Advanced Cryptography

Assignment #1

1. **Evaluate the following**

   a. **7503 mod 81** => 51

   b. -7503 mod 81 =>30

   c. 81 mod 7503 =>81

   d. -81 mod 750 =>7422

2. **Use exhaustive key search to decrypt the following cipher text, which was encrypted using shift cipher:**
   "BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD "

Ans: Here we apply 0-25 key for decrypting the given cipher text. If we found meaningful text then we stop decrypting. For decryption we use following formula,

i.e, $d_k(x)=(y-k) \bmod 26$

First we convert cipher text into corresponding integer sequence which are,

```
 1  4  4  0 10  5 24  3  9 23 20 16 24  7 24  9  8 16 17 24  7
19 24  9  8 16  5  1 16  3 20 24  9  8  8 10  5 20  7  2 16  3
```

Next we subtract 1 from each value and apply modulo 26 then we get ,

```
 0  3  3 25  9  4 23  2  8 22 19 15 23  6 23  8  7 15 16 23
 6 18 23  8  7 15  4  0 15  2 19 23  8  7  7  9  4 19  6  1 15  2
```

Finally we convert the sequence of integers to alphabetic characters. They are,

addzjexciwtpxgxihpqxgsxihpeapctxihhjetgbpc

Similarly apply key 2,3,4.....

zccyidwbhvsowfwhgopwfrwhgodzobswhggidsfaob
ybbxhcvagurnvevgfnoveqvgfncynarvgffhcrezna
xaawgbuzftqmudufemnudpufembxmzqufeegbqdymz
.
.
.
.
.

At last applying key as 16 i.e, 'Q' then we get,

lookupintheairitsabirditsaplaneitssuperman

That's why the key is 16(Q) and plain text is

look up in the air its a bird its a plane its superman

3. Determine the number of key in affine cipher over Zm for m=30, 100 and 1225.

Ans:

$30 = 2 \times 3 \times 5$, so $\varphi(30) = 1 \times 2 \times 4 = 8$. The affine cipher over Z_{30} and has $30 \times 8 = 240$ keys.

$100 = 2^2 \times 5^2$, so $\varphi(100) = (2^2 - 2)(5^2 - 5) = 40$. The affine cipher over Z_{100} and has $100 \times 40 = 4000$ keys.

$1225 = 5^2 \times 7^2$, so $\varphi(1225) = (5^2 - 5)(7^2 - 7) = 840$. The affine cipher over Z_{1225} and has $1225 \times 840 = 1029000$ keys.

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}.

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

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM.

Ans:

a)=> For π^{-1} we should interchange the given two rows and rearranging the column.

First interchanging given rows.

π (x)	4	1	6	2	7	3	8	5
x	1	2	3	4	5	6	7	8

Now rearrange into ascending order

π (x)	1	2	3	4	5	6	7	8
π^{-1}(x)	2	4	6	1	8	3	5	7

b)=> given cipher is "TGEEMNELNNTDROEOAAHDOETCSHAEIRLM". Here m=8 so we partition into group of 8 letter.

TGEEMNEL| NNTDROEO | AAHDOETC | SHAEIRLM

Now each letter in group is replace according permutation π(x). Then we get

GENTLEME | NDONOTRE | ADEACHOT | HERSMAIL

The finial plain text is, "gentle men do not read each others mail"

5. **Here is how we might cryptanalyze the Hill Cipher using a cipher text only attack. Suppose that we know that m=2. Break the cipher text into blocks of length two letters (diagrams). Each such diagrams are the encryption of a plain text diagrams and assume it in the encryption of a common diagrams for example, TH or ST. Each such guess, proceed as I the known plaintext attack, until the correct encryption matrix is found.**

   Here is a sample of cipher text to decrypt using this method

   LMQETXYEAGTXCTUIEWNCTXLZEWUAISPZYVAPEWLMGQWYA
   XFTCJMSQCADAGTXLMDXNXSNPJQSYVAPRIQSMHNOCVAXFV

Ans: Not competed

6. **Suppose we are told that the plaintext "breathtaking" yields the Ciphertext "RUPOTENTOIFV" where the Hill Cipher is used (but m is not specified). Determine the encryption matrix.**

Ans: The given plaintext is "breathtaking".

The cipher text is "RUPOTENTOIFV"

We know encryption method for hill cipher,

C=K*P

Where K is encryption matrix. Now encryption key K can be calculate by,

$K= P^{-1} *C$

P and C matrix can be formed by integer sequence of alphabet. Here we take only 9 alphabet for matrices.

$$P = \begin{bmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{bmatrix} \text{ and } C = \begin{bmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{bmatrix}$$

Now,

$K = P^{-1} * C$

$$= \begin{bmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{bmatrix} * \begin{bmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{bmatrix}$$

That's why encryption matrix is $\begin{bmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{bmatrix}$

7. **Decrypt the following Ciphertext, obtained from theAutokey Cipher, by using exhaustive key search:**

MALVVMAFBHBUQPTSOXALTGVWWRG

Ans: Here we apply 0-25(A-Z) key for decrypting the given cipher text. If we found meaningfultext then we stop decrypting. For decryption we use following formula,

i.e, $d_z(y)=(y-z) \bmod 26$

Where z is the set of key stream and the initial value i.e, z_1 is key(K) itself.

First we convert cipher text into corresponding integer sequence which are,

12 0 11 21 21 12 0 5 1 7 1 20 16 15

19 18 14 23 0 11 19 6 21 22 22 17 6

We use key 0 i.e, 'A' for decipher the cipher text. First we generate key stream 'z' for the decryption. So that initial character of keystream is key itself.

Z = 0

Now we subtract last value of keystream from cipher text character and apply module 26. Then second value would be,

Z = 0 12

Again subtract last value of keystream i.e, 12 from another value of the cipher text i.e, 0 and apply module 26. Then we get

Z= 0 12 14 (where 0-12 = -12 mod 26 => 14)

Similarly, applying same method for all character of given cipher text then we get keystream as

0 12 14 23 24 23 15 11 20 7 0 1 19 23

18 1 17 23 0 0 11 8 24 23 25 23 20 12

Next we subtract keystream value from each values of cipher text and apply modulo 26 then we get ,

12 14 23 24 23 15 11 20 7 0 1 19 23

18 1 17 23 0 0 11 8 24 23 25 23 20 12

Finally we convert the sequence of integers to alphabetic characters. They are,

moxyxpluhabtxsbrxaaliyxzxum

Similarly apply key 1, 2, 3,.....

zccyidwbhvsowfwhgopwfrwhgodzobswhggidsfaob
ybbxhcvagurnvevgfnoveqvgfncynarvgffhcrezna
xaawgbuzftqmudufemnudpufembxmzqufeegbqdymz
.
.
.
.
.

At last applying key 19 i.e, 'T' then we get,

lookupintheairitsabirditsaplaneitssuperman

That's why the key is 19(T) and plain text is

look up in the air its a bird its a plane its superman