

BÀI TẬP CHƯƠNG 01

1. BÀI TẬP QUỐC TẾ VỀ MÃ HÌNH XÃ HỘ VÀ CÁC HỆ THỐNG

Dùng thuật toán辗转相除法, tìm được khóa $K = 4$, từ đó tìm được bùn số:

LOVE MEANS NEVER HAVING TO SAY YOU ARE SORRY.

d. b) Theo đề ta có : F giải mã thành x ($5 \rightarrow 02$)

Ta thống kê được C xuất hiện nhiều nhất: 33 lần.

Theo hàm tạo mã, ta có: $y = ax + b \pmod{06}$

Giả sử $C \rightarrow T$ ($0 \rightarrow 7$), ta có hpt:

$$\begin{cases} 5 = 02a + b \\ 0 = 7a + b \end{cases} \Rightarrow \begin{cases} a = 1 \\ b = 5 \end{cases} \quad (\text{loci})$$

Giả sử $C \rightarrow T$ ($0 \rightarrow 19$), ta có hpt:

$$\begin{cases} 5 = 02a + b \\ 0 = 19a + b \end{cases} \Leftrightarrow \begin{cases} a = 1 \\ b = 9 \end{cases}$$

Vì $\text{UCLN}(1, 06) = 1$ nên ta có thể xem $K(1, 9)$ là khóa

\Rightarrow Hàm giải mã: $x = y - 9 \pmod{06}$

\Rightarrow Bùn số: VDXCFJLUTXUETLTNPJWYETXTPBIGLOCN

XPTZTFOPTZGATBHGBLXBDFCZTXZETXRTBJEZJRTPB

GTT...

c) Thông số lần xuất hiện:

A(13), B(21), C(32), D(9), E(13), F(10), H(1), I(16),
J(6), K(20), N(1), O(2), P(20), Q(4), R(12), S(1),
U(6), V(4), X(2), Y(1), Z(4)

Sắp xếp: C(32), B(21); K, P(20); I(16)...

Tổng tiếng anh, tần suất xuất hiện của "E" là cao nhất,
tiếp theo là "T, A, O..."

Nếu giả sử $C = d \rightarrow E = 4, B = 1 \rightarrow T = 19$

Mục tiêu tìm khóa $K(a, b) \Rightarrow$ ta có hệ pt

$$4 = da + b \pmod{26}$$

$$19 = a + b \pmod{26}$$

$$\Rightarrow a = 11, b = 8 \quad \text{gcd}(11, 26) = 1$$

\Rightarrow (8, 11) là khóa

Dùng hàm giải mã: $x = 11^{-1} \cdot (y - 8) \pmod{26}$

$$K \Leftrightarrow x = 9/11 \pmod{26}$$

$$M \Leftrightarrow x = (26k + 11)/11 \Rightarrow x = 11 \Rightarrow M$$

$$W \Leftrightarrow x = 8/11 \pmod{26}$$

$$V \Leftrightarrow x = (26k + 8)/11 \Rightarrow x = 8 \Rightarrow V$$

$$E \Leftrightarrow x = -4/11 \pmod{26}$$

$$C \Leftrightarrow x = (26k - 4)/11 \Rightarrow x = 4 \Rightarrow C$$

Bản lô: MWC

d) Theo thông lệ, ta có cách ký tự xuất hiện nhiều nhất là: L, S(13); V(16); M, V(14); ...

Theo hàm tạo mã ($y = ax + b \pmod{26}$)

Giả sử $L(11) \rightarrow e(4)$; $S(18) \rightarrow t(19)$; ta có hệ pt

$$11 = 4a + b \quad | \quad a = 13$$

$$18 = 19a + b \quad | \quad b = 13$$

Vì $\text{gcd}(a, 26) = 1 \rightarrow K(13, 13)$ là khóa của bản mã.

Hàm giải mã: $x = 13^{-1} (y - 13) \pmod{26}$

Bản lô: CMS...

4.

CONVERSATION: $\alpha 14 \ 13 \ \alpha 1 \ 4 \ 17 \ 18 \ 0 \ 19 \ 8 \ 14 \ 13$

HARRTHYUS: $7 \ 8 \ 0 \ 17 \ 17 \ 19 \ 13 \ \alpha 0 \ \alpha 4 \ 19 \ \alpha 0 \ 18$

Xét $m = 2$: Ta có các cặp tử vi ứng với :

$$x = (\alpha 14) (13, \alpha 1) (4, 17) (18, 0) (19, 8) (14, 3)$$

$$y = (7, 8) (0, 17) (17, 19) (13, \alpha 0) (\alpha 4, 19) (\alpha 0, 18)$$

$$\Rightarrow \text{Khoá có dạng } K = \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix}$$

\Rightarrow Hàm tia mă $y = xK \Rightarrow$ Ta có hệ pt:

$$\alpha. K_{11} + 14. K_{21} = 7$$

$$\alpha. K_{12} + 14. K_{22} = 8$$

$$13. K_{11} + \alpha 1. K_{12} = 0$$

$$13. K_{21} + \alpha 1. K_{22} = 17$$

Vô nghiệm \Rightarrow loci

Xét $m = 3$, ta có các cặp tử vi ứng với

$$x = (\alpha 14, 13), (\alpha 1, 4, 17), (18, 0, 19), (8, 14, 13)$$

$$y = (7, 8, 0), (17, 17, 19), (13, \alpha 0, \alpha 4), (19, \alpha 0, 18)$$

$$\Rightarrow \text{Khoá có dạng } K = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix}$$

\Rightarrow Hàm tia mă $y = xK \Rightarrow$ Ta có hệ pt:

$$\alpha. K_{11} + 14. K_{21} + 13. K_{31} = 7$$

$$\alpha. K_{12} + 14. K_{22} + 13. K_{32} = 8$$

$$\alpha. K_{13} + 14. K_{23} + 13. K_{33} = 0$$

$$\alpha 1. K_{11} + 4. K_{21} + 17. K_{31} = 17$$

$$\alpha 1. K_{12} + 4. K_{22} + 17. K_{32} = 17$$

$$\alpha 1. K_{13} + 4. K_{23} + 17. K_{33} = 19$$

$$18.K_{11} + 0.K_{21} + 19.K_{31} = 13$$

$$18.K_{12} + 0.K_{22} + 19.K_{32} = 20$$

$$18.K_{13} + 0.K_{23} + 19.K_{33} = 24$$

$$\Leftrightarrow K_{11} = 2 \quad K_{21} = 16 \quad K_{31} = 7$$

$$K_{12} = 15 \quad K_{22} = 4 \quad K_{32} = 6$$

$$K_{13} = 3 \quad K_{23} = 20 \quad K_{33} = 8$$

$$\Rightarrow \text{Ma trận mã hóa } K = (2 \ 15 \ 3)$$

$$(16 \ 4 \ 20)$$

$$(7 \ 6 \ 8)$$

5.

ADISPLAYEDCAUTION

0 3 8 18 15 11 0 24 4 3 4 16 0 20 19

8 14 13

DSRMSTOPLXTBZUUM

3 18 17 12 18 8 14 15 11 23 11 9 1 25 20

11 11 12

Vì $m = 3$, ta có các cặp tử tựng ứng với:

$$x = (0, 3, 8) (18, 15, 11) (0, 24, 4) (3, 4, 16) (0, 20, 19) (8, 14, 13)$$

$$y = (3, 18, 17) (12, 18, 8) (14, 15, 11) (23, 11, 9) (1, 25, 20) (11, 12)$$

$$\Rightarrow \text{Mã hóa có dạng } K = (K_{11} \ K_{12} \ K_{13})$$

$$(K_{21} \ K_{22} \ K_{23}) + (b_1, b_2, b_3)$$

$$(K_{31} \ K_{32} \ K_{33})$$

 \Rightarrow Hàm tao mã $y = xK + b \Rightarrow$ Ta có hệ pt:

$$0.K_{11} + 3.K_{21} + 8.K_{31} + b_1 = 3$$

$$0.K_{12} + 3.K_{22} + 8.K_{32} + b_2 = 18$$

$$0.K_{13} + 3.K_{23} + 8.K_{33} + b_3 = 17$$

$$18.K_{11} + 15.K_{21} + 11.K_{31} + b_1 = 12$$

$$18.K_{12} + 15.K_{22} + 11.K_{32} + b_2 = 18$$

$$18.K_{13} + 15.K_{23} + 11.K_{33} + b_3 = 8$$

$$0.K_{11} + 24.K_{21} + 4.K_{31} + b_1 = 14$$

$$0.K_{12} + 24.K_{22} + 4.K_{32} + b_2 = 15$$

$$0.K_{13} + 24.K_{23} + 4.K_{33} + b_3 = 11$$

$$3.K_{11} + 4.K_{21} + 16.K_{31} + b_1 = 23$$

$$3.K_{12} + 4.K_{22} + 16.K_{32} + b_2 = 11$$

$$3.K_{13} + 4.K_{23} + 16.K_{33} + b_3 = 9$$

$$\Leftrightarrow K_{11} = 3 \quad K_{21} = 5 \quad K_{31} = 17 \quad b_1 = 8$$

$$K_{12} = 6 \quad K_{22} = 15 \quad K_{32} = 8 \quad b_2 = 13$$

$$K_{13} = 18 \quad K_{23} = 22 \quad K_{33} = 9 \quad b_3 = 9$$

$$\Rightarrow K = (3 \ 6 \ 18)$$

$$(5 \ 15 \ 22) + (8, 13, 9)$$

$$(17, 8, 9)$$

6. Bản mã : LMQETXYEAGTXCTUIEWNICTXLZEWNAITSP

Z XVAPEWLMGQWXAXFTGMSQCIDAGTXL

MDXNIXSNPTQS WAPRIQSMHNIOCVAXEV.

11 10 16 4 19 23 24 4 0 6 19 23 2 19 20 8 4 2

13 2 19 23 11 25 4 22 20 0 8 18 15 25 24 21 0 15

4 22 11 12 6 16 22 21 0 23 5 19 6 12 18 16 2 0

3 0 6 19 23 11 12 3 23 13 23 18 15 15 9 16 18

24 21 0 15 17 8 16 18 12 7 13 14 2 21 0 23 5 2

Sắp xếp theo thứ tự tần suất xuất hiện của từng cặp (cứ từ $(m=2)$) :

$(T, x): 3$

$(E, x1), (L, M), (V, A) : 2$

Đặt $K = (K_{11} \ K_{12})$

$(K_{21} \ K_{22})$

* Giả sử cặp (T, x) là (T, H) và (E, W) là (S, T)

$$\alpha_9 = \alpha_9 \cdot K_{11} + 7 \cdot K_{21}$$

$$\alpha_3 = \alpha_9 \cdot K_{12} + 7 \cdot K_{22}$$

$$\alpha_4 = 18 \cdot K_{11} + 19 \cdot K_{21}$$

$$\alpha_2 = 18 \cdot K_{12} + 19 \cdot K_{22}$$

$$\Rightarrow K = \begin{pmatrix} \alpha_5 & \alpha_3 \\ \alpha_6 & \alpha_4 \end{pmatrix} \Rightarrow K \text{ tồn tại } K^{-1} \Rightarrow \text{tối}.$$

* Giả sử cặp (T, x) là (T, H) và (I, N) là (S, T) , ta có hệ pt,

$$\alpha_9 = \alpha_9 \cdot K_{11} + 7 \cdot K_{21}$$

$$\alpha_3 = \alpha_9 \cdot K_{12} + 7 \cdot K_{22}$$

$$\alpha_1 = 18 \cdot K_{11} + 19 \cdot K_{21}$$

$$\alpha_2 = 18 \cdot K_{12} + 19 \cdot K_{22}$$

$$\Leftrightarrow K_{11} = \alpha_4 \quad K_{21} = \alpha_3 \quad \Rightarrow K = \begin{pmatrix} \alpha_4 & \alpha_5 \\ \alpha_3 & \alpha_2 \end{pmatrix} \Rightarrow K = \det(K)^{-1} \cdot K$$

$$K_{12} = \alpha_5 \quad K_{22} = \alpha_4$$

$$\Rightarrow K^{-1} = \begin{pmatrix} \alpha_2 & -\alpha_1 \\ -\alpha_3 & \alpha_4 \end{pmatrix}$$

7.

a) - Chia binh mã thành các khối có m*n ký tự

- Sắp xếp lại các khối theo cách sau:

$$1+0.n, 1+1.n, 1+\alpha.n, \dots, 1+(m-1).n$$

$$\alpha+0.n, \alpha+1.n, \alpha+\alpha.n, \dots, \alpha+(m-1).n$$

$$n+0.n, n+1.n, n+\alpha.n, \dots, n+(\alpha-1).n$$

b) MYAMRARUYIQTEENCTORAHROYWDDSOYECUARRGDDERNG

Mã trên có 42 ký tự, ta có thể chia thành các từng bộ:

$\alpha \times 21, \alpha \times \alpha, 3 \times 14, 14 \times 3, 6 \times 7, 7 \times 6$. Dùng thuật toán

KILOG

vết cạn, tìm ra rằng sốt phù hợp là 6×7 (chia bén mà thành 7 khối, mỗi khối 6 ký tự ($m=3, n=2$)).

MARYNRA

RYQUIT

VICTOR

ATIROVIXI

DSOYEO

URRGAD

ERNIOGIX

\Rightarrow Sắp xếp lại các khối theo правило trên:

MARYNRA

RYQUIT

ECONTR

ARYHOW

DOESYO

URRGARD

ENIGROW

\Rightarrow MARY MARY QUITE CONTRARY HOW DOES YOUR GARDEN GROW.

Bài tập chương I.

8.

$$Pb(a) = \frac{1}{2}; Pb(b) = \frac{1}{3}; Pb(c) = \frac{1}{6}$$

Các khóa đồng xác suất: $Pk(k_1) = Pk(k_2) = Pk(k_3) = \frac{1}{3}$

$$Pc(1) = \frac{1}{2} \cdot \frac{1}{3} + \frac{1}{6} \cdot \frac{1}{3} = \frac{2}{9}$$

$$Pc(2) = \frac{1}{3} \cdot \frac{1}{3} + \frac{1}{6} \cdot \frac{1}{2} = \frac{5}{18}$$

$$Pc(3) = \frac{1}{2} \cdot \frac{1}{3} + \frac{1}{6} \cdot \frac{1}{3} + \frac{1}{3} \cdot \frac{1}{2} = \frac{1}{3}$$

$$Pc(4) = \frac{1}{3} \cdot \frac{1}{3} + \frac{1}{6} \cdot \frac{1}{3} = \frac{1}{6}$$

$$H(P) = -\frac{1}{2} \cdot \log_2 \frac{1}{2} - \frac{1}{3} \cdot \log_2 \frac{1}{3} - \frac{1}{6} \cdot \log_2 \frac{1}{6} = 1,46$$

Date:

No:

KIẾN GÓC

$$H(K) = -\frac{1}{3} \cdot 3 \log_2 \frac{1}{3} = 1,58$$

$$H(C) = 1,95$$

$$H(K|C) = H(K) + H(P) - H(C) = 1,09$$

$$H(X|C) = H(X)$$

9

$$a = 1573, b = 308$$

$$\text{Đặt } (A_1, A_2, A_3) = (1, 0, 1573)$$

$$(B_1, B_2, B_3) = (0, 1, 308)$$

$$Q = A_3 / B_3 = 5$$

$$\text{Đặt } (A_1, A_2, A_3) = (0, 1, 308)$$

$$(B_1, B_2, B_3) = (1, -4, 33)$$

$$Q = 9$$

$$(A_1, A_2, A_3) = (1, -4, 33)$$

$$(B_1, B_2, B_3) = (-9, 37, 11)$$

$$Q = 3$$

$$(A_1, A_2, A_3) = (-9, 37, 11)$$

$$(B_1, B_2, B_3) = (28, -115, 0)$$

$$\sqrt{B_3} = 0 \text{ nên } \text{UCINI}(1573, 308) = A_3 = 11$$

$$10. \quad 3^{22} \bmod 23 = ?$$

Thiết kế:

$$a = 3; K = 22; n = 23$$

$$K_i = 10110; t = 4$$

$$\text{Gán } b = 1; \text{ nếu } K_i = 0 \text{ return } 1;$$

$$\text{Gán } A = a; \text{ nếu } K_i = 1 \Rightarrow b = a;$$

for ($i = 0$; $i < t$; $i++$)

$$A = A^2 \bmod n;$$

$$\text{nếu } K_i = 1 \Rightarrow b = A \cdot b \bmod n;$$

Return b ;

Date: . . .	No: . . .
-------------	-----------

Bảng mô tả các bước diễn:

i	0	1	2	3	4
α^i	0	1	2	3	4
A	3	9	12	6	13
b	1	9	16	16	1

Vậy $3^{\text{el}} \text{ mod } 37 = 1$.

11. Tính các căn bậc d của $10 \text{ mod } 37$.

(Dùng thuật toán SGK 143)

$$\alpha = 10, p = 37 (p = 5 \text{ mod } 8)$$

Tính Legendre ($10/37$)

$$(10/37) = (4/37) \cdot (3/37) = (2/37)^d \cdot (3/37)$$

$$= -1^d \cdot 1 = 1$$

$$\Rightarrow d = 10^{(37-1)/4} \text{ mod } 37 = 10^9 \text{ mod } 37$$

$$= (10^3)^3 \text{ mod } 37 = 1$$

$$\text{Vậy } x = 10^{(37+3)/18} \text{ mod } 37 = 10^5 \text{ mod } 37 = 7$$

$$\Rightarrow -x = -7$$

Vậy các căn bậc d của $10 \text{ mod } 37$ là $(7, -7)$

12.

$$\phi(19) = 19 - 1 = 18 = 2 \cdot 3^2$$

Tìm các phân tử nguyên thủy sao cho

$$x^{18/2} \text{ mod } 37 = 1 \Leftrightarrow x^9 \text{ mod } 37 = 1$$

$$x^{18/3} \text{ mod } 37 = 1 \quad x^6 \text{ mod } 37 = 1$$

$$\text{Xét } x = 2 \Leftrightarrow 2^9 \text{ mod } 37 = 31 \neq 1$$

$$2^6 \text{ mod } 37 = 27 \neq 1$$

$\Rightarrow 2$ là phân tử nguyên thủy của Z_{19}

Nếu $\text{lcm}(i, \phi(19)) = 1$ thì i thuộc Z_{18}

$$Z_{18} = \{1, 5, 7, 11, 13, 17\}$$

Date:	.	No:
-------	---	-----

KẾT QUẢ

$$\omega^1 \bmod 19 = 2; \omega^5 \bmod 19 = 13$$

$$\omega^7 \bmod 19 = 14; \omega^{11} \bmod 19 = 15$$

$$\omega^{13} \bmod 19 = 3; \omega^{17} \bmod 19 = 10$$

Vậy các phần tử nguyên thủy của nhóm nhân \mathbb{Z}_{19} là
 $\{2, 3, 10, 13, 14, 15\}$

13.

Tìm phần tử nghịch đảo hàng của 3 trong \mathbb{Z}_{31} .

Gọi x là phần tử nghịch đảo của 3, ta có:

$$3x \equiv 1 \pmod{31}$$

$$\Leftrightarrow 3x - 1 = 31k \quad (k=1, 2, 3, \dots)$$

$$\Leftrightarrow x \equiv 21$$

15. Tính $\phi(490)$; $\phi(768)$ a) $\phi(490)$

$$490 = \omega^5 \cdot 7^2$$

$$\phi(490) = 490 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right)$$

b) $\phi(768)$

$$768 = \omega^8 \cdot 3$$

$$\phi(768) = 768 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 1024.$$

16. Giải hệ pt đồng dư:

$$5x \equiv 10 \pmod{6}$$

$$6x \equiv 6 \pmod{5}$$

$$4x \equiv 5 \pmod{7}$$

$$\begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 1 \pmod{5} \end{cases}$$

$$x \equiv 3 \pmod{7}$$

$$M = 6 \cdot 5 \cdot 7 = 210$$

$$M_1 = 35, M_2 = 42, M_3 = 30$$

Date: . . .	No: . . .
-------------	-----------

$$35y_1 = 4 \pmod{6} \Leftrightarrow y_1 = 2$$

$$49y_2 = 1 \pmod{5} \Leftrightarrow y_2 = 3$$

$$30y_3 = 3 \pmod{7} \Leftrightarrow y_3 = 5$$

$$\Rightarrow x = M_1 \cdot y_1 + M_2 \cdot y_2 + M_3 \cdot y_3 \pmod{M}$$

$$= 346 \pmod{210} = 136 \pmod{210}.$$

17.

Dùng Euclidean mở rộng để tính:

$$a) 17^{-1} \pmod{101}$$

$$\text{Đối } (A_1, A_2, A_3) = (1, 0, 101)$$

$$(B_1, B_2, B_3) = (0, 1, 17)$$

 $Q = 5$

$$(A_1, A_2, A_3) = (0, 1, 17)$$

$$(B_1, B_2, B_3) = (1, -5, 16)$$

 $Q = 1$

$$(A_1, A_2, A_3) = (1, -5, 16)$$

$$(B_1, B_2, B_3) = (-1, 6, 1)$$

$$\sqrt{B_3} = 1 \text{ nên } 17^{-1} \pmod{101} = B_2 = 6.$$

$$b) 357^{-1} \pmod{1234}$$

$$\text{Đối } (A_1, A_2, A_3) = (1, 0, 1234)$$

$$(B_1, B_2, B_3) = (0, 1, 357)$$

 $Q = 3$

$$(A_1, A_2, A_3) = (0, 1, 357)$$

$$(B_1, B_2, B_3) = (1, -3, 163)$$

 $Q = 2$

$$(A_1, A_2, A_3) = (1, -3, 163)$$

$$(B_1, B_2, B_3) = (-2, 7, 31)$$

Date: . . .	No: _____
-------------	-----------

$$Q = 5$$

$$(A_1, A_2, A_3) = (-2, 7, 31)$$

$$(B_1, B_2, B_3) = (11, -38, 8)$$

$$Q = 3$$

$$(A_1, A_2, A_3) = (11, -38, 8)$$

$$(B_1, B_2, B_3) = -35, 121, 7)$$

$$Q = 1$$

$$(A_1, A_2, A_3) = (35, 121, 7)$$

$$(B_1, B_2, B_3) = (-24, -159, 1)$$

$$\tilde{w} B_3 = 1 \text{ nén } 35^{-1} \bmod 1234 = B_2 = -159$$

$$c) 3125^{-1} \bmod 9987.$$

$$\text{Đây } (A_1, A_2, A_3) = (1, 0, 9987)$$

$$(B_1, B_2, B_3) = 0, 1, 3125)$$

$$Q = 3. \quad (A_1, A_2, A_3) = (0, 1, 3125)$$

$$(B_1, B_2, B_3) = (1, -3, 612)$$

$$Q = 5. \quad (A_1, A_2, A_3) = (1, -3, 612)$$

$$(B_1, B_2, B_3) = (-5, 16, 65)$$

$$Q = 9. \quad (A_1, A_2, A_3) = (-5, 16, 65)$$

$$(B_1, B_2, B_3) = (46, -147, 27)$$

$$Q = d. \quad (A_1, A_2, A_3) = (46, -147, 27)$$

$$(B_1, B_2, B_3) = (-97, 310, 11)$$

$$Q = d. \quad (A_1, A_2, A_3) = (-97, 310, 11)$$

$$(B_1, B_2, B_3) = (240, -767, 5)$$

$$Q = d. \quad (A_1, A_2, A_3) = (240, -767, 5)$$

$$(B_1, B_2, B_3) = (-570, 1844, 1)$$

$$\tilde{w} B_3 = 1 \text{ nén } 3125^{-1} \bmod 9987 = B_2 = 1844.$$