điệp sau “chung toi la sinh vien khoa cong nghe thong tin” với khóa “352641”. Nêu cách giải mã.

11. Có bao nhiêu khóa mã dịch chuyển có độ dài k

2. MÃ DÒNG

1. Giải thích sơ đồ hoạt động của mã dòng



Ví dụ: Mã hóa

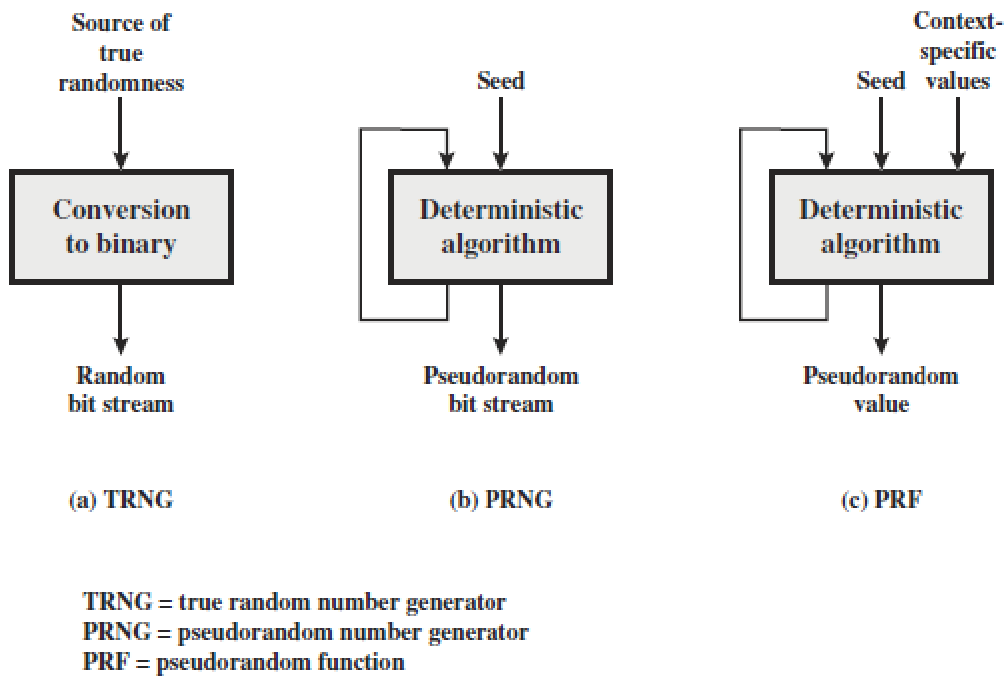
```
  11001100  plaintext
⊕ 01101100  key stream
  10100000  ciphertext
```

Giải mã:

```
  10100000  ciphertext
⊕ 01101100  key stream
  11001100  plaintext
```

2. Cho hàm random() sinh số ngẫu nhiên trong khoảng (0, 1). Tạo hàm sinh số ngẫu nhiên trong khoảng (0, N)
3. Tạo hàm sinh số ngẫu nhiên nguyên tố trong khoảng (0, N)

Một số dạng cấu trúc sinh đại lượng ngẫu nhiên:



BÀI 2: MÃ ĐỐI XỨNG HIỆN ĐẠI

1. MÃ DES

MÃ DES ĐƠN GIẢN

Mã DES đơn giản là mã khối mà mã khối 8 bit sử dụng khóa 10 bit và đầu ra là khối mã 8 bit.

Thuật toán mã hóa bao gồm 5 bước theo thứ tự sau:

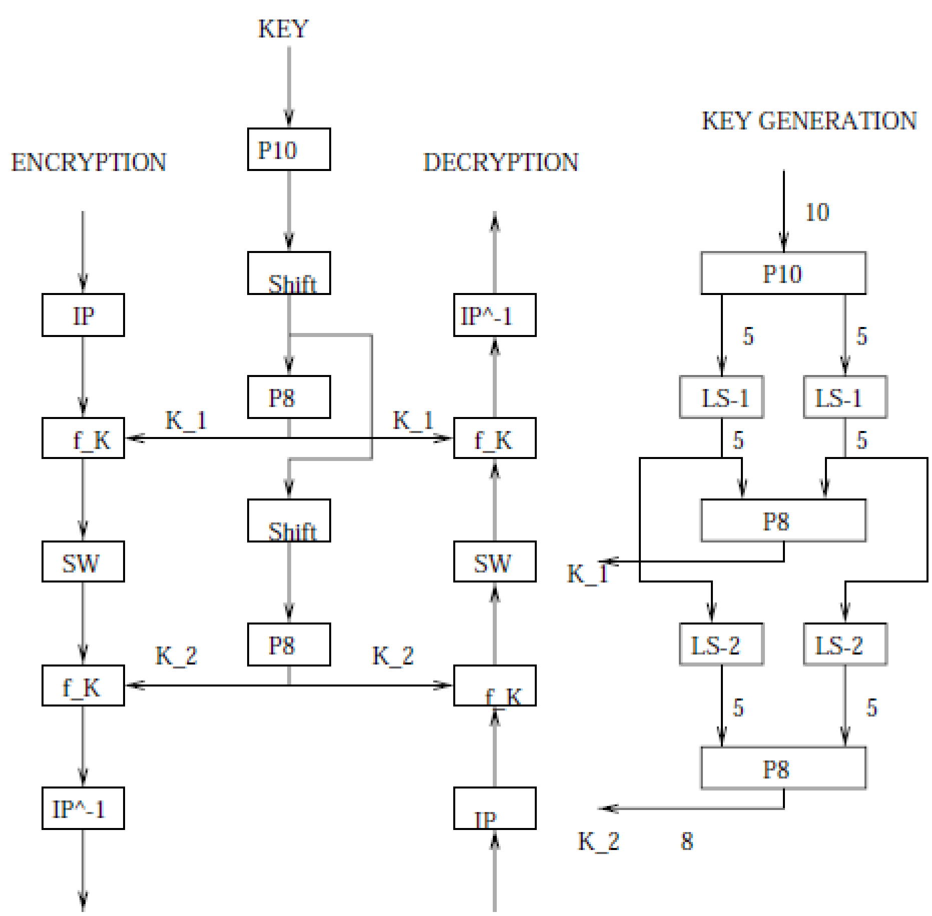
1. Hoán vụ ban đầu IP
2. Hàm f_K
3. Hàm đổi mà đổi hai nửa
4. Hàm f_K lần nữa
5. Hoán vị ngược IP^{-1} cua IP

Bước 2 và bước 4 sử dụng hai khóa K_1 và K_2 tương ứng, mà được sinh ra thông quan thuật toán sinh khóa.

Thuật toán sinh khóa:

Thuật toán sinh khóa gồm ba hàm mà áp dụng qua 5 bước để sinh ra hai khóa con:

1. Hoán vị P10 mà hoán vị 10 bit khóa ban đầu
2. Thao tác tách hai nửa và dịch trái mỗi nửa
3. Ghép hai nửa lại và cho qua hoán vị tám bit P8 để lấy 8 bit đầu ra làm khóa con thứ nhất K_1
4. Lặp lại bước 2 với dịch trái hai lần
5. Hoán vị tám bit để lấy ra 8 bit đầu ra làm khóa con thứ hai K_2



Sơ đồ mã DES đơn giản

Cấu trúc mã DES đơn giản:

S-Boxes:

$$S0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \quad S1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

Permutation P10:

$$\begin{pmatrix} 3 & 5 & 2 & 7 & 4 & 10 & 1 & 9 & 8 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$$

Permutation P8:

$$\begin{pmatrix} 6 & 3 & 7 & 4 & 8 & 5 & 10 & 9 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

Permutation P4:

$$\begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Ví dụ sinh khóa:

1. **key:**	1010000010	$:= K$
2. $P10$:	1000001100	
3. Split:	10000	01100
4a. L-Shift:	00001	11000
5a. Merge:	0000111000	
6a. $P8$:	10100100	$:= K_1$
4b. Double L-Shift:	00100	00011
5b. Merge:	0010000011	
6b. $P8$:	01000011	$:= K_2$

Như vậy khóa 10 bit K = 1010000010 ban đầu được sử dụng để sinh ra hai khóa con 8 bit: K_1 = 10100100 và K_2 = 01000011.

Các hàm cơ bản của mã DES đơn giản:

1. Mã hóa:

$$y = E_K(x) = IP^{-1} \circ f_{K_2} \circ SW \circ f_{K_1} \circ IP(x),$$

trong đó

$$\begin{aligned} K_1 &= P8(Shift(P10(K)) \\ K_2 &= P8(Shift(Shift(P10(K)))) \end{aligned}$$

2. Giải mã

$$x = D_K(y) = IP^{-1} \circ f_{K_1} \circ SW \circ f_{K_2} \circ IP(y)$$

3. IP là hoán vị dữ liệu 8 bit ban đầu :

$$\mathbf{IP} : \begin{pmatrix} 2 & 6 & 3 & 1 & 4 & 8 & 5 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

4. IP^{-1} là hoán vị ngược với IP:

$$\mathbf{IP}^{-1} : \begin{pmatrix} 4 & 1 & 3 & 5 & 7 & 2 & 8 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

5. Hàm đổi SW:

Đổi 4 bit trái và 4 bit phải cho nhau sao cho áp dụng lần hai hàm f_K được thực hiện trên 4 bit khác. Trong lần hai các đầu vào E, S0, S1, P4 vẫn như cũ và chỉ có khóa đầu vào là mới: K_2.

6. Hàm dịch trái vòng quanh: Đây là hàm dịch dãy bit sang trái vòng quang một vị trí được sử dụng trong thuật toán sinh khóa con.

7. Hàm f_K:

$$f_K(L, R) = (L \oplus F(R, SK), R),$$

Ở đây L và R là 4 bit trái và 4 bit phải của đầu vào dữ liệu 8 bit, được đưa vào làm đối số cho f_K, F là ánh xạ từ đầu vào là 4 bit và khóa con SK 8 bit với đầu ra là 4 bit. Chẳng hạn, giả sử L = 1011, R = 1101, F(R, SK) = 1110. Khi đó

$$\begin{aligned} f_K(L, R) &= (L \oplus F(R, SK), R) \\ &= (1011 \oplus 1110, 1101) \\ &= (0101, 1101) \end{aligned}$$

8. Hàm mở rộng: E mở rộng xâu 4 bit thành xâu 8 bit được cho như sau:

$$\begin{pmatrix} 4 & 1 & 2 & 3 & 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

Tám bit đầu ra của E biểu diễn dạng sau:

$$E = (n_4, n_{1,} n_2, n_{3, ,} n_2, n_{3, ,} n_4, n_1)$$

Giả sử 8 bit của khóa K_1 là:

$$K_1 = (k_{11}, k_{12}, k_{13}, k_{14}, k_{15}, k_{16}, k_{17}, k_{18})$$

Khi đó, kết quả E xor K_1 là dãy 8 bit:

n_4 xor $k_{11,}$ n_1 xor $k_{12,}$ n_2 xor $k_{13,}$ n_3 xor $k_{14,}$

n_2 xor $k_{15,}$ n_3 xor $k_{16,}$ n_4 xor $k_{17,}$ n_1 xor k_{18}

Kết quả tên được viết gọn dạng:

$$\begin{matrix} p_{00} & p_{01} & p_{02} & p_{03} \\ p_{10} & p_{11} & p_{12} & p_{13} \end{matrix}$$

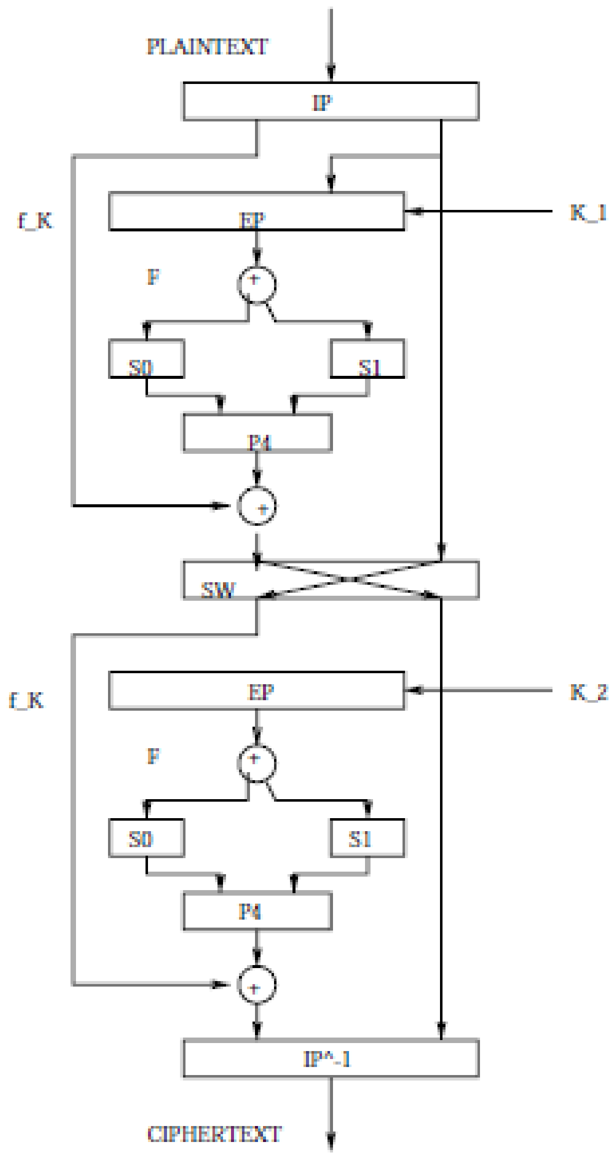
Bây giờ ta đẩy các hàng vào các hộp S box; 4 bit hàng trên vào hộp S1 và 4 bit hàng dưới vào hộp S2

9. Các hộp S box: Bốn bit đầu tiên (hang thứ nhất) được đẩy vào hộp S0 tạo hai bit đầu ra và bốn bit còn lại (hàng hai) được đẩy vào hộp S1 tạo hai bit đầu ra khác. Các hộp S box hoạt động như sau: Bit thứ nhất và bit thứ tư đầu vào được coi như số hai bit mà xác định hang của hộp S box, còn bit thứ hai và bit thứ ba tương tự xác định cột

của S box. Đầu ra là số của hộp S box ở vị trí hàng và cột đó và biểu diễn qua số hai bit. Tương tự đối với hộp S1.

Ví dụ: Giả sử: $p_{00}\ p_{01}\ p_{02}\ p_{03}$ = 0110 là.bốn bit hàng trên. Khi đó $p_{00}\ p_{03} = 00 =_2 0$, $p_{01}\ p_{02} = 11 =_2 3$ và đầu ra nằm ở hang 0 cột 3 của hộp S0 là số 2 có biểu diễn bit là 10. Như vậy kết quả đầu ra là hai bit 10.

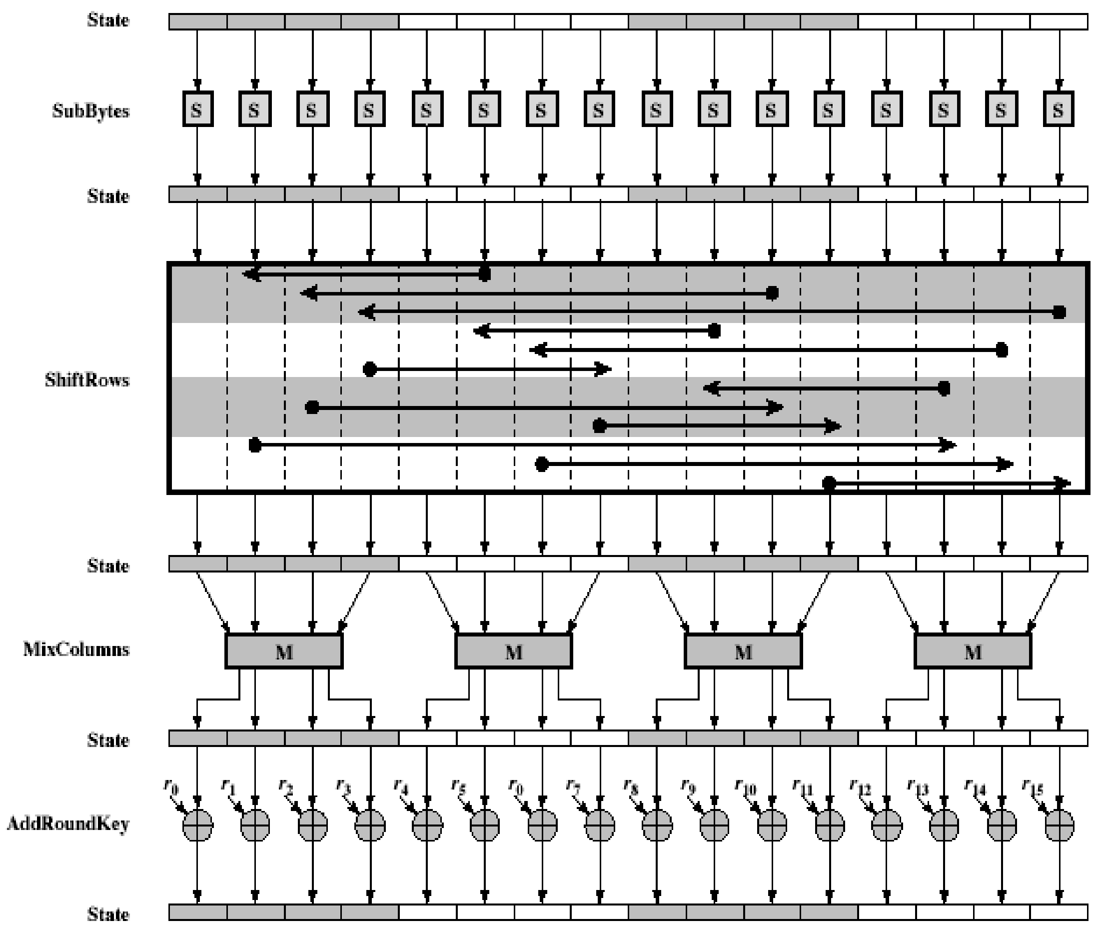
Sau đó bốn bit cho qua hoán vị P4 và bốn bit đầu ra đó là đầu ra của hàm F



Bài tập mã DES đơn giản:

1. Sinh cặp khóa K1, K2 từ khóa: K = 1001110110
2. Mã hai vòng một dữ liệu p = 01100011

2. MÃ AES:



Phép trộn cột:

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

- Sử dụng các đa thức bậc nhỏ hơn hoặc bằng n

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

- Có một số cách khác nhau
  - Có thể thực hiện các phép toán thông thường trên đa thức
  - Các phép toán trên đa thức với các hệ số trên module p
  - Các phép toán trên đa thức với các hệ số trên mod p và sau đó lấy mod m(x) (modulo theo đa thức m(x))
- Phép toán đa thức thông thường
- Cộng trừ các hệ số tương ứng
- Nhân mọi hệ số với cùng một số

Giả sử $f(x) = x^3 + x^2 + 2$ và $g(x) = x^2 - x + 1$

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

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

$f(x) \text{ x } g(x) = x^5 + 3x^2 - 2x + 2$

- Cho số nguyên tố p tùy ý
- Tính các hệ số theo module p
  - Tạo thành vành
- Quan tâm đến mod 2
  - là mọi hệ số là 0 hoặc 1
  - Chẳng hạn $f(x) = x^3 + x^2$ và $g(x) = x^2 + x + 1$

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

    $f(x) \text{ x } g(x) = x^5 + x^2$

- Cho đa thức g(x)
  - Viết f(x) dạng: $f(x) = q(x)\, g(x) + r(x)$
  - Có thể coi $r(x)$ là phần dư
  - **Ta viết:** $\boldsymbol{r(x) = f(x) \bmod g(x)}$
- Nếu không có phần dư ta nói g(x) là ước của f(x) hay g(x) chia hết f(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
- VD $x^3 + x + 1$ là nguyên tố; $x^4 + 1$ không nguyên tố $(x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1)$
- Số học đa thức theo module của đa thức nguyên tố tạo thành trường
- Có thể tính trên trường $GF(2^n)$
- Đa thức với các hệ số module 2 và bậc nhỏ hơn bằng n,

- Có thể rút gọn theo module của đa thức nguyên tố bậc n (đối với phép nhân)
- Tạo thành trường hữu hạn
- Có thể tìm được nghịch đảo nhờ thuật toán Euclide mở rộng

  Ví dụ Trường GL(2^3)

Table 4.6 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

Ước chung lớn nhất của hai đa thức:

- *c(x)* = 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 để tìm

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

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

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

3. R(x) = A(x) mod B(x)

4. A(x) = B(x)

5. B(x) = R(x)

6. goto 2

Trường GL(2^n) theo modulo đa thức:

Thuật toán nhân hai đa thức:
Cộng và nhân theo Shift và xor

- Vì các hệ số là 0, 1 nên các đa thức có thể biểu diễn như các xâu bit
- Phép cộng trở thành XOR trên các xâu bit đó

- Nhân trở thành Shift và XOR
- Phép tính module đa thức nguyên tố thực hiện bằng phép lặp thế bậc cao nhất với phần dư

Ví dụ: $(x^3 + x + 1).(x^2 + x + 1) \bmod (x^4 + 1)$

Sử dụng phương pháp Horners, viết dạng:

$(x^3 + x + 1) . (1 + x (1 + x)) \bmod (x^4 + 1)$

Đa thức nhân với x tương đương Shift sang trái <, phép xor tiến hành bất cứ lức nào khi dãy bit có độ dài 5, bằng độ dài của đa thức $x^4 + 1$ là 10001.
nên thực hiện dưới dạng dãy bit như sau:
1011 + (1011 < xor 10001) + (1011 < xor 10001) < =
1011 + (10110 xor 10001) + (0111 <) =
1011 + 0111 + 1110 =
1100 + 1110 = 10 -> x

AES đơn giản: (sẽ bổ sung)

BÀI 3: SỐ HỌC MODULO

1. Số học đồng dư

- Giả sử n là số nguyên dương, a là số nguyên, ta biểu diễn dưới dạng:

$$a = \lfloor a/n \rfloor . n + a \bmod n \qquad (*)$$

- Viết công thức (*) cho các cặp số (n, a) sau:
  - (15, 51): 51 = ?
  - (15, -51): -51 = ?
- Tìm đại diện của các số 215 và -157 theo mod 29
  - 215 mod 29 =
  - (-157) mod 29 =
- Theo modulo 13: chia tập các số từ -26 đến 25 thành các lớp tương đương, nêu các đại diện của chúng?
- Biểu thức nào đúng:
  - $101 \equiv 36 \bmod 13$?
  - $(-101) \equiv (-36) \bmod 13$?
  - $165 \equiv 34 \bmod 65$?
  - $(-165) \equiv 30 \bmod 65$?
- Viết công thức (*) cho các cặp số (n, a) sau:
  - (15, 51): 51 = 3.15 + 6; Do đó theo định nghĩa: 51 mod 15 = 6
  - (15, -51): -51 =-4.15 + 9; Vậy: (-51) mod 15 = 9
- Tìm đại diện của các số 215 và -157 theo mod 29
  - 215 mod 29 = 12; Do đó theo định nghĩa: 12 là đại diện của 215 theo modulo 29
  - -158 mod 29 = 29 – 158 mod 29 = 29 – 13 = 16
- Các lớp tương đương và đại diện modulo 13:

-26	-25	-24	-23	-22	-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

Hàng viết đậm từ 0 đến 12 gồm các đại diện của modulo 13.

- Quan hệ tương đương đồng dư: hai số có quan hệ đồng dư theo modulo n, nếu chúng có cùng số dư khi chia cho n:
  - $101 \equiv 36 \bmod 13$? – Đúng
  - $-101 \equiv -36 \bmod 13$? – Sai
  - $165 \equiv 34 \bmod 65$? - Sai
  - $-165 \equiv 30 \bmod 65$? - Đúng

Các công thức cộng, trừ, nhân theo modulo:

$$(a \pm b) \bmod n = [a \bmod n \pm b \bmod n] \bmod n \qquad (**)$$

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

- Lập bảng nhân theo modulo 11, nêu các cặp nghịch đảo nhau trong bảng.
- Bạn có thể thay các số bằng các số tương đương theo mod n bất cứ lúc nào?
    - (74 - 215) mod 9 = ?
    - (244.315) mod 250 = ?
    - (144.315 – 265.657) mod 51 = ?

Bảng nhân modulo 11

X	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	8	2	6	10	3	4
5	0	5	10	4	8	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	11	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Các cặp sau nghịch đảo nhau theo modulo 11, vì chúng có tích theo modulo bằng 1:
(1, 1), (2, 6), (3, 4), (4, 3), (5, 9), (6, 2), (7, 8), (8, 7), (9, 5), (10, 10)
Cộng, nhân modulo

- Áp dụng tính chất (**):
  (74 -215) mod 9 = -141 mod 9 = 9 -141 mod 9 = 9-6=3
  hay   (74 mod 9 - 215 mod 9) mod 9 =
  (2 - 8) mod 9 = -6 mod 9 = 3
- Áp dụng tính chất (***):
  (244 . 315) mod 250 = (244 mod 250 . 315 mod 250) mod 250
  = ((-6) mod 250 . 65 mod 250) mod 250   = (-6 .65) mod 250 = (-390) mod 250
  = 250 - 390 mod 250 = 250 -140 =110
- (144.315 – 265.657) mod 51

= (144.315 mod 51 – 265.657 mod 51) mod 51

= (-9.9 mod 51– (10.(-6)) mod 51) mod 51

= (-81 + 60) mod 51 = -21 mod 51 = 51 – 21 mod 51 = 30

Thuật toán Euclid

Áp dụng thuật toán Euclid:

2110 = 1 x 1945 + 165	gcd(1945, 165)
1945 = 11 x 165 + 130	gcd(165, 130)
165 = 1 x 130 + 35	gcd(130, 35)
130 = 3 x 35 + 25	gcd(35, 25)
35 = 1 x 25 + 10	gcd(25, 10)
25 = 2 x 10 + 5	gcd(10, 5)
10 = 2 x 5 + 0	gcd(5, 0)

Vậy ta có ước chung cần tìm là 5:

GCD(2110, 1945) = GCD(5, 0) = 5

Thuật toán Euclid mở rộng

- Số a được gọi là nghịch đảo của b theo mod m, ký hiệu $a = b^{-1}$ mod m, nếu

  (a.b) mod m = 1

  Nếu gcd(b, m) = 1, tức là hai số nguyên tố cùng nhau, thì tồn tại b^{-1} mod m
- Tìm trực tiếp bằng định nghĩa **đối với modulo theo**
  - 6^{-1} mod 11 = ?
  - 5^{-1} mod 11 = ? Gợi ý: (-10) mod 11 = 1 mod 11
  - 6^{-1} mod 13 = ? Gợi ý: (-12) mod 13 = 1 mod 13
  - 12^{-1} mod 13 = ?; $(n-1)^{-1}$ mod n = ?
  - 13^{-1} mod 15 = ? Gợi ý: 13^{-1} mod 15 = $(-2)^{-1}$ mod 15
  - 21^{-1} mod 25 = ? Gợi ý: 21^{-1} mod 25 = $(-4)^{-1}$ mod 25 và (-24) mod 25 = 1 mod 25

Giải:

- 6^{-1} mod 11 = 2, vì 6.2 mod 11 = 1
- 5^{-1} mod 11 = 9, vì 9.5 mod 11 = 1
- 6^{-1} mod 13 =11, vì (-2).6 mod 13 = 1
- 12^{-1} mod 13 = $(-1)^{-1}$ mod 13 = -1 mod 13 = 12
- $(n-1)^{-1}$ mod n = n-1

- 13^{-1} mod 15 = $(-2)^{-1}$ mod 15 = -8 mod 15 = 7
- 21^{-1} mod 25 = $(-4)^{-1}$ mod 15 = 6

Tìm nghịch đảo theo mod 19:

- 2^{-1} mod 19 = 10
- 3^{-1} mod 19 = (-6) mod 19 = 13   Lưu ý: (-18) ≡ 1 mod 19
- 4^{-1} mod 19 = 5
- 5^{-1} mod 19 = 4
- 6^{-1} mod 19 = (-3) mod 19 = 16
- 7^{-1} mod 19 = (-8) mod 19 = 11   Lưu ý: 19*3-1 = 56; (-56) ≡ 1 mod 19
- 8^{-1} mod 19 = (-7) mod 19 = 12
- 9^{-1} mod 19 = (-2) mod 19 = 17
- 10^{-1} mod 19 = 2
- 11^{-1} mod 19 = 7
- 12^{-1} mod 19 = $(-7)^{-1}$ mod 19 = 8
- 13^{-1} mod 19 = $(-6)^{-1}$ mod 19 = 3
- 14^{-1} mod 19 = $(-5)^{-1}$ mod 19 = (-4) mod 19 = 15
- 15^{-1} mod 19 = $(-4)^{-1}$ mod 19 = (-5) mod 19 = 14
- 16^{-1} mod 19 = $(-3)^{-1}$ mod 19 = 6
- 17^{-1} mod 19 = $(-2)^{-1}$ mod 19 = (-10) mod 19 = 9
- 18^{-1} mod 19 = 19

Bài tập:

a) Tìm nghịch đảo theo mod 23

b) Tìm nghịch đảo theo mod 29

- Với các số lớn thì ta dùng thuật toán nào để tìm nghịch đảo của số b theo modulo n?
  - 845^{-1} mod 2011 = ? Ta sử dụng thuật toán Euclid mở rộng để tìm nghịch đảo.

Q	A1	A2	A3	B1	B2	B3
—	1	0	2011	0	1	845
2	0	1	845	1	–2	321
2	1	–2	321	–2	5	203
1	–2	5	203	3	–7	118

1	3	-7	118	-5	12	85
1	-5	12	85	8	-19	33
2	8	-19	33	-21	50	19
1	-21	50	19	29	-69	14
1	29	-69	14	-50	119	5
2	-50	119	5	129	-307	4
1	129	-307	4		426	1

- Vậy 845^{-1} mod 2011 = 426 mod 2011= 426

Bài tập:

a) Tìm nghịch đảo: 47^{-1} mod 187;

b) Tìm nghịch đảo: 101^{-1} mod 323;

c) Tìm nghịch đảo: 357^{-1} md 809

2. Các định lý số học cơ bản

- **Định lý Ferma nhỏ:** Cho p là số nguyên tố và a là số nguyên dương không là bội của p, tức là GCD(a, p) = 1. Khi đó

  $$a^{p-1}(\text{mod } p) = 1$$

  hay $$a^{p}(\text{mod } p) = a\ (\text{mod } p)$$

- Tính các giá trị sau:
  - $5^{12}(\text{mod } 13) = 1$
  - $8^{13}(\text{mod } 13) = 8$
  - $10^{100}(\text{mod } 17) = (10^{16})^{6} \cdot 10^{4}(\text{mod } 17) = 9^{2}\text{mod } 17 = 13$
  - $15^{125}(\text{mod } 19) = (15^{18})^{7}.15^{-1}(\text{mod } 19) = 14$

Bài tập. Áp dụng Định ý Fecma tính:

a) 159^{130} mod 31

b) 713^{520} mod 101

- **Hàm Euler**. Hàm Euler của một số n là số các số nguyên tố cùng nhau với n và nhỏ hơn n.

N	Φ(n)	Điều kiện

P	P – 1	p nguyên tố
p^n	$p^n - p^{n-1}$	p nguyên tố
s.t	$\Phi(s).\Phi(t)$	s, t nguyên tố cùng nhau
p.q	(p-1)(q-1)	p, q hai nguyên tố khác nhau

- Tính giá trị hàm Euler:
  - $\Phi(23) = 22$
  - $\Phi(55) = \Phi(5.11) = \Phi(5).\Phi(11) = 4.10 = 40$
  - $\Phi(180) = \Phi(4.5.9) = \Phi(4).\Phi(5).\Phi(9) = \Phi(2^2).\Phi(5).\Phi(3^2) = (2^2 -2).4.(3^2-3) = 48$
  - $\Phi(200) = \Phi(8.25) = \Phi(2^3).\Phi(5^2) = (2^3 -2^2).(5^2-5) = 80$
  - $\Phi(900) = \Phi(4.9.25) = \Phi(4).\Phi(9).\Phi(25) = \Phi(2^2).\Phi(3^2).\Phi(5^2)$
    $= (2^2 -2).(3^2-3).(5^2-5) = 2.6.20 = 240$
  - $\Phi(6300) = \Phi(7.900) = \Phi(7).\Phi(900) = 6.240 = 1440$

Bài tập. Tính giá trị hàm Euler:

a) $\Phi(47)$

b) $\Phi(247)$

c) $\Phi(5400)$

Định lý Euler

- Cho a, n là hai số tự nhiên nguyên tố cùng nhau, tức là gcd(a,n) = 1. Khi đó

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

- Tính:
  - 4^8 mod 15= 1, vì $\Phi(15) = 8$, gcd(4, 15) = 1.
  - 11^9 mod 20= 10, vì $\Phi(20) = 8$, gcd(11, 20) = 1
  - 12^{402} mod 25= 19, vì $\Phi(25) = 20$, gcd(12, 25) = 1, 402 = 20.20 + 2,
  - 12^{402} mod 25= $12^{400}.12^2$mod 25= 144 mod 25 = 19
  - 135^{162} mod 64= (135 mod 64)$^{32.5+2}$ mod 64 = 7^2mod 64=49, vì $\Phi(64) = \Phi(2^6) = 64 - 32 = 32$
  - 335^{453} mod 23= (335 mod 23)$^{22.20+13}$ mod 23 = 5^{13}mod 23 =$5^8.5^4.5$mod 23 = 16.4.5 mod 23 = 21, vì $\Phi(23) = 22$
  - $(3/7)^8$ mod 10=$(3.7^{-1})^8$mod 10 = $(3.3)^8$ mod 10 = $(-1)^8$ mod 10 = 1

Bài tập. Áp dụng Định ý Euler tính:

a) 15^{39} mod 51
b) 143^{230} mod 60
c) 37^{168} mod 187
d) 613^{520} mod 437

Lũy thừa theo modulo

- Dựa vào định lý Euler đơn giản bài toán:
  11^{183} mod 187 = ?
  $\Phi(187) = \Phi(11.17) = 10.16 = 160$
  11^{183} mod 187 = $11^{183 \bmod 160}$ mod 187 = 11^{23} mod 187

- Theo thuật toán lũy thừa dựa trên biểu diễn nhị phân của số mũ n
  - 11^{23} mod 187
    $23 = 16 + 4 + 2 + 1$; $23_2 = 10111$

    $11^{23} \bmod 187 = ((((1^2.11)^2)^2.11)^2.11)^2.11) \bmod 187$
    $= ((((121)^2)^2\ 11)^2\ 11)^2\ 11 \bmod 187$
    $= (((55)^2\ 11)^2\ 11)^2\ 11 \bmod 187$
    $= ((33.11)^2\ 11)^2\ 11 \bmod 187$
    $= (121.11)^2.11 \bmod 187$
    $= 110.11 \bmod 187$
    $= 88$
- Sử dụng công thức đệ qui để tính lũy thừa một cách hiệu quả:
  $a^n = (a^{n/2})^2$ nếu n chẵn
  $a^n = a.(a^{n-1/2})^2$ nếu n lẻ
  Hay khi tính bằng tay:
  $a^n = (a^2)^{n/2}$ nếu n chẵn
  $a^n = a.(a^2)^{n-1/2}$ nếu n lẻ

- Trên thực tế tính toán bằng tay được dựa trên phép lặp bình phương và nhân với cơ số
  - $11^{23} \bmod 187 = 11.(11^2)^{11} \bmod 187$
    $= 11.121.(121^2)^5 \bmod 187$
    $= 11.121.55.(55^2)^2 \bmod 187$
    $= 11.121.55.33^2 \bmod 187$
    $= (11.121.55.154) \bmod 187$

$= 88$

Định lý Trung Hoa:

- **Tính toán theo modulo số lớn.** Để tính A mod M, với M 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 $M_i = M/m_i$

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

Ví dụ. Tính 101^{59} mod 323. Áp dụng định lý phần dư Trung Hoa, ta coi

$A = 101^{59}$, $m_1 = 17$, $m_2 = 19$. Khi đó $M_1 = 19$, $M_2 = 17$ và

$19^{-1} \bmod 17 = 2^{-1} \bmod 17 = 9$, suy ra $c_1 = 19.9 = 171$

$17^{-1} \bmod 19 = (-2)^{-1} \bmod 19 = (-10) \bmod 19 = 9$, suy ra $c_2 = 17.9 = 153$

$a_1 = 101^{59} \bmod 17 = (101 \bmod 17)^{59 \bmod 16} \bmod 17$
$= 16^{11} \bmod 17 = (-1)^{11} \bmod 17 = 16$

$a_2 = 101^{59} \bmod 19 = (101 \bmod 19)^{59 \bmod 18} \bmod 19$
$= 6^5 \bmod 19 = 6.(6^2)^2 \bmod 19$
$= 6. (-2)^2 \bmod 19 = 5$

Vậy $A = 101^{59} \bmod 323 = (16.171 + 5.153) \bmod 323 = 271$

Bài tập

a. Tính: 113^{199} mod 247

b. Tính: 197^{211} mod 667

Giải hệ phương trình modulo.

Cho a_i = x mod 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. Coi x là biểu thức cần tính theo modulo số lớn M= $m_1 m_2 .. m_k$.

Ví dụ. Cho x ≡ 6 mod 11, x ≡ 4 mod 13 và , x ≡ 9 mod 17

Tìm x.

Áp dụng định lý phần dư Trung hoa, ta tính:

M_1 = 13.17 = 221, M_2 = 11.17 = 187, M_3 = 11.13 = 143

M_1^{-1} mod m_1 = 221^{-1} mod 11 = 1^{-1} mod 11 = 1

M_2^{-1} mod m_2 = 187^{-1} mod 13 = 5^{-1} mod 13 = 8

M_3^{-1} mod m_3 = 143^{-1} mod 17 = 7^{-1} mod 17 = 5

Như vậy

x = (6.221.1 + 4.187.8 + 9.143.5) mod (11.13.17) = 1590 mod 2431

Bài tập. Giải các hệ phương trình modulo sau:

a) x mod 29 = 18, x mod 37 = 25

b) x mod 17 = 8, x mod 23 = 20, x mod 29 = 14

c) x mod 15 = 8, x mod 32 = 23

d) x mod 8 = 7, x mod 9 = 5, x mod 25 = 12

3. Căn nguyên thủy

- Xét m để a^m mod n = 1.
  Nếu giá trị m = Φ(n) là số dương nhỏ nhất thoả mãn công thức trên thì, a được gọi là căn nguyên thủy của n.
- a = 2 có phải là căn nguyên thủy của 7 không? Φ(7)= 6
  2 mod 7 = 2 ; 2^2 mod 7 = 4 ; 2^3 mod 7 = 1 ;
  3 < 6 = Φ(7), vậy 2 không là căn nguyên thủy của 7.
- a = 2 có phải là căn nguyên thủy của 11 không? Φ(11)= 10
  2 mod 11 = 2 ; 2^2 mod 11 = 4 ; 2^3 mod 11 = 8;
  2^4 mod 11 = 5 ; 2^5 mod 11 = 10 ; 2^6 mod 11 = 9,
  2^7 mod 11 = 7 ; 2^8 mod 11 = 3 ; 2^9 mod 11 = 6, 2^{10} mod 11 = 1
  Vậy 2 là căn nguyên thủy của 11.
- a = 3 có phải là căn nguyên thủy của 11 không? Φ(11)= 10
  3 mod 11 = 3 ; 3^2 mod 11 = 9; 3^3 mod 11 = 5;
  3^4 mod 11 = 4; 3^5 mod 11 = 1;
  5 < 10 = Φ(11), vậy 3 không là căn nguyên thủy của 11.

Bài tập. Các khẳng định sau đây có đúng không?

a) 5 là căn nguyên thủy của 11?

b) 6 là căn nguyên thủy của 13?

c) 10 là căn nguyên thủy của 17?

d) 10 là căn nguyên thủy của 19?

e) 10 là căn nguyên thủy của 23?

f) 13 là căn nguyên thủy của 23?

4. **Logarit rời rạc**

- Cho a, b, p là các số tự nhiên, với gcd(a,p)=1 = gcd(b,p)
- Tìm x sao cho $a^x = b \bmod p$ Hay $x = \log_a b \bmod p$
- Dễ dàng thấy, nếu a là căn nguyên thủy của p thì luôn luôn tồn tại:
  - $x = \log_2 5 \bmod 11 = 4$

    $2^0 \bmod 11 = 1$; $2^1 \bmod 11 = 2$; $2^2 \bmod 11 = 4$;
    $2^3 \bmod 11 = 8$; $2^4 \bmod 11 = 5$;
  - $x = \log_2 5 \bmod 13 = 9$

    $2^0 \bmod 13 = 1$; $2^1 \bmod 13 = 2$; $2^2 \bmod 13 = 4$;

    $2^3 \bmod 13 = 8$; 24 mod 13 = 3 ; $2^5 \bmod 13 = 6$;

    $2^6 \bmod 13 = 12$; $2^7 \bmod 13 = 11$; $2^8 \bmod 13 = 9$;

    $2^9 \bmod 13 = 5$;
  - $x = \log_3 7 \bmod 13 = ?$

    $3^0 \bmod 13 = 1$; $3^1 \bmod 13 = 3$; $3^2 \bmod 13 = 9$;
    $3^3 \bmod 13 = 1$,

Vô nghiệm (3 không phải là căn nguyên thủy của 13).

- Trong khi lũy thừa là bài toán dễ dàng, thì bài toán logarit rời rạc là bài toán khó.

Bài tập. Tính các logarit rời rạc sau:

a) $\log_6 9 \bmod 13$?

b) $\log_6 11 \bmod 13$?

c) $\log_{10} 15 \bmod 17$?

d) $\log_{10} 16 \bmod 19$?

e) $\log_{10} 8 \bmod 23$?

BÀI TẬP ÔN TẬP

1. Tìm phần dư dương khi chia:

a. 51 cho 15
b. -51 cho 15

2. Tìm đại diện của các số 215 và -157 theo mod 29
3. Chia tập các số từ -26 đến 25 thành các lớp tương đương theo mod 13, nêu các đại diện của chúng?
4. Biểu thức nào đúng:
   a. $101 \equiv 36 \bmod 13$?
   b. $(-101) \equiv (-36) \bmod 13$?
   c. $165 \equiv 34 \bmod 65$?
   d. $(-165) \equiv 30 \bmod 65$?
5. Lập bảng nhân theo modulo 11, nêu cặp các số nghịch đảo nhau trong bảng.
6. Thay các số bằng các số tương đương đồng dư để tính các biểu thức sau
   a. (74 -215) mod 9
   b. (244 . 315) mod 250
   c. (144.315 – 265.657) mod 51
7. Tìm các số nghịch đảo sau trực tiếp bằng định nghĩa:
   a. $6^{-1} \bmod 11 = ?$
   b. $5^{-1} \bmod 11 = ?$
   c. $6^{-1} \bmod 13 = ?$
   d. $12^{-1} \bmod 13 = ?$; $(n-1)^{-1} \bmod n = ?$
   e. $13^{-1} \bmod 15 = ?$
   f. $21^{-1} \bmod 25 = ?$
8. Tìm ước chung GCD(2110, 1945) theo thuật toán Euclide.
9. Dùng thuật toán Euclide mở rộng để tìm nghịch đảo $845^{-1} \bmod 2011 = ?$
10. Giải hệ phương trình Modulo sau: cho X mod 25 = 5 và X mod 23 = 15 . Tìm X
11. Dùng Định lý Ferma tính
    a. $5^{12} (\bmod 13) = ?$
    b. $8^{13} (\bmod 13) = ?$
    c. $10^{100} (\bmod 17) = ?$
    d. $15^{125} (\bmod 19) = ?$
12. Tính giá trị hàm Euler:
    a. $\Phi(23) = ?$
    b. $\Phi(55) = ?$

c. $\Phi(180) = ?$
d. $\Phi(200) = ?$
e. $\Phi(900) = ?$
f. $\Phi(6300) = ?$

13. Dùng Định lý Euler tính giá trị các biểu thức sau:
    a. 4^{10} mod 15= ?
    b. 11^{7} mod 20= ?
    c. 12^{402} mod 25= ?
    d. 135^{162} mod 64= ?
    e. 335^{453} mod 23= ?
    f. $(3/7)^{8}$ mod 10= ?
14. Sử dụng thuật toán lũy thừa dựa trên biểu diễn nhị phân của số mũ n, tính 11^{23} mod 187.
15. Tính toán các lũy thừa sau dựa trên phép lặp bình phương và nhân với cơ số:
    a. 11^{23} mod 187
    b. 43^{101} mod 247
16. Kiểm tra các khẳng định sau:
    a. a = 2 có phải là căn nguyên thủy của 3 không? .
    b. a = 2 có phải là căn nguyên thủy của 5 không?
    c. a = 3 có phải là căn nguyên thủy của 7 không?
17. Tính logarit rời rạc sau:
    - $\log_2 5$ mod 11 = ?
    - $\log_2 5$ mod 13 = ?
    - $\log_3 7$ mod 13 = ?
    - $\log_2 5$ mod 9 = ?
    - $\log_2 6$ mod 9 = ?
    - $\log_2 7$ mod 9 = ?
    - $\log_2 4$ mod 9 = ?
18. Tính logarit rời rạc sau:
    - $\mathrm{Log}_{10} 5$ mod 17 = ?
    - $\mathrm{Log}_{10} 9$ mod 17 = ?
    - $\mathrm{Log}_{10} 7$ mod 19 = ?
    - $\mathrm{Log}_{10} 4$ mod 19 = ?

- $\text{Log}_{10}\ 6 \bmod 23 =\ ?$

BÀI 4: MÃ VÀ TRAO ĐỔI KHÓA CÔNG KHAI

1. Mã công khai RSA

- Chọn ngẫu nhiên 2 số nguyên tố p và q
- Tính: $N = p.q$; $\Phi(N) = (p - 1).(q - 1)$
- Người dùng A chọn ngẫu nhiên khoá công khai (hoặc riêng) e: $1 < e < \Phi(N)$, $gcd(e, \Phi(N)) = 1$.
- Tìm khóa riêng (hoặc công khai) d của A: $(e.d) \bmod \Phi(N) = 1$, $0 < d < \Phi(N)$.
- Để mã hoá mẩu tin gửi cho A, người gửi B:
  - Tính $C = M^e \bmod n$, trong đó $0 \leq M < n$.
  - Để giải mã, người sở hữu khóa riêng:
  - Tính $M = C^d \bmod n$
- Để ký mẩu tin M gửi cho B, người gửi A mã bằng khóa riêng của mình:
  - Tính $C = M^d \bmod n$, trong đó $0 \leq M < n$.
  - Để kiểm tra chữ ký, người nhận giải mã bằng khóa công khai của người gửi:
  - Tính $M = C^e \bmod n$
- Cho p = 3; q = 11; khóa công khai e = 7; thông điệp M = 5.
  - $N = 3.11 = 33$; $\Phi(N) = 2.10 = 20$;
  - $d = e^{-1} \bmod \Phi(N) = 7^{-1} \bmod 20 = 3$, khóa riêng d = 3;
  - Mã: $C = M^e \bmod n = 5^7 \bmod 33 = 5.(5^2)^3 \bmod 33 = 5.25.(-8)^2 \bmod 33 = 14$;
  - Giải mã: $M = C^d \bmod n = 14^3 \bmod 33 = (-2).14 \bmod 33 = 5$.
- Cho p = 5; q = 11; khoá riêng e = 3; thông điệp M = 9.
  - $N = 5.11 = 55$; $\Phi(N) = 4.10 = 40$;
  - $d = e^{-1} \bmod \Phi(N) = 3^{-1} \bmod 40 = 27$, khóa công khai d = 27;
  - Ký: $C = M^e \bmod n = 9^3 \bmod 55 = 26.9 \bmod 55 = 14$;
  - Kiểm tra chữ ký: $M = C^d \bmod n = 14^{27} \bmod 55 = 14.(14^2)^{13} \bmod 55 =$ $14\ 196^{13} \bmod 55 = 14.31.(31^2)^6 \bmod 55 = 14.31.961^6 \bmod 55 =$ $14.31.26^6 \bmod 55 = 14.31.(26^2)^3 \bmod 55 = 14.31.16^3 \bmod 55 =$ $14.31.16.36od\ 55 = (26(-6)) \bmod 55 = 9$;
    ($14^2 mod55=31$, $14^4 mod55=26$, $14^8 mod55=16$, $14^{16} mod55=36$)
- Cho p = 7; q = 11; khoá công khai e = 13; thông điệp M = 3.
  - $N = 7.11 = 77$; $\Phi(N) = 6.10 = 60$;
  - Khóa riêng $d = e^{-1} \bmod \Phi(N) = 13^{-1} \bmod 60 = 37$;
  - Mã: $C = M^e \bmod n = 3^{13} \bmod 77 = (3^8 3^4 3) \bmod 77 = (4^2.4.3) \bmod 77 = 38$;
  - Giải mã: $M = C^d \bmod n = 38^{37} \bmod 77 = 3$.

- Có thể dùng định lý phần dư Trung Hoa để giải mã cho nhanh:
  - Tính C^d mod 7 = 38^{37} mod 7 = 3^{37} mod 7 = $3^{36}.3$ mod7 = 3;
  - Tính C^d mod 11 = 38^{37} mod11 = 5^{37} mod 11 = $5^{30}.5^7$ mod11 = 3;
  - Tính $a_1 = 11^{-1}$ mod 7 = 4^{-1} mod 7 = 2;
  - Tính $a_2 = 7^{-1}$ mod 11 = 8;
  - $c_1 = 11.(11^{-1}$ mod 7) = 11.2 = 22;
  - $c_2 = 7(7^{-1}$ mod 11) =7.8 = 56;
- Vậy M = ($a_1c_1 + a_2c_2$) mod77 = (3.22 + 3.56) mod 77 = 3.

Bài tập:

a. Cho p = 11, q = 13, Tính N, Φ(N).
   A lấy khóa riêng e = 17, tính khóa công khai d?
   B dùng khóa công khai d của A mã thông điệp m = 8. Tính bản mã C.
   A sử dụng Định lý phần dư Trung hoa giải mã. Nếu tính toán của A

b. Cho p = 13, q = 17, Tính N, Φ(N).
   A lấy khóa riêng e = 53, tính khóa công khai d?
   A dùng khóa riêng e ký thông điệp m = 31 sử dụng Định lý phần dư Trung Hoa. Tính bản ký C
   B sử dụng khóa công khai của A giải mã C. Nếu tính toán của B

c. Cho p = 17, q = 19, Tính N, Φ(N).
   A lấy khóa riêng e = 29, tính khóa công khai d?
   B dùng khóa công khai d của A mã thông điệp m = 8. Tính bản mã C.
   A sử dụng Định lý phần dư Trung hoa giải mã. Nếu tính toán của A

d. Cho p = 19, q = 23, Tính N, Φ(N).
   A lấy khóa riêng e = 41, tính khóa công khai d?
   A dùng khóa riêng e ký thông điệp m = 15 sử dụng Định lý phần dư Trung Hoa. Tính bản ký C
   B sử dụng khóa công khai của A giải mã C. Nếu tính toán của B

2. Trao đổi khóa DIFFIE - HELLMAN

- Mọi người dùng thỏa thuận dùng tham số chung:
  - Lấy số nguyên tố rất lớn q;
  - Chọn α là căn nguyên tố của q.
- Mỗi người dùng (A chẳng hạn) tạo khoá của mình:
  - Chọn một khoá mật (số) $x_A < q$;
  - Tính khoá công khai $y_A = \alpha^{x_A} \bmod q$

- Mỗi người dùng thông báo công khai khóa của mình y_A
- Khóa bộ phận dùng chung cho hai người sử dụng A, B là K_{AB}
  - $K_{AB} = \alpha^{x_A . x_B} \bmod q$

    $= y_A^{x_B} \bmod q$ (mà B có thể tính)

    $= y_B^{x_A} \bmod q$ (mà A có thể tính)
- Hai người dùng A và B muốn trao đổi khoá phiên:
  - Đồng ý chọn số nguyên tố $q = 11$ và $\alpha = 2$;
  - A chọn khoá riêng $x_A = 9$; B chọn khóa riêng $x_B = 3$;
  - Tính các khoá công khai:

    $y_A = \alpha^{x_A} \bmod q = 2^9 \bmod 11 = 6$

    $y_B = \alpha^{x_B} \bmod q = 2^3 \bmod 11 = 8$
- Tính khoá phiên chung:

  $K_{AB} = y_B^{x_A} \bmod q = 8^9 \bmod 11 = 7$ (A)

  $K_{AB} = y_A^{x_B} \bmod q = 6^3 \bmod 11 = 7$ (B)
- Hai người sử dụng A và B muốn trao đổi khoá phiên:
  - Đồng ý chọn số nguyên tố $q = 13$ và $\alpha = 6$
  - A chọn khoá riêng $x_A = 5$; B chọn khóa riêng $x_B = 7$
  - Tính các khoá công khai:

    $y_A = \alpha^{x_A} \bmod q = 6^5 \bmod 13 = 2$

    $y_B = \alpha^{x_B} \bmod q = 6^7 \bmod 13 = 7$
- Tính khoá phiên chung:

  $K_{AB} = y_B^{x_A} \bmod q = 7^5 \bmod 13 = 11$ (A)

  $K_{AB} = y_A^{x_B} \bmod q = 2^7 \bmod 13 = 11$ (B)

Bài tập. : Trao đổi khóa Diffie-Hellman

a. Cho $q = 43$, $\alpha = 3$. Chứng tỏ rằng 3 là căn nguyên thủy của 43.

Người sử dụng A chọn khóa riêng $x_A = 13$.

Người sử dụng B chọn khóa riêng $x_B = 37$.

Nêu tính toán khóa chung K_{AB} của A.

Nêu tính toán khóa chung K_{AB} của B.

b. Cho $q = 17$, $\alpha = 10$, $x_A = 7$, $x_B = 5$. Tính y_A ; y_B và nêu tính toán của A, B tìm khoá chung K_{AB}.
c. Cho $q = 23$, $\alpha = 10$, $x_A = 8$, $x_B = 12$. Tính y_A ; y_B và nêu tính toán của A, B tìm khoá chung K_{AB}.
d. Cho $q = 809$, $\alpha = 3$.

Người sử dụng A chọn khóa riêng $x_A = 343$.

Người sử dụng B chọn khóa riêng $x_B = 257$.

Nêu tính toán khóa chung K_{AB} của A.

Nêu tính toán khóa chung K_{AB} của B.

3. Mã Elgamal

Mã RSA đòi hỏi mỗi người sử dụng có một cặp số nguyên tố lớn (p, q) riêng. Hai người sử dụng không được dùng chung cặp số (p, q), vì như vậy sẽ lộ khóa riêng. Chính vì vậy mã khóa công khai RSA đòi hỏi trả giá tính toán nhiều, vì kiểm tra số nguyên tố lớn là việc làm không đơn giản.

Người ta mong muốn một loại mã khóa công khai mà có các số nguyên tố lớn dùng chung, ở đó mỗi người sử dụng chỉ việc chọn cho mình một khóa riêng và tính tooán khóa công khai chia sẻ với mọi người, mà việc tìm khóa riêng khi biết khóa công khai vẫn là một bài toán khó.

Nhóm giao hoán hữu hạn là một tập hợp, trên đó có định nghĩa phép nhân hai phần tử, thỏa mãn các tính chất sau:

- Tích hai phần tử của tập hợp là một phần tử của tập hợp đó
- Phép nhân có tính giao hoán
- Có phần tử đơn vị e: a.e = e.a = a   đối với mọi phần tử a của tập hợp đó
- Mọi phần tử a đều có phần tử nghịch đảo a^{-1}, sao cho: $a.a^{-1} = a^{-1}.a = e$

Số phần tử của tập hợp hữu hạn đó được gọi là bậc của nhóm.

Nếu một nhóm giao hoán hữu hạn G bậc q có phần tử g sao cho:

$$G = \{g^0 = e, g, g^2, ..., g^{q-1}\}$$

thì G được gọi là nhóm xiclic có g là phần tử sinh.

Mã Elgamal:

Không giống như các thuật toán RSA, trong mã hóa Elgamal có một số thông số nào đó có thể được chia sẻ bởi một số người sử dụng. Chúng được gọi là các thông số tên miền. Khi đó thuật toán mã hóa Elgmal tiến hành qua các bước sau:

Bước 1: Chọn p một "nguyên tố lớn" sao cho bài toán Logarit rời rạc trong F_p là khó giải, qua đó chúng ta có nghĩa là một với khoảng 1024 bits, như vậy là (p – 1) chia hết cho một 'số nguyên tố vừa' q khoảng 160 bit.

Chọn g một phần tử của F_p^* của số nguyên tố q, ví dụ: $g = r^{\frac{p-1}{q}} \pmod p) \neq 1$ (với $r \in F_p^*$)

Một khi các tham số miền đã được cố định, các khóa công khai và khóa riêng có thể được xác định.

Bước 2: Các khóa riêng được chọn là một số nguyên x, trong khi khóa công khai được cho bởi: $h = g^x (\bmod p)$

Chú ý rằng trong khi mỗi người dùng trong RSA cần thiết để tạo ra hai số nguyên tố lớn để thiết lập cặp khóa của họ (đó là một công việc tốn kém), để mã hóa Elgamal mỗi người dùng chỉ cần tạo ra một số ngẫu nhiên và thực hiện một lũy thừa mô–đun để tạo một cặp khóa.

Bước 3: Mã hóa một thông điệp $m \in F_p^*$, chúng ta tính các đại lượng:

+) Tạo ra một cách ngẫu nhiên khóa k

+) Đặt $c_1 = g^k (\bmod p)$

+) Đặt $c_2 = m.h^k (\bmod p)$

Bản mã có hai thành phần $c = (c_1, c_2)$

Bước 4: Giải mã

Để giải mã một bản mã $c = (c_1, c_2)$, chúng ta cần tính toán:

$$\frac{c_2}{c_1^x} = \frac{m.h^k}{g^{xk}} = \frac{m.g^{xk}}{g^{xk}} = m$$

1. **Phương án gốc:**

Giả sử p là số nguyên và g là căn nguyên thủy của p. Ta tiến hành các bước 2, 3 và 4 của Thuật toán trên.

Ví dụ. Cho p = 809 và g = 3 (có thể kiểm tra g là căn nguyên thủy của p, tuy không đơn giản).

A sinh cặp khóa công khai:

Khóa riêng $x_{A\,=}$ 57,

Khóa công khai của A: $h = g^{xA} = 3^{57} \bmod 809 = 31$

B mã thông điệp m = 270 gửi cho A:

- Sinh số ngẫu nhiên k = 150
- Tính $c_1 = 3^{150} \bmod 809 = 665$
- Tính $c_2 = 270.\ 31^{150} \bmod 809 = 270.622 \bmod 809 = 47$
- B gửi cho A: c = (665, 477)

A giải mã:

$c_1^{xA} = 665^{57} \bmod 809 = 622$

$622^{-1} \bmod 809 = 199$

$m = c_2/\ c_1^{xA} = 477.199 \bmod 809 = 270$

2. **Phương án cải tiến:**

Lưu ý: Vì việc tìm số p là số nguyên tố lớn với a là căn nguyên thủy của p là việc không đơn giản. Nên thay vì như trên người ta tìm nhóm nhân G_q bậc số nguyên tố q và phần tử sinh g được lựa chọn một cách dễ dàng và áp dụng cho thuật toán Elgamal, Diffie – Hellman, DSA, cùng nhiều thuật toán khác.

Tạo nhóm xiclic G_q bậc số nguyên tố q với các phần tử sinh g chọn tùy ý trong phạm vi thích hợp.

Cặp số nguyên tố p, q: thỏa mãn tính chất p-1 chia hết cho q. Khi đó lấy một số h tùy ý trong Z_p. (p cỡ 1024 bit, q cỡ 160 bit)

Khi đó $g = h^{p-1/q} \bmod p$ sẽ là phần tử sinh nhóm nhân xiclic G_q.

Thực vậy $g^q \bmod p = h^{p-1} \bmod p = 1$. Và q là số nguyên tố, nên bậc của g là q và g là phần tử sinh của nhóm G_q gồm các lũy thừa của g theo mod p.

Ví dụ. Giả sử ta chọn p = 809, q = 101 và h = 3. Ta có $g = h^{(809-1/101)} \bmod 809 = 89$. Khi đó g = 89 là phần tử sinh của nhóm Aben bậc 101: $g^{101} \bmod 809 = 89^{101} \bmod 809 = 1$.

Như vậy ta có g là phần tử sinh của nhóm $<g> = \{1=g^0, g, g^2, \ldots, g^{100}\}$ lấy theo mod 809.

g và p, q chia sẻ.

Mã Elgamal: người A chọn khóa riêng $x_A = 31$, tính khóa công khai

$y_A = g^{xA} \bmod p = 89^{31} \bmod 809 = 613$

B mã M = 723 thuộc F_p^*, lấy k ngẫu nhiên, chẳng hạn k = 53

B tính: $g^k = 89^{53} \bmod 809 = 745$

$m.y_A^k = 723.\ 613^{53} \bmod 809 = 723.578 \bmod 809 = 450$

B gửi (745, 450) cho A

A giải mã, tính $m = 450 / 745^{31} \bmod 809 = 450 / 578 \bmod 809 = 450*7 \bmod 809 = 723$

Bài tập.

a. Cho p = 43, g = 3 (3 là căn nguyên thủy của 43). Người A chọn $x_A = 25$. Tính khóa công khai h của A? Người B lấy số ngẫu nhiên k = 16, tính mã Elgamal c gửi cho A. Tính bản mã c. Và nêu tính toán của A giải mã.

b. Cho p = 47, q = 2, chọn ngẫu nhiên r = 10, tính $g = r^{(p-1)/q} \bmod p$. Xét trong nhóm G_q.

Người A chọn $x_A = 13$. Tính khóa công khai h của A? Người B lấy số ngẫu nhiên k = 12, tính mã Elgamal c gửi cho A. Tính bản mã c. Và nêu tính toán của A giải mã.

c. Cho p = 809, g = 3 (3 là căn nguyên thủy của 809). Người A chọn $x_A = 55$. Tính khóa công khai h của A? Người B lấy số ngẫu nhiên k = 31, tính mã Elgamal c gửi cho A. Tính bản mã c. Và nêu tính toán của A giải mã.

d. Cho p = 607, q = 101, chọn ngẫu nhiên r = 34, tính $g = r^{(p-1)/q} \bmod p$. Xét trong nhóm G_q. Người A chọn $x_A = 29$. Tính khóa công khai h của A? Người B lấy số ngẫu nhiên k = 24, tính mã Elgamal c gửi cho A. Tính bản mã c. Và nêu tính toán của A giải mã.

Trao đổi khóa Diifie-Hellman cũng dung nhóm G_q được sinh như trên.

Bài tập.

1. Cho p = 607, q = 101, chọn ngẫu nhiên r = 5, tính $g = r^{(p-1)/q} \bmod p$. Xét trong nhóm G_q.

Người sử dụng A chọn khóa riêng $x_A = 53$.

Người sử dụng B chọn khóa riêng $x_B = 31$.

Nêu tính toán khóa chung K_{AB} của A.

Nêu tính toán khóa chung K_{AB} của B.

2. Cho p = 809, q = 101, chọn ngẫu nhiên r = 18, tính $g = r^{(p-1)/q} \bmod p$. Xét trong nhóm G_q.

Người sử dụng A chọn khóa riêng $x_A = 49$.

Người sử dụng B chọn khóa riêng $x_B = 87$.

Nêu tính toán khóa chung K_{AB} của A.

Nêu tính toán khóa chung K_{AB} của B.

BÀI 5: XÁC THỰC THÔNG ĐIỆP VÀ CHỮ KÝ ĐIỆN TỬ

1. Hàm băm SHA:

Nghịch lý ngày sinh nhật:

Một kết quả của lý thuyết xác suất cơ bản mà chúng ta cần để thấy sự va chạm của hàm băm là không nhỏ là nghịch lý ngày sinh nhật.

Giả sử một túi có m quả bóng, tất cả có màu khác nhau. Ta rút một quả ra khỏi túi mỗi lần và ghi lại màu của quả bóng đó, rồi lại bỏ lại và lại rút ra.

Nếu ta định nghĩa

$$m^{(n)} = m.(m - 1)(m - 2) \ldots (m - n + 1)$$

thì, xác suất sau khi n quả bóng được lấy ra khỏi túi (có bỏ lại) mà nhận được ít nhất có một quả bóng được rút hai lần, tức là màu trùng với lần trước đó là

$$1 - m^{(n)} / m^{n}$$

Nếu m trở nên ngày một lớn hơn, thì số bóng dự kiến cần phải rút ra trước khi có thể có lần trùng màu đầu tiên là $\sqrt{\frac{\pi m}{2}}$

Để nhận thấy tại sao người ta gọi là nghịch lý ngày sinh nhật, ta xét xác suất để hai người trong một lớp có cùng ngày sinh nhật. Ban đầu nhiều người nghĩ là xác suất này rất nhỏ.

Có thể tính được số người trong lớp ít nhất là bao nhiêu, để xác suất có hai người trong lớp trùng ngày sinh nhật lớn hơn ½:

$$1 - 365^{(23)} / 365^{23} \approx 0.507$$

Thực tế xác suất này tăng khá nhanh, khi số người trong lớp là 30, nó xấp xỉ bằng 0.706, và trong phòng có 100 người, thì xác suất đó là trên 0.9999996.

Nếu tính gần đúng ta có:

$$\sqrt{\frac{\pi\, 365}{2}} \approx 23.4$$

Đây là số học sinh trung bình trong lớp cần phải có để sau đó từ học sinh thứ 24 trở đi xác suất trùng ngày sinh với các học sinh trước đó lớn hơn ½.

2. Chữ ký điện tử DSA:

Bài tập:

- Chọn p = 23, q = 11, h = 6

  chọn $g = h^{(p-1)/q} \pmod p$

  ở đó $h < p-1$; $h^{(p-1)/q} \pmod p > 1$
- $g = h^2 \bmod 23 = 13$
- Chọn x = 8, $y = 13^8 \bmod 23 = 2$

Tạo chữ ký điện tử

- k = 9, H(M) = 10
- $r = (g^k \pmod p) \pmod q$

  $r = (13^9 \bmod 23) \bmod 11 = (3 \bmod 23) \bmod 11 = 3$
- $s = (k^{-1}(H(M) + x.r)) \pmod q$

  $s = (9^{-1}.(10 + 8.3)) \bmod 11 = (5.1) \bmod 11 = 5$

- Chữ ký điện tử (r,s) = (3,5)

Kiểm tra chữ ký điện tử

$w = s^{-1} \pmod q$

$u1 = (H(M).w) \pmod q$

$u2 = (r.w) \pmod q$

$v = (g^{u1}.y^{u2} \pmod p) \pmod q$

- $w = 5^{-1} \bmod 11 = 9$
- $u_1 = 10.9 \bmod 11 = 2$
- $u_2 = 3.9 \bmod 11 = 5$
- $v = (13^2.2^5 \bmod 23) \bmod 11 = 3 \bmod 11 = 3$
- v = r, chữ ký điện tử đúng

Bài tập

a. Cho p = 47 và q = 23 và h = 7. Tính g. Bạn chọn khoá riêng x = 13, rồi tính khoá công khai y. Bạn gửi bức thư có bản băm H(M) = 11 và chọn một số ngẫu nhiên k = 5, rồi ký. Sinh chữ ký. Nêu cách người nhận kiểm tra chữ ký.

b. Cho p = 139 và q = 23 và h = 12. Tính g. Bạn chọn khoá riêng x = 14, rồi tính khoá công khai y. Bạn gửi bức thư có bản băm H(M) = 18 và chọn một số ngẫu nhiên k = 8, rồi ký. Sinh chữ ký. Nêu cách người nhận kiểm tra chữ ký.

c. Cho p = 607 và q = 101 và h = 11. Tính g. Bạn chọn khoá riêng x = 19, rồi tính khoá công khai y. Bạn gửi bức thư có bản băm H(M) = 14 và chọn một số ngẫu nhiên k = 8, rồi ký. Sinh chữ ký. Nêu cách người nhận kiểm tra chữ ký.

d. Cho p = 809 và q = 101 và h = 20. Tính g. Bạn chọn khoá riêng x = 16, rồi tính khoá công khai y. Bạn gửi bức thư có bản băm H(M) = 31 và chọn một số ngẫu nhiên k = 24, rồi ký. Sinh chữ ký. Nêu cách người nhận kiểm tra chữ ký.

3. Thuật toán SHA-1

Mô tả thuật toán. Đầu vào của thuật toán là một thông điệp có chiều dài bất kỳ nhỏ hơn 2^{64} bit, SHA-1 cho ra kết quả là một thông điệp rút gọn có độ dài là 160 bit. Đầu vào được xử lý theo các khối 512 bit. Thuật toán SHA1 được thực hiện theo các bước sau:

- Bổ sung bộ đệm bít. Thông điệp được bổ sung sao cho độ dài của nó đồng dư với 448 mod 512.
- Bổ sung độ dài. Thêm khối 64 bit vào cuối thông điệp, nó biểu diễn độ dài thực của thông điệp.
- Khởi tạo bộ đệm. 160 bit bộ đệm được sử dụng để giữ giá trị trung gian và cuối cùng của bản băm, gồm năm thanh ghi 32 bit: A, B, C, D, E.
- Xử lý các khối dữ liệu 512 bit hay 16 từ 32 bit gồm bốn vòng, mỗi vòng 20 bước. Bốn vòng sử dụng bốn hàm logic f_1, f_2, f_3, f_4.

Mở rộng thông điệp

Thông điệp M được mở rộng trước khi thực hiện băm. Mục đích của việc mở rộng này là để đảm bảo cho thông điệp mở rộng có độ dài là bội số của 512. Thông điệp M được mở rộng trước khi thực hiện băm. Mục đích của việc mở rộng này là để đảm bảo cho thông điệp mở rộng có độ dài là bội số của 512.

Thông điệp M được mở rộng trước khi thực hiện băm. Mục đích của việc mở rộng này là để đảm bảo cho thông điệp mở rộng có độ dài là bội số của 512.

Giả sử độ dài của thông điệp là L bit. Thêm bit 1 vào cuối thông điệp, theo sau là k bit 0 (k là số dương không âm nhỏ nhất sao cho L + 1 + k = 448 (mod 512)) . Sau đó thêm khối 64 bit là biểu diễn nhị phân của L.

Bốn hàm logic với 20 bước trong mỗi vòng, f(t;B,C,D) được định nghĩa như sau:

$$f(t;B,C,D) = (B \text{ AND } C) \text{ OR } ((\text{NOT } B) \text{ AND } D) \qquad (0 \le t \le 19)$$

$$f(t;B,C,D) = B \text{ XOR } C \text{ XOR } D \qquad (20 \le t \le 39)$$

$$f(t;B,C,D) = (B \text{ AND } C) \text{ OR } (B \text{ AND } D) \text{ OR } (C \text{ AND } D) \qquad (40 \le t \le 59)$$

$$f(t;B,C,D) = B \text{ XOR } C \text{ XOR } D \qquad (60 \le t \le 79).$$

Phân tích thông điệp mở rộng:

Sau khi thông điệp đã được mở rộng, thông điệp mở rộng được phân tích thành N khối 512 bit M(1), M(2),…, M(N). Trong đó 512 bit của khối dữ liệu đầu vào có thể được thể hiện bằng 16 từ 32 bit,

Khởi tạo giá trị băm:

Giá trị băm là một chuỗi bit có kích thước bằng kích thước của thông điệp băm gồm các từ ghép lại. Trong đó $H_j^{(i)}$ là từ j trong giá trị băm ở lần lặp i với $0 \le i \le N$ (số block có được sau khi chia văn bản được đệm) và $0 \le j \le$ (số từ trong giá trị băm - 1). Trước khi thực hiện giá trị băm, với mỗi thuật toán băm an toàn, giá trị băm ban đầu H(0) phải được thiết lập. Kích thước và số lượng từ trong H(0) tùy thuộc vào kích thước thông điệp băm rút gọn.

SHA-1 sử dụng dãy các hằng số K(0),…,K(79) có giá trị như sau:

K(t) = 5A827999 (0 <= t <= 19)

K(t) = 6ED9EBA1 (20 <= t <= 39)

K(t) = 8F1BBCDC (40 <= t <= 59)

K(t) = CA62C1D6 (60 <= t <= 79).

Thuật toán của bước tính giá trị băm SHA-1

SHA-1 được sử dụng để băm thông điệp M có độ dài L bit thoả mãn điều kiện $0 \le L \le 2^{64}$. Thuật toán sử dụng:

- Một bảng phân bố thông điệp gồm 80 từ 32 bit
- 5 biến 32 bit
- Một giá trị băm gồm 5 từ 32 bit

Kết quả của SHA-1 là một thông điệp băm rút gọn có độ dài 160 bit. Các từ của bảng phân bố thông điệp được ký hiệu W(0),W(1),…,W(79). 5 biến được ký hiệu là A, B, C, D, E. Các từ của giá trị băm ký hiệu $H_0^{(i)}$,$H_1^{(i)}$, $H_2^{(i)}$, $H_3^{(i)}$,$H_4^{(i)}$. H(0) giữ giá trị băm ban đầu và được thay thế bằng các giá trị băm thành công. H(i) sau mỗi khối thông điệp được xử lý và kết thúc bằng giá trị băm cuối cùng H(N).

Tính toán thông điệp băm

Định nghĩa: $S^n(X)$ = (X << n) or (X >> 32-n).

X << n có nghĩa là loại bỏ từ trái sang phải n bit và thêm vào kết quả n số 0 vào bên phải. X >> n có nghĩa là loại bỏ từ phải qua trái n bit và thêm vào kết quả n số 0 vào bên trái.

Khởi tạo các giá trị của H:

H0 = 67452301 ; H1 = EFCDAB89

H2 = 98BADCFE ; H3 = 10325476

H4 = C3D2E1F0.

Chia khối 512 bit M(i) thành 16 từ W(0), W(1),…,W(15)

For t = 16 to 79

W(t) = S^1(W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)).

Đặt A = H0 , B = H1, C = H2, D = H3, E = H4

For t = 0 to 79 do

TEMP = S^5(A) + f(t;B,C,D) + E + W(t) + K(t);

E = D; D = C; C = S^{30}(B); B = A; A = TEMP;

Đặt H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4+ E.

Sau khi tính toán được hết M(n), thông điệp băm rút gọn là một chuỗi 160 bit là biểu diễn của 5 từ: H0 H1 H2 H3 H4.

Câu hỏi.

Đối với một hàm băm

a. Độ dài thông điệp có hạn chế không. Kích thước bản băm có cố định không?
b. Thế nào là va chạm yếu, va chạm mạnh.
c. Thế nào là một hàm băm tốt.

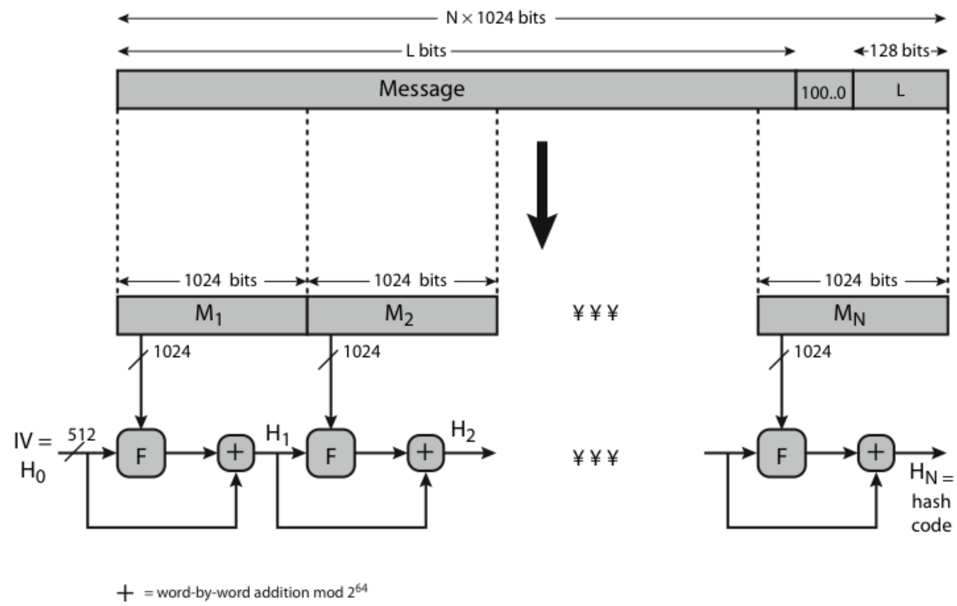
Trong SHA1:

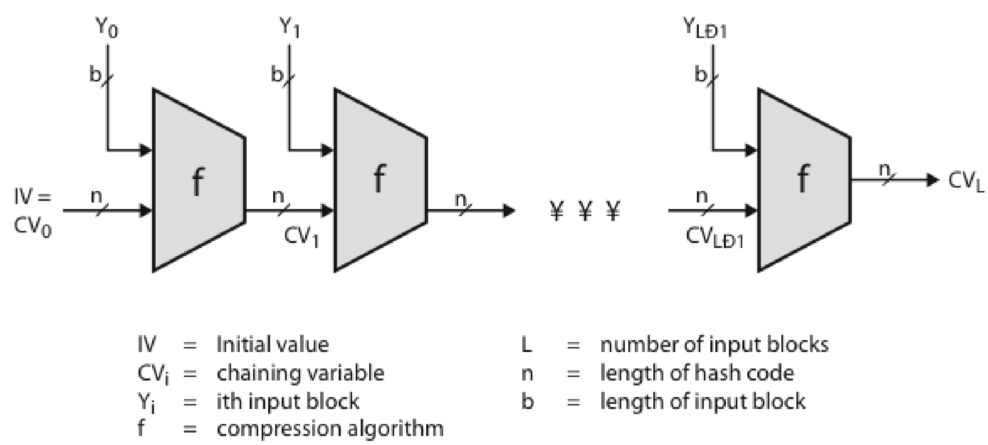
d. Dữ liệu được mở rộng và chia thành các khối như thế nào? Một từ có độ dài bao nhiêu bit? Mỗi khối có bao nhiêu từ? Giả sử có N khối ký hiệu W_i : 0 < = i <= N-1, ký hiệu $W_i(0)$, …,$W_i(15)$.
e. Bảng phân bố thông điệp s ử d ụng bao nhi êu t ừ: W(0), …, W(15), … W(79)
f. 80 từ hằng số K(0), …, K(79) có tính chất gì?
g. Bản băm cuối SHA1(M) có độ dài bao nhiêu?
h. H(0) = H0, H1, H2, H3, H4 là các dãy bit có tính chất gì?
i. 5 biến từ A, B, C, D, E được khởi tạo như thế nào: A = H0, B = H1, C = H2, D = H3, E = H4.
j. Số vòng xử lý liên quan thế nào với số khối. Giá trị bản băm của mỗi vòng ký hiệu $H_0^{(i)}$,$H_1^{(i)}$, $H_2^{(i)}$, $H_3^{(i)}$,$H_4^{(i)}$
k. Ban đầu mỗi vòng một khối dữ liệu 512 chia thành 16 từ: W(0), …, W(15). Các từ W(16), …, W(79) được xác định như thế nào?
l. Hàm $S^n(X)$ được định nghĩa như thế nào?
m. Qua mỗi vòng các biến từ A, B, C, D, E và các từ H0, H1, H2, H3, H4 được cập nhật như thế nào?
n. Bản băm Hash (M) được xác định như thế nào?

Chuẩn Hash an toàn nâng cao

Viện chuẩn công nghệ quốc gia NIST xuất bản bản sửa FIPS 180-2 vào năm 2002, đề nghị bổ sung ba phiên bản mới của SHA: SHA-256, SHA-384, SHA-512. Các phiên bản trên được thiết kế tương thích với việc tăng độ an toàn được cung cấp bởi chuẩn mã nâng cao AES. Về cấu trúc và chi tiết giống SHA-1, suy ra việc phân tích cũng tương tự, nhưng mức độ an toàn cao hơn nhiều so với SHA-1.

Tổng quan SHA 512



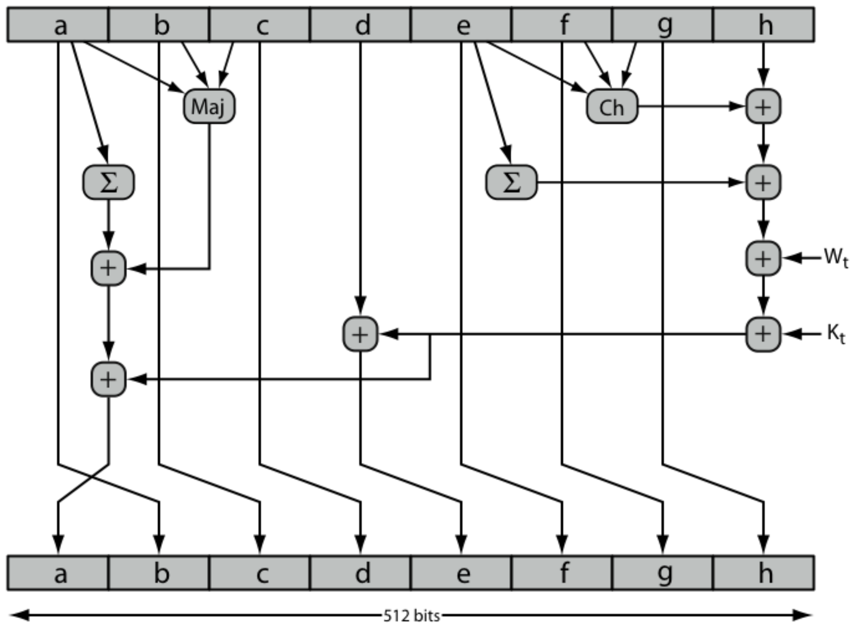


Hàm nén SHA-512

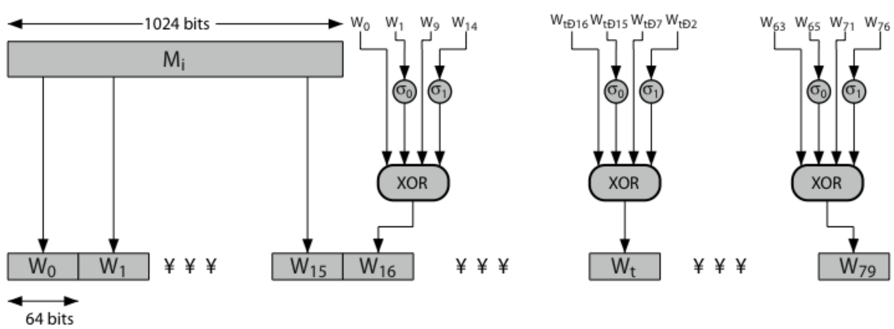
SHA-512 là trọng tâm của thuật toán. Ở đây xử lý mẩu tin với các khối 1024 bit và bao gồm 80 vòng:

- Cập nhật bộ đệm 512 bit;
- Sử dụng giá trị Wt 64 bit được lấy ra từ block hiện tại của mẩu tin;
- Và hằng số quay vòng dựa trên căn bậc ba của 80 số nguyên tố đầu tiên.

Hàm quay vòng của SHA-512



a b c d e f g h
Maj
Ch
Σ
Σ
Wt
Kt
a b c d e f g h
512 bits



1024 bits
Mi
W0 W1 W9 W14
WtÐ16 WtÐ15 WtÐ7 WtÐ2
W63 W65 W71 W76
σ0 σ1
XOR
W0 W1 ¥ ¥ ¥ W15 W16 ¥ ¥ ¥ Wt ¥ ¥ ¥ W79
64 bits