**BÀI TẬP VỀ NHÀ BUỔI 2:**

**Bài 4:**

C O N V E R S A T I O N:

2 14 13 21 4 17 18 0 19 8 14 13

H I A R R T N U Y T U S:

7 8 0 17 17 19 13 20 24 19 20 18

- Xét m = 2; Ta có các cặp từ tương ứng với:

x = (2,14) (13,21) (4,17) (18,0) (19,8) (14,13)

y = (7,8) (0,17) (17,19) (13,20) (24,19) (20, 18)

=> Khóa có dạng k = (k11 k12)

(k21 k22)

=> Hàm tạo mã y = xk => Ta có hệ PT:

2\*k11 + 14\*k21 = 7

2\*k12 + 14\*k22 = 8

13\*k11 + 21\*k12 = 0

13\*k12 + 21\*k22 = 17

Vô nghiệm => loại

- Xét m = 3; Ta có các cặp từ tương ứng với:

x = (2,14,13) (21,4,17) (18,0,19) (8, 14, 13)

y = (7,8,0) (17,17,19) (13,20,24) (19,20,18)

=> Khóa có dạng K = (k11 k12 k13)

(k21 k22 k23)

(k31 k32 k33)

=>Hàm tạo mã y = xk => Ta có hệ PT:

2\*k11 + 14\*k21 + 13\*k31 = 7

2\*k12 + 14\*k22 + 13\*k32 = 8

2\*k13 + 14\*k23 + 13\*k33 = 0

21\*k11 + 4\*k21 + 17\*k31 = 17

21\*k12 + 4\*K22 + 17\*k32 = 17

21\*k13 + 4\*K23 + 17\*k33 = 19

18\*k11 + 0\*k21 + 19\*k31 = 13

18\*k12 + 0\*k22 + 19\*k32 = 20

18\*k13 + 0\*k23 + 19\*k33 = 24

<=> k11=2 k21=16 k31=7

k12=15 k22=4 k32=6

k13=3 k23=20 k33=8

=>Ma trận mã hóa k = (2 15 3)

(16 4 20)

(7 6 8)

**Bài 5:**

A D I S P L A Y E D E Q A

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

U T I O N:   
20 19 8 14 13

D S R M S I O P L X L J B

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

Z U L L M:

25 20 11 11 12

Vì m = 3; Ta có các cặp từ tương 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) (11,11,12)

=> Khóa có dạng K = (k11 k12 k13)

(k21 k22 k23) + (b1,b2,63)

(k31 k32 k33)

=> Hàm tạo mã y = ax + b => Ta có hệ PT:

0\*k11 + 3\*k21 + 8\*k31 + b1 = 3

0\*k12 + 3\*k22 + 8\*k32 + b2 = 18

0\*k13 + 3\*k23 + 8\*k33 + b3 = 17

18\*k11 + 15\*k21 + 11\*k31 + b1 = 12

18\*k12 + 15\*k22 + 11\*k32 + b2 = 18

18\*k13 + 15\*k23 + 11\*k33 + b3 = 8

0\*k11 + 24\*k21 + 4\*k31 + b1 = 14

0\*k12 + 24\*k22 + 4\*k32 + b2 = 15

0\*k13 + 24\*k23 + 4\*k31 + b3 = 11

3\*k11 + 4\*k21 + 16\*k31 + b1 = 23

3\*k12 + 4\*K22 + 16\*k32 + b2 = 11

3\*k13 + 4\*K23 + 16\*k33 + b3 = 9

k11=3 k21=5 k31=17 b1=8

<=> k12=6 k22=15 k32=8 b2=13

k13=18 k23=22 k33=9 b3=9

(3 6 18)

=> K = (5 15 22) + (8, 13, 9)

(17 8 9)

**Bài 7:**

a/ Cách giải:

- chia bản mã thành các khối có m\*n ký tự

- Sắp xếp lại các khối theo cách sau:

1 + 0 \* n, 1 + 1 \* n, 1 + 2 \* n, ...., 1 + (m-1) \* n.

2 + 0 \* n, 2 + 1 \* n, 2 + 2 \* n, ...., 2 + (m-1) \* n

...

...

n + 0 \* n, n + 1 \* n, 1 + 2 \* n, ...., n + (m-1) \* n

b/ MYAMRARUYIQTENCTORAHROYWDDSOYEOUARRGDDERNOGW

Mã trên có 42 ký tự, ta có thể chia thành các trường hợp: 2x21, 21x2, 3x14, 14x3, 6x7, 7x6. Dùng thuật toán vét cạn, tìm ra trường hợp phù hợp là 6x7 (chia bản mã thành 7 khối, mỗi khối 6 ký tự (m=3, n=2)):

MYAMRA

RUYIQT

VICTOR

AHROYW

DSOYEO

UARRGD

ERNOGW

=> Sắp xếp lại các khối theo giải thuật trên:

MARYMA

RYQUIT

ECONTR

ARYHOW

DOESYO

URGARD

ENGROW

=> MARY MARY QUITE CONTRARY HOW DOES YOUR GARDEN GROW

**Bài 8**:

Pb(a) = 1/2; Pb(b) = 1/3; Pb(c) = 1/6

Các khóa đồng xác xuất: Pk (K1) = Pk (K2) = Pk (K1) = 1/3

PC (1) = 1/2 \* 1/3 + 1/6 \* 1/3 = 2/9

PC (2) = 1/3 \* 1/3 + 1/3 \* 1/2 = 5/18

PC (3) = 1/2 \* 1/3 + 1/6 \* 1/3 + 1/3 \* 1/3 = 1/3

PC (4) = 1/3 \* 1/3 + 1/6 \* 1/3 = 1/6

H (C) = - (2/9 log2 (2/9) + 5/18 log2 (5/18) + 1/3 log2 (1/3) + 1/6 log2 (1/6)) =1.95

H (P) = - (1/2 log2 (1/2) - 1/3 log2 (1/3) - 1/6 log2 (1/6) = 1.46

H (K) = -1/3 \* 3 \* log2 (1/3) = 1.58

H (K|C) = H (K) + H (P) - H (C) = 1.09

Pb (a/1) = (1/2 \* 1/3) / (2/9) = 3/4, Pb (a/2) = 3/5, Pb (a/3) = 1/2, Pb (a/4) = 0

Pb (b/1) = 0, Pb (b/2) = 2/5, Pb (b/3) = 2/6, Pb (b/4) = 2/3

Pb (c/1) = 1/4, Pb (c/2) = 0, Pb (c/3) = 1/6, Pb (c/4) = 1/3

**Bài 9:**

a = 1573; b = 308

Đặt (A1, A2, A3) = (1, 0, 1573)

(B1, B2, B3) = (0, 1, 308)

Q = A3/B3 = 5

Đặt (A1, A2, A3) = (0, 1, 308)

(B1, B2, B3) = (1, -4, 33)

Q = 9

(A1, A2, A3) = (1, -4, 33)

(B1, B2, B3) = (-9, 37, 11)

Q = 3

(A1, A2, A3) = (-9,37,11)

(B1, B2, B3) = (28, -115,0)

Vì B3 = 0 nên UCLN (1573,308) = A3 = 11

**Bài 10:**

**3^22 mod 23 =?**

Thuật toán:

a = 3; k=22; n =23

ki = 10110; t=4

Gán b = 1; nếu k = 0 return 1;

Gán A = a; nếu ki = 1 => b = a;

For (i=0; i<=t; i++)

A = A^2 mod n;

Nếu ki=1 => b = A.b mod n;

Return b;

Bảng mô tả các bước trên:

i: 0 1 2 3 4

ki: 0 1 1 0 1

A: 3 9 12 6 13

b: 1 9 16 16 1

Vậy 3^22 mod 23 = 1

**Bài 11:**

Tính các căn bậc 2 của 12 mod 37

a = 12, p = 37 (p = 5 mod 8)

-Tính Legendre (12/37)

(12/37) = (4/37) \* (3/37) = (2/37) ^ 2 \* (3/37)

= (-1) ^ 2 \* 1 = 1

=> d = 12 ^ (37-1)/4 mod 37 = 12 ^ 9 mod 37

= (12 ^ 3) ^ 3 mod 37 = 1

Vậy r = 12 ^ (37+3)/8 mod 37 = 12 ^ 5 mod 37

= 7

=> -r = -7

Vậy các căn bậc 2 của 12 mod 37 là (7, -7)

**Bài 12:**

Phi (19) = 19-1 = 18 = 2\*3\*2

Tìm các phần tử nguyên thủy sao cho:

X ^ (18/2) mod 37! = 1 <=> x ^ 9 mod 37! = 1

X ^ (18/3) mod 37! =1 x ^ 6 mod 37! = 1

Xét x = 2 <=> 2 ^ 9 mod 37 = 31! = 1

2 ^ 6 mod 37 = 27! = 1

=> 2 là phần tử nguyên thủy của Z19

Đế UCLN (i, phi (19)) = 1 thì i thuộc Z18;

Z18 = {1,5,7,11,13,17}

2 ^ 1 mod 19 = 2;

2 ^ 5 mod 19 = 13

2 ^ 7 mod 19 = 14;

2 ^ 11 mod 19 = 15;

2 ^ 13 mod 19 = 3;

2 ^ 17 mod 19 = 10;

Vậy các phần tử nguyên thủy của nhóm nhân Z19 là {2,3,10, 13, 14, 15}

**Bài 13**:

Tìm phần tử nghịch đảo của 3 trong 731

Gọi x là phần tử nghịch đảo của 3; Ta có:

3x = 1 (mod 31)

<=> 3x - 1 = 31k (k=1,2,3...)

<=> x = 21

**Bài 15**:

Tính phi (490); phi (768)

a/ phi (490)

490 = 2 \* 5 \* 7 ^ 2

Phi (490) = 490 \* (1 - 1/2) \* (1 - 1/5) \* (1-1/7) = 168

b/ phi (768)

768 = 2 ^ 8 \*3

Phi (768) = 768 \* (1 - 1/2) \* (1 - 1/3) = 256

**Bài 16**:

Giải hệ PT đồng dư:

5x = 20 mod 6

6x = 6 mod 5

4x = 5 mod 77

x = 4 mod 6 (1)

<=> x = 1 mod 5 (2)

x = 3 mod 7 (3)

M = 6 \* 5 \* 7 = 210;

M1 = 7 \* 5 = 35;

M2 = 6 \* 7 = 42;

M3 = 6 \* 5 = 30;

35y1 = 4 mod 6 <=> y1 = 2

42y2 = 1 mod 5 <=> y2 = 3

38y3 = 3 mod 7 <=> y3 = 5

=> x = M1 \* y1 + M2 \* y2 + M3 \* y3 mod M

= 346 mod 210

= 136 mod 210

= 136

**Bài 17:**

Dùng Euclide mở rộng để tính:

**a/ 17 ^ (-1) mod 101**

Đặt (A1, A2, A3) = (1, 0, 101)

(B1, B2, B3) = (0, 1, 17)

Q = 5

(A1, A2, A3) = (0,1,17)

(B1, B2, B3) = (1, -5,16)

Q = 1

(A1, A2, A3) = (1, -5,16)

(B1, B2, B3) = (-1,6,1)

Vì B3 = 1 nên 17 ^ (-1) mod 101 = B2 = 6

**b/ 357 ^ (-1) mod 1234**

Đặt (A1, A2, A3) = (1,0,1234)

(B1, B2, B3) = (0,1,357)

Q = 3

(A1, A2, A3) = (0,1,357)

(B1, B2, B3) = (1, -3,163)

Q = 2

(A1, A2, A3) = (1, -3,163)

(B1, B2, B3) = (-2,7, 31)

Q = 5

(A1, A2, A3) = (-2,7,31)

(B1, B2, B3) = (11, -38, 8)

Q = 3

(A1, A2, A3) = (11, -38,8)

(B1, B2, B3) = (-35,121,7)

Q = 1

(A1, A2, A3) = (-35, 121,7)

(B1, B2, B3) = (-24, -159, 1)

Vì B3 = 1 nên 357 ^ (-1) mod 1234 = B2 = -159

**c/ 3125 ^ (-1) mod 9987**

Đặt (A1, A2, A3) = (1,0,9987)

(B1, B2, B3) = (0,1,3125)

Q = 3

(A1, A2, A3) = (0,1,3125)

(B1, B2, B3) = (1, -3, 612)

Q = 5

(A1, A2, A3) = (1, -3,612)

(B1, B2, B3) = (-5, 16, 65)

Q = 9

(A1, A2, A3) = (-5,16,65)

(B1, B2, B3) = (46, -147, 27)

Q = 2

(A1, A2, A3) = (46, -147, 27)

(B1, B2, B3) = (-97,310,11)

Q = 2

(A1, A2, A3) = (-97,310,11)

(B1, B2, B3) = (240, -767,5)

Q = 2

(A1, A2, A3) = (240, -767,5)

(B1, B2, B3) = (-577,1844,1)

Vì B3 = 1 nên 3125 ^ (-1) mod 9987 = B2 = 1844

**Bài 1:**

Dùng thuật toán vét cạn, tìm được khóa k = 4

PSZI QIERW RIZIV LEZMRK XS WEC CSY EVI WSVVE

từ đó tìm được bản rõ:

LOVE MEANS NEVER HAVING TO SAY YOU ARE SORRY