ÔN TẬP AN TOÀN VÀ BẢO MẬT HỆ THỐNG THÔNG TIN

I – THUẬT TOÁN LŨY THỪA NHANH

***Ví dụ*:** Tính $876^{611} \bmod 899$

Giải

Ta có $876^{611} = 876^{512}.876^{64}.876^{32}.876^{2}.876^{1}$

$876 \bmod 899 = 876$

$876^2 \bmod 899 = (876.876) \bmod 899 = \left[(876 \bmod 899).(876 \bmod 899)\right] \bmod 899$

$= (876 \bmod 899)^2 \bmod 899 = 876^2 \bmod 899 = 529$

$876^4 \bmod 899 = \left(876^2 \bmod 899\right)^2 \bmod 899 = 529^2 \bmod 899 = 252$

$876^8 \bmod 899 = \left(876^4 \bmod 899\right)^2 \bmod 899 = 252^2 \bmod 899 = 574$

$876^{16} \bmod 899 = \left(876^8 \bmod 899\right)^2 \bmod 899 = 574^2 \bmod 899 = 442$

$876^{32} \bmod 899 = \left(876^{16} \bmod 899\right)^2 \bmod 899 = 442^2 \bmod 899 = 281$

$876^{64} \bmod 899 = \left(876^{32} \bmod 899\right)^2 \bmod 899 = 281^2 \bmod 899 = 748$

$876^{128} \bmod 899 = \left(876^{64} \bmod 899\right)^2 \bmod 899 = 748^2 \bmod 899 = 326$

$876^{256} \bmod 899 = \left(876^{128} \bmod 899\right)^2 \bmod 899 = 326^2 \bmod 899 = 194$

$876^{512} \bmod 899 = \left(876^{256} \bmod 899\right)^2 \bmod 899 = 194^2 \bmod 899 = 777$

$\Rightarrow 876^{611} \bmod 899 = \left(876^{512}.876^{64}.876^{32}.876^{2}.876^{1}\right) \bmod 899$

$= \left[\left(876^{512} \bmod 899\right).\left(876^{64} \bmod 899\right).\left(876^{32} \bmod 899\right).\left(876^{2} \bmod 899\right).(876 \bmod 899)\right] \bmod 899$

$= (777.748.281.529.876) \bmod 899$

$= \left\{\left[(777.748) \bmod 899\right].\left[(281.529.876) \bmod 899\right]\right\} \bmod 899$

$= (442.869) \bmod 899 = 225.$

II – HÀM PHI Ơ-LE

Với mỗi số nguyên *N*, giá trị của hàm Phi Ơ-le của *N* là tổng số tất cả các số nguyên thuộc Z_N và nguyên tố cùng nhau với *N*.

Nếu *P* là một số nguyên tố thì $\phi(P) = P - 1$

Nếu $N = PQ$ với P và Q là hai số nguyên tố cùng nhau thì $\phi(N) = (P-1)(Q-1)$

Trong trường hợp tổng quát nếu dạng phân tích ra thừa số nguyên tố của N là

$$N = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$$

trong đó p_i là các số nguyên tố, còn α_i là các số nguyên dương thì giá trị của hàm Phi Ơ-le được tính như sau:

$$\phi(N) = (p_1 - 1) p_1^{\alpha_k - 1} (p_2 - 1) p_2^{\alpha_k - 1} ... (p_k - 1) p_k^{\alpha_k - 1}$$

***Ví dụ*:** Tính $\phi(26)$.

Giải

Ta có $26 = 13.2 \Rightarrow \phi(26) = (13-1)(2-1) = 12.$

III – TÌM PHẦN TỬ NGHỊCH ĐẢO

$a \in Z_N$ và tồn tại $b \in Z_N$ sao cho $ab = (ab) \bmod N = 1$. Khi đó b được gọi là phần tử nghịch đảo của a trên Z_N và ký hiệu là $a^{-1} = b$.

Giải thuật tìm phần tử nghịch đảo trên Z_N

```
ReverseModulo(b, a)
{
    int y0 = 0, y1 = 1, a0 = a;
    while (b > 0)
    {
        int r = a % b;
        if (r == 0) break;
        int q = a / b;
        y = y0 – y1 * q;
        a = b;
        b = r;
        y0 = y1;
        y1 = y;
    }
    while (y < 0) y += a0;
    return y;
}
```

***Ví dụ*:** Tìm phần tử nghịch đảo của 30 theo Module 101.

a	b	r	q	y_0	y_1	y
101	30	11	3	0	1	–3
30	11	8	2	1	–3	7
11	8	3	1	–3	7	–10
8	3	2	2	7	–10	27
3	2	1	1	–10	27	–37
2	1	0				

Vậy phần tử nghịch đảo của 30 theo Module 101 là $-37+101=64.$

IV – PHƯƠNG TRÌNH ĐỒNG DƯ BẬC NHẤT MỘT ẨN

Dạng: $ax=b \bmod N$ trong đó $a,b\in Z_N$ là các hệ số, còn *x* là ẩn số. (1)

Giả sử $g=\text{GCD}(a,N)$ và *b* chia hết cho *g* thì phương trình (1) sẽ có *g* nghiệm có dạng:

$$x=\left(\frac{b}{g}x_0+\frac{N}{g}t\right)\bmod N$$

trong đó $t = 0, 1, 2, \ldots, g-1$ và x_0 là nghiệm của phương trình: $\frac{a}{g}x=1 \bmod \frac{N}{g}$.

***Ví dụ*:** Giải các phương trình sau

a) $5x=2 \bmod 7$

b) $5x=4 \bmod 11$

Giải

a) $5x=2 \bmod 7$ (1)

Ta có $g=\text{GCD}(5,7)=1$ nên phương trình (1) có một nghiệm duy nhất.

Nghiệm của phương trình có dạng $x=(2x_0+7t) \bmod 7$ với x_0 là nghiệm của phương trình $5x_0=1 \bmod 7 \Leftrightarrow x_0=5^{-1} \bmod 7=3.$

Vậy phương trình có nghiệm $x=(2.3+7.0) \bmod 7=6.$

b) $5x=4 \bmod 11$ (2)

Ta có $g=\text{GCD}(5,11)=1$ nên phương trình (2) có một nghiệm duy nhất

Nghiệm của phương trình có dạng $x = (4x_0 + 11t) \bmod 11$ với x_0 là nghiệm của phương trình $5x_0 = 1 \bmod 11 \Leftrightarrow x_0 = 5^{-1} \bmod 11 = 9.$

Vậy phương trình có nghiệm $x = (4.9 + 11.0) \bmod 11 = 3.$

V – HỆ MÃ CAESAR

Hệ mã Caesar là một hệ mã thay thế đơn âm làm việc trên bảng chữ cái tiếng Anh. Để mã hóa, người ta đánh số các chữ cái từ 0 đến $N - 1$. Không gian khóa $K = Z_N$. Với mỗi khóa $k \in K$ hàm mã hóa và giải mã một ký tự có số thứ tự là I sẽ được thực hiện như sau:

Mã hóa: $E_K(i) = (i + k) \bmod N$

Giải mã: $D_K(i) = (i - k) \bmod N$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

VI – HỆ MÃ AFFINE

$K = \{(a,b) : a,b \in Z_N, \text{GCD}(a,N) = 1\}$

Mã hóa: $E_K(x) = (ax + b) \bmod N$

Giải mã: Tính a^{-1} và tiến hành giải mã $D_K(y) = a^{-1}(y - b) \bmod N$

Số khóa có thể sử dụng cho hệ mã Affine: $|K| = \phi(N)N$

***Ví dụ 1*:** Mã hóa xâu "ADVENGER" với không gian khóa của bảng mã là (27, 7).

Giải

Ta có: A: $E_K(0) = (27.0 + 7) \bmod 26 = 7$ nên A → H

D: $E_K(3) = (27.3 + 7) \bmod 26 = 10$ nên D → K

V: $E_K(21) = (27.21 + 7) \bmod 26 = 2$ nên V → C

E: $E_K(4) = (27.4 + 7) \bmod 26 = 11$ nên E → L

N: $E_K(13) = (27.13 + 7) \bmod 26 = 20$ nên N → U

G: $E_K(6) = (27.6 + 7) \bmod 26 = 13$ nên G → N

R: $E_K(17) = (27.17 + 7) \bmod 26 = 24$ nên R → Y

Vậy mã hóa xâu "ADVENGER" ta được "HKCLUNLY"

***Ví dụ 2*:** Cho hệ mã Affine được cài đặt trên Z_{99}. Khi đó khóa là các cặp (a,b) trong đó $a,b \in Z_{99}$ với $\text{GCD}(a,99)=1$. Hàm mã hóa $E_K(x)=(ax+b)\bmod 99$ và hàm giải mã $D_K(x)=a^{-1}(x-b)\bmod 99$.

a) Hãy xác định số khóa có thể được sử dụng cho hệ mã này.

b) Nếu như khóa giải mã là $K^{-1}=(16,7)$, hãy thực hiện mã hóa xâu *m* = "DANGER".

Giải

a) Số khóa có thể được sử dụng cho hệ mã này là:

$$|K|=\phi(N)N=\phi(99)99=(9-1)(11-1)99=7920 \text{ (khóa)}$$

b) Khóa giải mã là $K^{-1}=(16,7)\Rightarrow a^{-1}=16,\ b=7$.

$\Rightarrow a=\left(a^{-1}\right)^{-1}\bmod 99=16^{-1}\bmod 99=31$

Ta có D: $E_K(3)=(31.3+7)\bmod 26=22$ nên D → W

A: $E_K(0)=(31.0+7)\bmod 26=7$ nên A → H

N: $E_K(13)=(31.13+7)\bmod 26=20$ nên N → U

G: $E_K(6)=(31.6+7)\bmod 26=11$ nên G → L

E: $E_K(4)=(31.4+7)\bmod 26=1$ nên E → B

R: $E_K(17)=(31.17+7)\bmod 26=14$ nên R → O

Mã hóa xâu "DANGER" ta được xâu "WHULBO"

***Ví dụ 3*:** Giả sử hệ mã Affine được cài đặt trên Z_{126}.

a) Hãy xác định số khóa có thể có của hệ mã.

b) Giả sử khóa mã hóa là (23, 7), hãy xác định khóa giải mã.

Giải

a) Số khóa có thể có của hệ mã:

$$|K|=\phi(N)N=(2-1).(3-1).3.(7-1).126=4536 \text{ (khóa)}$$

b) Khóa mã hóa là (23, 7) $\Rightarrow a=23,\ b=7$.

$a^{-1}=a^{-1}\bmod N=23^{-1}\bmod 126=107$.

Vậy khóa giải mã là (107, 7).

VII – HỆ MÃ HILL

Tồn tại ma trận K kích thước $M \times M$ gồm các phần tử là các số nguyên thuộc Z_N với N là phần tử thuộc bảng chữ cái. Điều kiện để ma trận K có thể sử dụng làm khóa của hệ mã là tồn tại ma trận nghịch đảo của ma trận K trên Z_N

Mã hóa: $C = P \times K$

Giải mã: $P = C \times K^{-1}$

Với $K = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$ và $\det(K) = (k_{11}k_{22} - k_{21}k_{12}) \bmod N$ là một phần tử nghịch đảo trên Z_N thì khóa giải mã sẽ là $K^{-1} = \det^{-1}(K) \begin{bmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{bmatrix}$.

***Ví dụ 1*:** Cho hệ mã Hill có $M = 2$.

a) Ma trận $A = \begin{bmatrix} 5 & 3 \\ 13 & 17 \end{bmatrix}$ có thể được sử dụng làm khóa cho hệ mã trên không? Hãy giải thích.

b) Cho $A = \begin{bmatrix} 12 & 5 \\ 3 & 7 \end{bmatrix}$, hãy thực hiện mã hóa và giải mã với xâu S = "HARD".

Giải

a) Điều kiện để ma trận A có thể sử dụng làm khóa của hệ mã là tồn tại ma trận nghịch đảo của ma trận A trên Z_{26}, tức là tồn tại $\det^{-1}(A)$, $\det(A)$ và 26 có ước chung lớn nhất là 1.

Ta có $\det(A) = (5.17 - 13.3) \bmod 26 = 20,$ mà $\text{GCD}(20, 26) = 2$ nên ma trận A không thể được sử dụng làm khóa cho hệ mã Affne.

b) Để mã hóa, ta chia xâu bản rõ thành hai ma trận hàng hai chiều "HA" $\begin{bmatrix} 7 & 0 \end{bmatrix}$ và "RD" $\begin{bmatrix} 17 & 3 \end{bmatrix}$ và tiến hành mã hóa lần lượt.

Với $P_1 = \begin{bmatrix} 7 & 0 \end{bmatrix}$ ta có:

$$C_1 = P_1 \times K = \begin{bmatrix} 7 & 0 \end{bmatrix} \times \begin{bmatrix} 12 & 5 \\ 3 & 7 \end{bmatrix} = \begin{bmatrix} (7.12 + 0.3) \bmod 26 & (7.5 + 0.7) \bmod 26 \end{bmatrix} = \begin{bmatrix} 6 & 9 \end{bmatrix}$$

$\Rightarrow$ "GJ"

Với $P_2 = [17 \quad 3]$ ta có:

$$C_2 = [17 \quad 3] \times \begin{bmatrix} 12 & 5 \\ 3 & 7 \end{bmatrix} = [(17.12 + 3.3) \bmod 26 \quad (17.5 + 3.7) \bmod 26] = [5 \quad 2]$$

$\Rightarrow$ "FC"

Vậy bãn mã thu được là "GJFC".

Để giải mã, ta tìm K^{-1}. Ta có $\det(K) = (12.7 - 3.5) \bmod 26 = 17.$

$$\det^{-1}(K) = \det^{-1}(K) \bmod 26 = 17^{-1} \bmod 26 = 23$$

$$\Rightarrow K^{-1} = \det^{-1}(K) \begin{bmatrix} 7 & -5 \\ -3 & 12 \end{bmatrix} = 23 \begin{bmatrix} 7 & -5 \\ -3 & 12 \end{bmatrix} = \begin{bmatrix} 161 & -115 \\ -69 & 276 \end{bmatrix}$$

Quá trình giải mã cũng tương tự với quá trình mã hóa.

Giải mã $C_1 = [G \quad J]$ ta được:

$$P_1 = C_1 \times K^{-1} = [6 \quad 9] \times \begin{bmatrix} 161 & -115 \\ -69 & 276 \end{bmatrix}$$

$$= [(6.161 - 69.9) \bmod 26 \quad (-115.6 + 276.9) \bmod 26] = [7 \quad 0] = [H \quad A]$$

Giải mã $C_2 = [F \quad C]$ ta được:

$$P_2 = C_2 \times K^{-1} = [5 \quad 2] \times \begin{bmatrix} 161 & -115 \\ -69 & 276 \end{bmatrix} = [17 \quad 3] = [R \quad D]$$

Vậy giải mã bản mã thu được, ta có "HARD"

***Ví dụ 2*:** Cho hệ mã Hill có $M = 2$

a) Ma trận $A = \begin{bmatrix} 5 & 3 \\ 11 & a \end{bmatrix}$ được sử dụng làm khóa cho hệ mã trên. Hãy tìm tất cả các khóa có thể sử dụng của hệ mã trên.

b) Giả sử người ta sử dụng hệ mã trên để mã hóa bản rõ P = "EASY" và thu được bản mã là "UMQA". Hãy thực hiện giải mã với bản mã là C = "MCDZUZ" và đưa ra bản rõ.

Giải

a) Điều kiện để ma trận *A* có thể sử dụng làm khóa của hệ mã là tồn tại ma trận nghịch đảo của ma trận *A* trên Z_{26}, tức là ta có

$$\det(A) = (5a - 33) \bmod 26$$

Tức là $\text{GCD}(5a - 33, 26) = 1$

$$\Leftrightarrow 5a - 33 = \{1,3,5,7,9,11,15,17,19,21,23,25\}$$

$$\Leftrightarrow a = \{8,10\}$$

b) Mã hóa bản rõ "EASY" thi được "UMQA" với *M* = 2 thì ta có $P_1 = [\text{E} \quad \text{A}] = [4 \quad 0]$ thu được $C_1 = [\text{U} \quad \text{M}] = [20 \quad 12]$, và $P_2 = [\text{S} \quad \text{Y}] = [18 \quad 24]$ thu được $C_2 = [\text{Q} \quad \text{A}] = [16 \quad 0]$.

$$C_1 = P_1 \times K \Leftrightarrow [20 \quad 12] = [4 \quad 0] \times \begin{bmatrix} 5 & 3 \\ 11 & a \end{bmatrix} = [20 \quad 12] \text{ (Luôn thỏa mãn với mọi } a\text{)}$$

$$C_2 = P_2 \times K \Leftrightarrow [16 \quad 0] = [18 \quad 24] \times \begin{bmatrix} 5 & 3 \\ 11 & a \end{bmatrix} = [16 \quad (54 + 24a) \bmod 26]$$

$$\Leftrightarrow (54 + 24a) \bmod 26 = 0 \Leftrightarrow [54 \bmod 26 + (24a) \bmod 26] \bmod 26 = 0$$

$$\Leftrightarrow [2 + (24a) \bmod 26] \bmod 26 = 0 \Leftrightarrow (24a) \bmod 26 = 24 \Leftrightarrow a = 1$$

$$\Rightarrow \text{Khóa } K = \begin{bmatrix} 5 & 3 \\ 11 & 1 \end{bmatrix}$$

VIII – HỆ MÃ ĐỔI CHỖ

Một hệ mã hóa đổi chỗ là hệ mã hóa trong đó các ký tự của bản rõ vẫn được giữ nguyên, nhưng thứ tự của chúng được đổi chỗ cho nhau.

Các kỹ thuật:

- ***Đảo ngược toàn bộ bản rõ*:** nghĩa là bản rõ được viết theo thứ tự ngược lại để tạo ra bản mã.
- ***Mã hóa theo mẫu hình học*:** bản rõ được sắp xếp lại theo một mẫu hình học nào đó, thường là một mảng hoặc một ma trận hai chiều.
- ***Hoán vị các ký tự của bản rõ theo chu kỳ cố định d*:** nếu hàm *f* là một hoán vị của một khối gồm *d* ký tự thì khóa mã hóa được biểu diễn bởi $K(d, f)$.

IX – HỆ MÃ KNAPSACK

1. Bài toán xếp ba lô tổng quát

Cho *M*, *N* và $A_1,\ A_2,\ \ldots, A_N$ là các số nguyên dương, tìm các số x_i không âm sao cho $M = \sum_{i=1}^{N} x_i A_i$.

Vector $A = (A_1, A_2, ..., A_N)$ được gọi là vector xếp ba lô, còn vector $X = (x_1, x_2, ..., x_N)$ là vector nghiệm.

Một trường hợp riêng đáng quan tâm của bài toán xếp ba lô tổng quát là trường hợp mà $x_i \in \{0,1\}$. Khi đó ta có bài toán xếp ba lô 0/1.

2. Vector xếp ba lô siêu tăng

Trong trường hợp vector $A = (A_1, A_2, ..., A_N)$ được sắp lại thành $A' = (A'_1, A'_2, ..., A'_N)$ sao cho với $\forall i$ ta có $\sum_{j<i} A'_j < A'_i$ thì vector $A = (A_1, A_2, ..., A_N)$ được gọi là vector xếp ba lô siêu tăng.

Khi $A = (A_1, A_2, ..., A_N)$ là một vector xếp ba lô siêu tăng, ta có ngay tính chất: $M \geq A'_i \forall i$. Do đó việc giải bài toán xếp ba lô 0/1 trở nên dễ dàng hơn rất nhiều.

3. Cách xây dựng

- Chọn 1 vector siêu tăng $A' = (a'_1, a'_2, ..., a'_N)$, chọn 1 số $M > 2a'_N$, chọn ngẫu nhiên 1 số $u < M$ và $\text{GCD}(u, M) = 1$.
- Xây dựng vector $A = (a_1, a_2, ..., a_N)$ trong đó $a_i = (a'_i u) \bmod M$.
- Khóa $K_P = (A, M)$, $K_S = (u, u^{-1})$.
- Không gian các bản rõ là không gian mọi dãy *N* bit: $P = (x_1, x_2, ..., x_N)$.
  - Mã hóa: $C = \left(\sum_{i=1}^{N} a_i x_i \right) \bmod M$
  - Giải mã: Tính $C' = Cu^{-1} \bmod M$ sau đó giải bài toán xếp ba lô 0/1 với A', C' từ đó tìm được $P = (x_1, x_2, ..., x_N)$.

***Ví dụ*:** Cho hệ mã Knapsack có $A=\{11,15,30,60\}$, $M=150$ và $u=77$.

a) Hãy tìm khóa công khai K_P và khóa bí mật K_S của hệ mã trên.

b) Để mã hóa các thông điệp viết bằng tiếng Anh, người ta dùng một hàm chuyển đổi từ các ký tự thành các xâu nhị phân như sau:

Ký tự	Xâu bít	Ký tự	Xâu bít	Ký tự	Xâu bít	Ký tự	Xâu bít
A	00000	H	00111	O	01110	V	10101
B	00001	I	01000	P	01111	W	10110
C	00010	J	01001	Q	10000	X	10111
E	00100	L	01011	S	10010	Z	11001
F	00101	M	01100	T	10011		
G	00110	N	01101	U	10100		

Khi đó ví dụ xâu ABCD sẽ được chuyển thành 00000 00001 00010 00011 và cắt thành các xâu có độ dài 4 để thực hiện mã hóa. Kết quả thu được bản mã là một dãy các số thuộc Z_M. Hãy thực hiện mã hóa xâu *P* = "ANTI"

Giải

a) Ta có $u^{-1}=u^{-1}\bmod M=77^{-1}\bmod 150=113$

Nên $K_P=\{(11,150),(15,150),(30,150),(60,150)\}$, $K_S=(77,113)$.

b) Xâu "ANTI" chuyển thành xâu nhị phân, ta được:

00000 01101 10011 01000

Cắt thành xâu có độ dài là 4, ta được các xâu "0000", "0011", "0110", "0110", và "1000".

Mã hóa từng xâu trên

$$C_1=(11.0+15.0+30.0+60.0)\bmod 150=0$$
$$C_2=(11.0+15.0+30.1+60.1)\bmod 150=90$$
$$C_3=(11.0+15.1+30.1+60.0)\bmod 150=45$$
$$C_4=(11.0+15.1+30.1+60.0)\bmod 150=45$$
$$C_5=(11.1+15.0+30.0+60.0)\bmod 150=11$$

Bản mã thu được là $C=\langle 0,90,45,45,11\rangle$.

X – HỆ MÃ RSA

Để cài đặt RSA ban đầu mỗi người dùng sinh khóa công khai và khóa bí mật của mình bằng cách:

- Chọn hai số nguyên tố lớn ngẫu nhiên (cỡ gần 100 chữ số) khác nhau *p* và *q*.
- Tính $N = pq$.
- Chọn một số *e* nhỏ hơn *N* và $\text{GCD}\left(e, \phi\left(N\right)\right) = 1$, *e* được gọi là số mũ lập mã.
- Tìm phần tử nghịch đảo của *e* trên modulo $\phi\left(N\right)$, *d* là số mũ giải mã. Tức là $d = e^{-1} \bmod \phi\left(N\right)$
- Khóa công khai là $K_P = \left(e, N\right)$.
- Khóa bí mật là $K_S = K_P^{-1} = \left(d, p, q\right)$.

Sử dụng RSA

- Để mã hóa một thông điệp *M*: $C = M^e \bmod N \ \ \left(0 \le M < N\right)$.
- Giải mã: $M = C^d \bmod N$.

***Ví dụ 1*:** Cho hệ mã RSA có $p = 31,\ q = 41,\ e = 271$.

a) Hãy tìm khóa công khai K_P và khóa bí mật K_S của hệ mã trên.

b) Để mã hóa các thông điệp được viết bằng tiếng Anh, người ta dùng một hàm chuyển đổi các ký tự thành các số thập phân có hai chữ số như sau:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Khi đó ví dụ xâu ABC sẽ được chuyển thành 00 01 02 và sau đó cắt thành các số có 3 chữ số 000 (bằng 0) và 102 để mã hóa. Bản mã thu được là một tập các số thuộc Z_N. Hãy thực hiện mã hóa xâu *P* = "SERIUS".

c) Giả sử bản mã thu được là $C = \left\langle 201, 793, 442, 18 \right\rangle$, hãy thực hiện giải mã để tìm ra thông điệp bản rõ ban đầu.

Giải

a) Ta có $N = pq = 31.41 = 1271,\ \phi(N) = (31-1)(41-1) = 1200.$

$d = e^{-1} \bmod \phi(N) = 271 \bmod 1200 = 31.$

Vậy khóa công khai $K_P = (271, 1271),$ khóa bí mật $K_S = (31, 31, 41).$

b) Chuyển xâu "SERIUS" thành các số thập phân có hai chữ số, ta được:

18 04 17 08 20 18

Cắt thành các số có 3 chữ số, ta được các số: 180, 417, 82, 18.

Mã hóa từng số trên:

$$C_1 = M_1^e \bmod N = 180^{271} \bmod 1271 = 180$$
$$C_2 = M_2^e \bmod N = 417^{271} \bmod 1271 = 634$$
$$C_3 = M_3^e \bmod N = 82^{271} \bmod 1271 = 82$$
$$C_4 = M_4^e \bmod N = 18^{271} \bmod 1271 = 18$$

Bản mã thu được là $C = <180, 634, 82, 18>.$

c) Giải mã từng số bản rõ trên:

$$M_1 = C_1^d \bmod N = 201^{31} \bmod 1271 = 201$$
$$M_2 = C_2^d \bmod N = 793^{31} \bmod 1271 = 700$$
$$M_3 = C_3^d \bmod N = 442^{31} \bmod 1271 = 132$$
$$M_4 = C_4^d \bmod N = 18^{31} \bmod 1271 = 18$$

Từ đó ta chuyển thành xâu: 201700132018.

Tách thành các xâu có 2 chữ số, ta được 20 (U), 17 (R), 00 (A), 13 (N), 20 (U), 18 (S). Vậy, thông điệp ban đầu là URANUS.

X – HỆ MÃ EL GAMMAL

Ban đầu, người ta sẽ chọn một số nguyên tố lớn *p* và hai số nguyên tùy ý nhỏ hơn *p* là *a* (*a* là một phần tử nguyên thủy của Z_P^*) và *x* (*x* là của người nhận, bí mật), sau đó tính:

$$y = a^x \bmod p$$

Để mã hóa một thông điệp *M* (là một số nguyên trên Z_P) thành bản mã *C*, người gửi chọn một số ngẫu nhiên *k* nhỏ hơn *p* và tính khóa mã hóa $K = y^k \bmod p = a^{xk} \bmod p,$ sau đó tính cặp bản mã $C_1 = a^k \bmod p$ và $C_2 = KM \bmod p$ và gửi bản mã $C = (C_1, C_2)$ đi.

Để giải mã thông điệp, đầu tiên ta cần tính lại mã hóa thông điệp *K*:

$$K = C_1^x \bmod p = a^{kx} \bmod p$$

Sau đó tính *M* bằng cách giải phương trình $M = C_2 K^{-1} \bmod p$

Việc giải mã bao gồm việc tính lại khóa tạm thời *K*. Khóa công khai của hệ mã là (p, a, y), khóa bí mật là *x*.

***Ví dụ 1*:** Cho hệ mã El Gammal có $p = 31$, $a = 11$, và $x = 6$. Để mã hóa $M = 18$ người ta chọn $k = 7$. Hãy thực hiện tính toán và đưa ra bản mã kết quả.

Giải

Ta có $y = a^x \bmod p = 11^6 \bmod 31 = 4.$

Khóa mã hóa $K = y^k \bmod p = 4^7 \bmod 31 = 16.$

Cặp bản mã $C_1 = a^k \bmod p = 11^7 \bmod 31 = 13,\ C_2 = KM \bmod p = 16.18 \bmod 31 = 9.$

Vậy bản mã kết quả là $C = (13, 9).$

***Ví dụ 2*:** Cho hệ mã mật El Gammal có $p = 1187$, $a = 79$ là một phần tử nguyên thủy của Z_P^*, $x = 113.$

a) Hãy tìm khóa công khai K_P và khóa bí mật K_S của hệ mã trên.

b) Để mã hóa các thông điệp được viết bằng tiếng Anh, người ta dùng một hàm chuyển đổi các ký tự thành các số thập phân có hai chữ số như sau:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Khi đó ví dụ xâu ABC sẽ được chuyển thành 00 01 02 và sau đó cắt thành các số có 3 chữ số là 000 (bằng 0) và 102 để mã hóa. Bản mã thu được là một tập các cặp số (C_1, C_2) thuộc Z_P. Hãy thực hiện mã hóa xâu *m* = "TAURUS" với các giá trị $13 < k < 19.$

c) Giả sử thu được bản mã là một tập các cặp (C_1, C_2) là

$$\langle (358, 305), (1079, 283), (608, 925), (786, 391) \rangle$$

Hãy giải mã và đưa ra thông điệp ban đầu.

Giải

a) Ta có $y = a^x \bmod p = 79^{113} \bmod 1187 = 76.$

Khóa công khai $K_P = (p, a, y) = (1187, 79, 76)$ khóa bí mật $K_S = 113.$

b) Xâu "TAURUS" chuyển đổi thành các số thập phân có hai chữ số, ta được:

19 00 20 17 20 18

Cắt thành các số có 3 chữ số, ta được các số 190, 20, 172, 18.

- Với $k = 14$, ta có: $K = y^k \bmod p = 76^{14} \bmod 1187 = 1025.$

  $C_1 = a^k \bmod p = 79^{14} \bmod 1187 = 981.$

  $M = 190 \Rightarrow C_2 = KM \bmod p = 1025.190 \bmod 1187 = 82$

  $M = 20 \Rightarrow C_2 = KM \bmod p = 1025.20 \bmod 1187 = 321$

  $M = 172 \Rightarrow C_2 = KM \bmod p = 1025.172 \bmod 1187 = 624$

  $M = 18 \Rightarrow C_2 = KM \bmod p = 1025.18 \bmod 1187 = 645$

  Ta có tập các cặp số $C = \langle (981,82),(981,321),(981,624),(981,645) \rangle$

- Với $k = 15$, 16, 17, 18 làm tương tự (lười làm lắm, ahihi).

c) Với cặp $(358,305)$, ta có $K = C_1^x \bmod p = 358^{113} \bmod 1187 = 279,$

$K^{-1} = K^{-1} \bmod 1187 = 279^{-1} \bmod 1187 = 234.$

$\Rightarrow M = C_2 K^{-1} \bmod p = 305.234 \bmod 1187 = 150.$

Với cặp $(1079,283)$, ta có $K = C_1^x \bmod p = 1079^{113} \bmod 1187 = 212.$

$K^{-1} = K^{-1} \bmod 1187 = 212^{-1} \bmod 1187 = 28.$

$\Rightarrow M = C_2 K^{-1} \bmod 1187 = 283.28 \bmod 1187 = 802.$

Với cặp $(608,925)$, ta có $K = C_1^x \bmod p = 608^{113} \bmod 1187 = 925.$

$K^{-1} = K^{-1} \bmod 1187 = 925^{-1} \bmod 1187 = 965.$

$\Rightarrow M = C_2 K^{-1} \bmod 1187 = 925.965 \bmod 1187 = 1.$

Với cặp $(786,391)$, ta có $K = C_1^x \bmod p = 786^{113} \bmod 1187 = 858.$

$K^{-1} = K^{-1} \bmod 1187 = 858^{-1} \bmod 1187 = 184.$

$\Rightarrow M = C_2 K^{-1} \bmod 1187 = 391.184 \bmod 1187 = 724$

Ta được xâu "150 802 001 724"

Tách thành các xâu có hai chữ số, ta được 15 (P), 8 (I), 2 (C), 0 (A), 17 (R), 24 (Y).

Vậy, thông điệp ban đầu là PICARY.

XI – CHỮ KÝ ĐIỆN TỬ

Một sơ đồ chữ ký điện tử là bộ năm (P, A, K, S, V) thỏa mãn các điều kiện dưới đây:

- P là tập hữu hạn các bức điện (thông điệp, bản rõ) có thể.
- A là tập hữu hạn các chữ ký có thể
- K là tập không gian khóa (tập hữu hạn các khóa có thể).
- Với mỗi khóa $K \in K$ tồn tại một thuật toán ký $\text{sig}_K \in S$ và một thuật toán xác minh $\text{ver}_K \in V$. Mỗi $\text{sig}_K : P \to A$ và $\text{ver}_K : P \times A \to \{\text{true, false}\}$ là những hàm sao cho mỗi bức điện $x \in P$ và mỗi chữ ký $y \in A$ thỏa mãn phương trình dưới đây:

$$\text{ver}(x, y) = \begin{cases} \text{true} & \text{if } y = \text{sig}(x) \\ \text{false} & \text{if } y \neq \text{sig}(x) \end{cases}$$

XII – HỆ CHỮ KÝ RSA

Cho $n = pq$, trong đó p, q là các số nguyên tố. Đặt $P = A = Z_N$ và định nghĩa: $K = \{(n, p, q, a, b) : n = pq,\ p \text{ và } q \text{ là các số nguyên tố},\ ab = 1 \bmod \phi(N)\}$. Các giá trị n và b là công khai, còn p, q, a là bí mật.

Với $K = (n, p, q, a, b)$ ta xác định $\text{sig}_K(x) = x^a \bmod n$ và $\text{ver}_K(x, y) = \text{true} \Leftrightarrow x = y^b \bmod n$ với $x, y \in Z_n$.

***Ví dụ*:** Cho hệ chữ ký điện tử RSA có $p = 31,\ q = 41,\ b = 271$.

a) Hãy tìm khóa công khai K_P và khóa bí mật K_S của hệ mã trên.

b) Hãy tính chữ ký cho thông điệp $M = 100$.

Giải

a) Ta có $n = pq = 31.41 = 1271,\ \phi(n) = (p-1)(q-1) = (31-1)(41-1) = 1200.$

$ab = 1 \bmod \phi(n) \Leftrightarrow a = b^{-1} \bmod \phi(n) = 271^{-1} \bmod 1200 = 31.$

Vậy khóa công khai $K_P = (1271, 271)$, khóa bí mật $K_S = (31, 41, 31)$.

b) Ta có $\text{sig}(M) = M^a \bmod n = 100^{31} \bmod 1271 = 100.$

XIII – HỆ CHỮ KÝ EL GAMMAL

Cho p là một số nguyên tố như là bài toán logarit rời rạc trong Z_p, $\alpha \in Z_p^*$ là một phần tử nguyên tử và $P = Z_p^*$, $A = Z_p^* Z_{p-1}$, và định nghĩa $K = \{(p, \alpha, a, \beta) : \beta = \alpha^a \bmod p\}$ trong đó giá trị p, α, và β là công khai, còn a là bí mật.

Với $K = (p, \alpha, a, \beta)$ và chọn một số ngẫu nhiên $k \in Z_{p-1}^*$, định nghĩa: $\text{sig}_K(x,k) = (\gamma, \delta)$, trong đó $\gamma = \alpha^k \bmod p$, $\delta = (x - a\gamma)k^{-1} \bmod (p-1)$.

Với $x, \gamma \in Z_p^*$ và $\delta \in Z_{p-1}$, định nghĩa $\text{ver}(x, \gamma, \delta) = \text{true} \Leftrightarrow \beta^\gamma \gamma^\delta = \alpha^x \pmod p$.

***Ví dụ*:** Cho hệ chữ ký điện tử El Gammal có $p = 1019$, $a = 191$ là một phần tử nguyên thủy của Z_p^*, $\alpha = 37$.

a) Hãy tìm khóa công khai K_P và khóa bí mật K_S của hệ chữ ký trên.

b) Để ký lên bản rõ $M = 102$, người ta chọn $k = 143$, hãy thực hiện ký đưa ra chữ ký tương ứng.

c) Kiểm tra xem cặp $(K, S) = (251, 507)$ có là chữ ký lên văn bản $M = 127$ hay không.

Giải

a) Ta có $\beta = \alpha^a \bmod p = 37^{191} \bmod 1019 = 611$.

Khóa công khai $K_P = (1019, 37, 611)$, khóa bí mật $K_S = 191$.

b) Ta có $\text{sig}(M,k) = (\gamma, \delta)$

$\gamma = \alpha^k \bmod p = 37^{143} \bmod 1019 = 644$.

$\delta = (M - a\gamma)k^{-1} \bmod (p-1)$

$= \{[(M - a\gamma) \bmod (p-1)].[k^{-1} \bmod (p-1)]\} \bmod (p-1)$

$= \{[(102 - 191.644) \bmod (1019-1)].[143^{-1} \bmod (1019-1)]\} \bmod (1019-1)$

$= [(-122902) \bmod 1018].[143^{-1} \bmod 1018] \bmod 1018$

$= (276.299) \bmod 1018 = 66$.

$\Rightarrow \text{sig}(M,k) = (644, 66)$

c) Ta cần tính $\text{ver}(127, 251, 507)$

Ta kiểm tra $\beta^{\gamma}\gamma^{\delta} = a^{x} \bmod p$

$$\left(\beta^{\gamma}\gamma^{\delta}\right) \bmod 1019 = \left[\left(\beta^{\gamma} \bmod 1019\right).\left(\gamma^{\delta} \bmod 1019\right)\right] \bmod 1019$$

$$= \left[\left(611^{251} \bmod 1019\right)\left(251^{507} \bmod 1019\right)\right] \bmod 1019$$

$$= (593.310) \bmod 1019 = 410$$

$$\alpha^{x} \bmod p = 37^{127} \bmod 1019 = 975.$$

$$\Rightarrow \beta^{\gamma}\gamma^{\delta} \neq a^{x} \bmod p$$

Vậy $\text{ver}(127, 251, 507) = \text{false}$. Hay cặp (251, 507) không là chữ ký lên $M = 127$.