SC402: Introduction to Cryptography

2/9/2022

Assignment 1

Prof. Manish K. Gupta

Details:

Name: Madhvi Padshala

ID: 201901171

Q.1 Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a Shift Cipher:

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD

⇨ We have No. of possible keys are 26 (0<=k<=25)

K	Decrypted Ciphertext
0	BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD
1	ADDZJEXCIWTPXGXIHPQXGSXIHPEAPCTXIHHJETGBPC
2	ZCCYIDWBHVSOWFWHGOPWFRWHGODZOBSWHGGIDSFAOB
3	YBBXHCVAGURNVEVGFNOVEQVGFNCYNARVGFFHCREZNA
4	XAAWGBUZFTQMUDUFEMNUDPUFEMBXMZQUFEEGBQDYMZ
5	WZZVFATYESPLTCTEDLMTCOTEDLAWLYPTEDDFAPCXLY
6	VYYUEZSXDROKSBSDCKLSBNSDCKZVKXOSDCCEZOBWKX
7	UXXTDYRWCQNJRARCBJKRAMRCBJYUJWNRCBBDYNAVJW
8	TWWSCXQVBPMIQZQBAIJQZLQBAIXTIVMQBAACXMZUIV
9	SVVRBWPUAOLHPYPAZHIPYKPAZHWSHULPAZZBWLYTHU
10	RUUQAVOTZNKGOXOZYGHOXJOZYGVRGTKOZYYAVKXSGT
11	QTTPZUNSYMJFNWNYXFGNWINYXFUQFSJNYXXZUJWRFS
12	PSSOYTMRXLIEMVMXWEFMVHMXWETPERIMXWWYTIVQER
13	ORRNXSLQWKHDLULWVDELUGLWVDSODQHLWVVXSHUPDQ
14	NQQMWRKPVJGCKTKVUCDKTFKVUCRNCPGKVUUWRGTOCP
15	MPPLVQJOUIFBJSJUTBCJSEJUTBQMBOFJUTTVQFSNBO
16	LOOKUPINTHEAIRITSABIRDITSAPLANEITSSUPERMAN
17	KNNJTOHMSGDZHQHSRZAHQCHSRZOKZMDHSRRTODQLZM
18	JMMISNGLRFCYGPGRQYZGPBGRQYNJYLCGRQQSNCPKYL
19	ILLHRMFKQEBXFOFQPXYFOAFQPXMIXKBFQPPRMBOJXK
20	HKKGQLEJPDAWENEPOWXENZEPOWLHWJAEPOOQLANIWJ
21	GJJFPKDIOCZVDMDONVWDMYDONVKGVIZDONNPKZMHVI
22	FIIEOJCHNBYUCLCNMUVCLXCNMUJFUHYCNMMOJYLGUH
23	EHHDNIBGMAXTBKBMLTUBKWBMLTIETGXBMLLNIXKFTG
24	DGGCMHAFLZWSAJALKSTAJVALKSHDSFWALKKMHWJESF
25	CFFBLGZEKYVRZIZKJRSZIUZKJRGCREVZKJJLGVIDRE

Key 16: Look up in the air, it's a bird, it's a plane, it's a superman is our answer.

Here is the Code for the same:

```
string str;
cin>>str;
for(inr i=0;i<=25;i++)
{
    for(int j=0;j<str.length();j++)
    {
        if(str[j]-i>='A') cout<<(char)(s[j]-i);
        else cout<<(char)(s[j]+26-i);
    }
}
```

Q.2 Determine the number of keys in an Affine Cipher over Zm for m = 30, 100 and 1225.

➔ M=30 →Phi(30)= 2*3*5 = (2-1)*(3-1)*(5-1) = 8

So Affine cipher is, 8*30 = 240 keys

➔M=100→ Phi(100)= 2*2*5*5= (4-2)*(25-5) = 40

So affine cipher is 40*100 = 4000 keys

➔M=1225→ Phi(1225)= 5*5*7*7 = (25-5)*(49-7) = 840

So affine cipher is 840*1225=102900 keys

Q.3 List all the invertible elements in Zm for m = 28, 33 and 35.

➔Condition for the element a belongs to Zm is invertible , gcd(a,m)=1.

So Z_{28} : 1,3,5,9,11,13,15,17,19,23,25,27

Z_{33} : 1,2,4,5,7,8,10,13,14,16,17,19,20,23,25,26,28,29,31,32

Z_{35} : 1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34

Q.4

(a) Suppose that π is the following permutation of $\{1,\ldots,8\}$:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

Compute the permutation π^{-1} .

Ans. Here $(pi)^{-1}$ will be 2 4 6 1 8 3 5 7

B) Decrypt the following ciphertext, for a Permutation Cipher with m = 8, which was encrypted using the key π:

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM.

Ans:

T G E E M N E L(1 2 3 4 5 6 7 8) → G E N T L E M E (2 4 6 1 8 3 5 7)

N N T D R O E O(1 2 3 4 5 6 7 8) → N D O N O T R E (2 4 6 1 8 3 5 7)

A A H D O E T C(1 2 3 4 5 6 7 8) → A D E A C H O T (2 4 6 1 8 3 5 7)

S H A E I R L M(1 2 3 4 5 6 7 8) → H E R S M A I L (2 4 6 1 8 3 5 7)

⇨ Decrypted text is: **GENTLEMENT DO NOT READ EACH OTHERS MAIL**

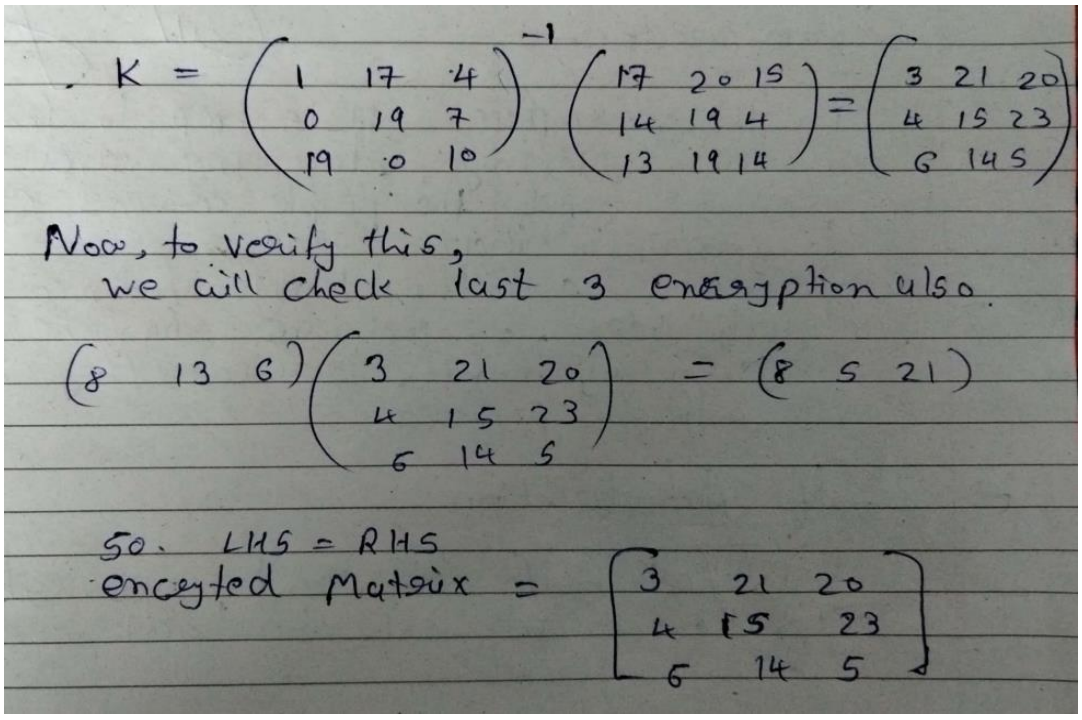
Q.5 Plain text: breathtaking , Cipher text: RUPOTENTOIFV

where the Hill Cipher is used (but m is not specified). Determine the encryption matrix.

➔So m is not specified we assume it 3x3

We can find the encryption matrix.

1. Consider the first element of both text and by using them find encryption matrix.
2. After that try that encrypted matrix as a key on other plain text and compare with cipher text.



Q.6 Modification in Hill cipher is given in the Question, Suppose Oscar has learned that the plaintext: adisplayedequation - is encrypted to give the ciphertext: DSRMSIOPLXLJBZULLM - and Oscar also knows that m = 3. Determine the key, showing all computations.

➔We get,

X1= (0,3,8) X2=(18,15,11) X3= (0,24,4)

X4=(3,4,16) X5=(20,0,9) X6=(8,14,13)

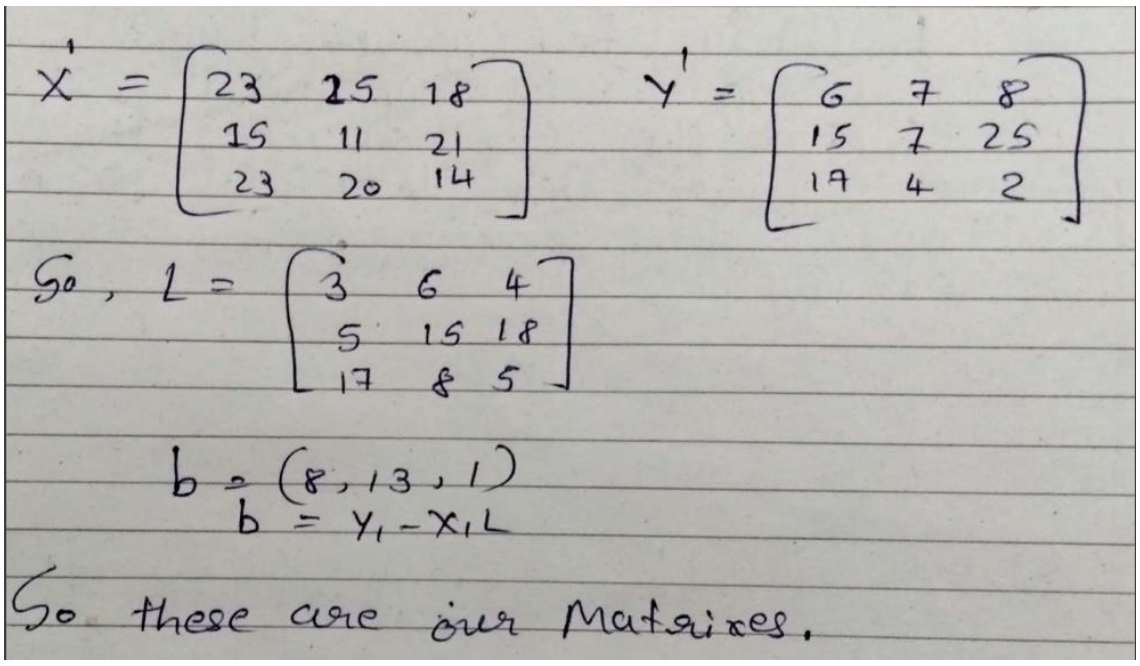
Y1= (3,18,17) Y2=(12,18,8) Y3= (14,15,11)

Y4=(23,11,9) Y5=(1,25,20) Y6=(11,11,12)

For 1 ≤ I ≤ 6 , it holds that Yi = Xi*L + b. Therefore, for1 ≤ I ≤ 3,

we have Yi-y4 = (Xi-X4)*L.

We form the 3 x 3 matrix Y' having rows Yi-Y4 (1 ≤ I ≤ 3); and then L= (X')-1 Y'. once we found L, we can determine b from the equation b= y1-XiL.



Q.7 Decrypt the following ciphertext, obtained from the Autokey Cipher, by using exhaustive key search:

MALVVMAFBHBUQPTSOXALTGVWWRG.

A	MOXYXPLUHABTXSBRXAALIYXZXUM
B	LPWZWQKVGBAUWTASWBZMHZWAWVL

C	KQVAVRJWFCZVVUZTVCYNGAVBVWK
D	JRUBUSIXEDYWUVYUUDXOFBUCUXJ
E	ISTCTTHYDEXXTWXVTEWPECTDTYI
F	HTSDSUGZCFWYSXWWSFVQDDSESZH
G	GURERVFABGVZRYVXRGURCERFRAG
H	FVQFQWEBAHUAQZUYQHTSBFQGQBF
I	EWPGPXDCZITBPATZPISTAGPHPCE
J	DXOHOYCDYJSCOBSAOJRUZHOIODD
K	CYNINZBEXKRDNCRBNKQVYINJNEC
L	BZMJMAAFWLQEMDQCMLPWXJMKMFB
M	AALKLBZGVMPFLEPDLMOXWKLLLGA
N	ZBKLKCYHUNOGKFOEKNNYVLKMKHZ
O	YCJMJDXITONHJGNFJOMZUMJNJIY
P	XDINIEWJSPMIIHMGIPLATNIOIJX
Q	WEHOHFVKRQLJHILHHQKBSOHPHKW
R	VFGPGGULQRKKGJKIGRJCRPGQGLV
S	UGFQFHTMPSJLFKJJFSIDQQFRFMU
T	THEREISNOTIMELIKETHEPRESENT
U	SIDSDJRONUHNDMHLDUGFOSDTDOS
V	RJCTCKQPMVGOCNGMCVFGNTCUCPR
W	QKBUBLPQLWFPBOFNBWEHMUBVBQQ
X	PLAVAMORKXEQAPEOAXDILVAWARP
Y	OMZWZNNSJYDRZQDPZYCJKWZXZSO
Z	NNYXYOMTIZCSYRCQYZBKJXYYYTN

Key T Produce meaning full sentence: THERE IS NO TIME LIKE THE PESENT

Here is the code for the same:

```
string msg;
cin>>msg;
for(int i=0;i<26;i++)
{
    char key=i+'A';
    string currentKey;
    currentKey+=key;
    string decryptMsg = "";
    cout<<key<<": ";
    for (int x = 0; x < msg.length(); x++) {
        int get1 = 'A'+msg[x];
        int get2 = 'A'+currentKey[x];
        int total = (get1 - get2) % 26;
        total = (total < 0) ? total + 26 : total;
        decryptMsg += total+'A';
        currentKey += total+'A';
    }
    cout<<decryptMsg;
}
```