Thứ ngày

Họ và tên: Đặng Như Ngọc

MSV: 11193747

Câu 1:

a, $23^{11} \bmod 17 = (23 \bmod 17)^{11} \bmod 17$

$= 6^{11} \bmod 17$

$= 6^2 . 6^4 . 6^5 \bmod 17$

$= [(6^2 \bmod 17)(6^4 \bmod 17)(6^5 \bmod 17)] \bmod 17$

Vì $6^2 \bmod 17 = 2 \Rightarrow 6^4 \bmod 17 = 4$

$6^5 \bmod 17 = (6 . 6^4) \bmod 17 = [(6 \bmod 17)(6^4 \bmod 17)] \bmod 17$

$= (6 . 4) \bmod 17 = 7$

Vậy $23^{11} \bmod 17 = (2 . 4 . 7) \bmod 17 = 5$

b, Ta có ma trận khoá:

d	a	i	h	o
c	k	t	q	b
e	f	g	l	m
n	p	r	s	u
v	w	x	y	z

Chia bản rõ: an to an ba om at th on gt in

Bản mã: Tìm được bản mã là:

dp bi dp ko bu ik qi d u r g d r

Câu 2:

Ban đầu giá trị của các thanh ghi X, Y, Z là:

X = 100101

Y = 01001110

Z = 10011001 1

Bước 0: $x_1 = 0$, $y_3 = 0$, $z_3 = 1 \Rightarrow m = 0$, quay X, quay Y

x = 110010

Thứ ngày . .

Y = 10100111 → $S_0 = 0 \oplus 1 \oplus 1 = 0$

Z = 100110011

Bước 1: $x_1 = 1$, $y_3 = 0$, $z_3 = 1 \Rightarrow m = 1 \rightarrow$ Quay X, quay Z

X = 111001

Y = 10100111 → $S_1 = 1 \oplus 1 \oplus 1 = 1$

Z = 010011001

Bước 2: $x_1 = 1$, $y_3 = 0$, $z_3 = 0 \rightarrow m = 0 \rightarrow$ Quay Y, quay Z

X = 111001

Y = 01010011 → $S_2 = 1 \oplus 1 \oplus 0 = 0$

Z = 101001100

Vậy bản mã là $P = 110 \oplus 010 = 100$ (chữ E)

Giải mã bản mã là: $100 \oplus 010 = 110$ (chữ g)

Câu 3.

a, Tìm khoá của hệ MHK trên:

- $K_u = (S, M)$ với $S = (S_1, \dots S_N) = (a'_1 * u) \bmod M, (a'_2 * u \bmod M) \dots$
  $= (11 * 77) \bmod 150, (15 * 77) \bmod 150, \dots (60 * 77) \bmod 150$
  $= (97, 105, 60, 120)$ và $M = 150$
- $K_S = (u, u^{-1})$

Ta có $u^{-1} = 77^{-1} \bmod 150$

Dòng	r_0	r_1	r_2	q	t_0	t_1
0	150	77	73	1	0	1
1	77	73	4	1	1	149
2	73	4	1	1	149	2
3	4	1	0	4	2	113

Vậy $u^{-1} = 113$

$\Rightarrow K_S = (77, 113)$

Thứ ngày

b. Mã hoá P = GRAPH

⇒ P = 00110 10001 00000 01111 00111

P bao gồm N = 25 phần tử

P là dãy N bit

P = (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)

Xét các xâu nhỏ: $P_1 = (0, 0, 1, 1)$

$P_2 = (0, 1, 0, 0)$

$P_3 = (0, 1, 0, 0)$

$P_4 = (0, 0, 0, 0)$

$P_5 = (1, 1, 1, 1)$

$P_6 = (0, 0, 1, 1)$

$P_7 = (1, 0, 0, 0)$

⇒ $C_1 = (0 \cdot 97 + 0 \cdot 105 + 1 \cdot 60 + 1 \cdot 120) \bmod 150 = 10$

Tương tự $C_2 = 105$

$C_3 = 105$

$C_4 = 0$

$C_5 = 82$

$C_6 = 30$

$C_7 = 97$.

Vậy bản mã C = (10, 105, 105, 0, 82, 30, 97)

Thứ ngày

c, C = (120, 105, 105, 0, 60, 75, 30, 22, 22, 30)

c = 569

$c' = c u^{-1} \bmod M$

$= 569 \cdot 113 \bmod 150$

$= 97$

A' = (111, 15, 30 60) c' = 97

c = M = 97 > $a_4 = 60 \rightarrow x_4 = 1$

$c_1 = c - x_4 a_4 = 97 - 1 \cdot 60 = 37 > 30 \rightarrow x_3 = 1$

$c_2 = c - x_3 a_3 = 37 - 1 \cdot 30 = 7 < 15 \rightarrow x_2 = 0$

$c_3 = c - x_2 a_2 = 7 - 0 \cdot 15 = 7 < 11 \rightarrow x_1 = 0$

Vậy $X = (x_1 x_2 x_3 x_4)^T = (0\ 0\ 1\ 1)^T$