**Họ và tên: Nguyễn Bảo Đạt**

**MSV: AT141010**

**Lớp: AT14L**

**Môn học: Cơ sở Lý thuyết Mật mã**

**CHƯƠNG 2**

**Bài 1:**

Sử dụng thuật toán vét cạn, ta tìm được khóa k = 4 từ đó áp dụng tìm bản rõ là:

LOVE MEANS NEVER HAVING TO SAY YOU ARE SORRY

**Bài 2:**

a/Mã thay thế: EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCKQPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCGOIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZUGFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNSACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNCIACZEJNCSHFZEJZEGMXCYHCJUMGKUCY

Đề cho F -> w (5 -> 22)

Ký tự xuất hiện nhiều nhất là C với 33 lần

Theo hàm tạo mã: y = ax+b (mod26)

Gỉả sử C -> e (2 -> 4);

Ta có hệ phương trình:

5 = 22a + b

2 = 4a + b

Vô nghiệm nên loại TH này

Gỉả sử C -> t (2 -> 19);

Ta có hệ phương trình:

5 = 22a + b <=> a = 1

2 = 19a + b b = 9

Vì UCLN(1,26) = 1 nên có thể xem K(1,9) là khóa

=> Hàm giải mã: x = y - 9 (mod 26)

=> Thu được bản rõ: VDXCFJLUTXUETLJNPJWYEJWTPBUGLDCN

XPZTFOPJZGATBHGBLXBDXFCZTXZETXRTBJEZJRTPBQJT

.....

d/Mã chưa xác định: BNVSNSIHQCEELSSKKYERIFJKXUMBGYKAMQLJTYAVFBKVTDVBPVVRJYYLAOKYMPQSCGDLFSRLLPROYGESEBUUALRWXMMASAZLGLEDFJBZAVVPXWICGJXASCBYEHOSNMULKCEAHTQOKMFLEBKFXLRRFDTZXCIWBJSICBGAWDVYDHAVFJXZIBKCGJIWEAHTTOEWTUHKRQVVRGZBXYIREMMASCSPBNLHJMBLRFFJELHWEYLWISTFVVYFJCMHYUYRUFSFMGESIGRLWALSWMNUHSIMYYITCCQPZSICEHBCCMZFEGVJYOCDEMMPGHVAAUMELCMOEHVLTIPSUYILVGFLMVWDVYDBTHFRAYISYSGKVSUUHYHGGCKTMBLRX

Ký tự xuất hiện nhiều nhất là: L,S(23); Y(22); M,V(21);...

Theo hàm tạo mã: y = ax+b (mod26)

Gỉả sử L(11) -> e(4); S(18) -> t(19); Ta có hệ phương trình:

11 = 4a+b <=> a = 23

18 = 19a+b b = 23

Vì UCLN(a,26) = 1 => K(23,23) có thể là khóa

của bản mã

Hàm giải mã: x = 23^(-1)(y-23) (mod26)

Bản rõ: CMS.....

c/Mã Affine: KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUPKRIOFKPACUZQEPBKRXPEIIEABDKPBCPFCDCCAFIEABDKPBCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFFERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERKIVKSCPICBRKIJPKABI

Thống kê 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)...

Trong tiếng Anh, tần suất xuất hiện của "E" là

cao nhất, tiếp theo là "T, A, O..."

Nên giả sử C=2 -> E=4, B=1 -> T=19

Mục tiêu tìm khóa k(a,b) => Ta có hệ phương trình:

4 = 2a+b (mod 26)

19 = a+b (mod 26)

=> a = 11, b = 8 UCLN(11,26) = 1

=> Có thể xem k(11,8) là khóa

Dùng hàm giải mã: x = 11^-1 \*(y-8) (mod 26)

K: x = 2/11 (mod26)

x = (26k+2)/11 => x = 12 => M

Q: x = 8/11 (mod26)

x = (26k+8)/11 => x = 22 => W

E: x = -4/11 (mod26)

x = (26k-4)/11 => x = 2 => C

.......... => Bản rõ: MWC...

**Bài 4:**

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

HIARRTNUYTUS: 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 phương trình:

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 phương trình:

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:**

ADISPLAYEDEQAUTION:

0 3 8 18 15 11 0 24 4 3 4 16 0 20 19 8 14 13

DSRMSIOPLXLJBZULLM:

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 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,b3)

(k31 k32 k33)

=>Hàm tạo mã y = xK + b => Ta có hệ phương trình:

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 6:**

Bản mã: LMQETXYEAGTXCTUIEWNCTXLZEWUAISPZYVAPEWLMGQWVAXFTGMSQCADAGTXLMDXNXSNPJQSYVAPRIQSMHNOCVAXFV

11 12 16 4 19 23 24 4 0 6 19 23 2 19 20 8 4 22 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 13 15 9 16 18 24

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

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

(T,X): 3

(E,W),(L,M),(V,A): 2

Đặt K = (k11 k12)

(k21 k22)

\*Gỉa sử cặp (T,X) là (T,H) và (E,W) là (S,T)

19 = 19\*K11 + 7\*K21

23 = 19\*K12 + 7\*K22

4 = 18\*K11 + 19\*K21

22 = 18\*K12 + 19\*K22

=> K = (25 23) => Không tồn tại K^(-1) => loại

(26 4)

\*Gỉả sử cặp (T,X) là (T,H) và (L,M) là (S,T), ta có hệ phương trình:

19 = 19\*K11 + 7\*K21

23 = 19\*K12 + 7\*K22

11 = 18\*K11 + 19\*K21

12 = 18\*K12 + 19\*K22

<=> K11=24 K21=23 => K = (24 15) => K^(-1) = det(K)^(-1)\*K

K12=15 K22=22 (23 22)

=> K^(-1) = (22 11)

(3 24)

**Bài 7:**

a/ Cách giải:

* Chia các 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, n+2\*n,....,n+(m-1)\*n

b/ Cho mã MAAMRARUYIQTENCTORAHROYWDDSOYEQUARRGDDERNOGW

Có 42 ký tự, ta có thể chia thành các trường hợp: 2x21, 21x2, 3x14, 14x3, 6x7, 7x6. Sử dụng thuật toán vét cạn, tìm được 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