# Assignment 3

● Graded

**Group**

HRISHITA AGRAWAL
RAJ AGRAWAL
RAHUL NARAYAN

✎ View or edit group

**Total Points**

**48 / 50 pts**

**Question 1**

## Commands

**5** / 5 pts

✓ **+ 5 pts** Correct (go enter pluck/pick back give back back thrnxxtzy read)

**+ 0 pts** Incorrect

**− 2 pts** Unnecessary story of commands presented but not a list of commands

**Question 2**

## Cryptosystem

**8** / 10 pts

✓ **+ 10 pts** Correct (monoalphabetic substitution and permutations cipher with block length 5)

**− 2 pts** Not mentioning monoalphabetic

✓ **− 2 pts** Not mentioning block length

**+ 0 pts** Incorrect

Question 3

## Analysis

Resolved **30** / 30 pts

✓ **+ 3 pts** Frequency analysis

✓ **+ 2 pts** Figured out the cryptosystem

✓ **+ 2 pts** Reason behind choosing block size 5

✓ **+ 5 pts** Identified permutation map. Permutation (Encryption) key: 43512 or 32401(when 0 is the first index) or Decryption Key: 45213.

✓ **+ 8 pts** Detailed cryptanalysis

✓ **+ 5 pts** Substitution map

✓ **+ 5 pts** Consider all cases, like uppercase, lower case and special characters, space etc.

**+ 0 pts** Wrong answer.

**− 2 pts** Just mentioned frequency analysis but the analysis isn't provided.

Regrade Request **Submitted on: Apr 04**

Respected sir,
Sir in the Code section I provided my code which is in c++ and that automatically remove special characters like space from our ciphertext so we didn't write that in this as we already mentioned our code.
So please regrade this once.
Thank you

updated

Reviewed on: Apr 06

Question 4

## Password

**5** / 5 pts

✓ **+ 5 pts** Correct (the_magic_of_wand)

**+ 0 pts** Incorrect

Question 5

## Codes

**0** / 0 pts

✓ **+ 0 pts** Correct

Question 6

## Group name

**0** / 0 pts

✓ **+ 0 pts** Correct

**+ 0 pts** Incorrect

## Q1 Commands

**5 Points**

List the commands was used in this level?

1.enter 2.enter 3.pick 4.back 5.give
6.back 7.back 8.thrnxxtzy 9.read

## Q2 Cryptosystem

**10 Points**

What cryptosystem was used in the game to reach the password?

Monoalphabetic Substitution-Permutation Cryptosystem.
in this type of cryptosystem , the plaintext firstly converted into ciphertext using monoalphabetic substitution then permutation is applied to that cipher( which was obtained after substitution ) using a key by breaking it into blocks. and then final ciphertext is obtained.

## Q3 Analysis

**30 Points**

What tools and observations were used to figure out the cryptosystem and the password? (Explain in less than 1000 lines)

First, we analysed the frequency of letters of cipher text, and we found that the frequencies of letters of cipher text are in the same proportions as that in general English literature. Then we changed the letters of high frequency in the cipher text(q, v, a) with letters of high frequency in general English literature(e, t, a). By mapping these 3 letters we got nothing useful, and by this we concluded that along with substitution cryptosystem, there is also some other cryptosystem used to encrypt the plain text. So we calculated frequencies of bigrams(fv) and trigrams(xja) which turn out to be very low and thus there has to be permutation(transposition) present. Then we thought that if some key was used to encrypt the plaintext and if some word was repeating in plaintext and it is also repeating in cipher text then the number of letters between these bigram and trigram by including one bigram or trigram would be the multiple of that key. And in this we observed that the no. of letters between 3 fv's(2 letter word) are 35 and 45 respectively and that of xja is 80. These all are multiple of 5. So by this we concluded that the key has to be of 5 numbers. Then we observed some one letter words(x and y) in cipher text. And according to general English literature single letter words are 'a' and 'i'. And we also know that 'a' has very high frequency. So we assumed that it is 'a' in that two places in the plaintext. Then we divided the cipher text into blocks of five letters each as our key length is 5. Then we observed the blocks in which those x and y were included and these were 'pqcsy' and 'quwxd' respectively. Now if both x and y places have to be for 'a' then these blocks should contain a common letter in them and in this case it was q. So 'q' have to be 'a'. And the frequency of 'q' in cipher text is very similar to that of 'a' in general English text. So our assumption of neglecting 'i' is justified. according to permutation cryptosystem we know that the letter 'q' of 'pqcsy' will be in place of 'y' in plaintext.so, the key for encryption has 2'nd number as 5 and similarly letter 'q' of 'quwxd' will be in place of letter 'x' in plaintext. So, key must have 1'st number as 4. so now we have the first two number of the key as '45'.and now we have to find the last three numbers of the key. So now we analysed the block 'fvxja' and according to the key till we have find this block will be of the form '_ _ _fv' and the letters 'x', 'j' and 'a' can be of any combination on this 1st , 2nd and 3rd place. So according to frequency analysis the letter v in cipher text must be e in plaintext. And as the last three letters of this block is a separate 3 letter word and the last letter of this word is 'e' so there is a high probability that the word might be 'the' or 'are,' but it cannot be 'are' as the block does not contain the letter 'q' which is 'a' in plain text. And according to frequency analysis, the probability of occurrence of 'a' in ciphertext is very similar to that of probability of occurrence of 't' in general English text. So the word has to be 'the'. And accordingly 'f' maps to 'h' and it is also satisfying frequency analysis. So the block will be of form '_ _ afv'. And accordingly we get the key like '45_ _3'. So the decryption key is '43512'. We observed some blocks containing 'f', 'a' 'v' letters as 'afv' is 'the'. Then we found a block 'lhfav' and from cipher text 'lhf' is a 3 letter independent word so it should be 'the' after decryption or we can say 'afv' after permutation. So according to this the key will be '45213'. So now according to the key we arranged the ciphertext. So now our ciphertext is converted into perfect monoalphabetic substitution cipher. Now we have to apply frequency analysis to get the plaintext.

So, the mapping is like that

a=t

b=v

c=i

d=u

e=c

f=h

g=g

h=p

i=q

j=b

k=z (most probably as k appers in only one word which is repeated twice in cipher and it appears that it is name of someone so we left with three word only i.e. x ,z, j so, it should be z )

l=s

m=k

n=r

p=d

q=a

r=w

s=f<br>
t=l<br>
u=m<br>
v=e<br>
w=o<br>
x=y<br>
y=n<br>
Letters 'z' and 'o' are not present in the ciphertext.<br>
so anyone of the z and o match with x and other match with j.

So, the final plaintext is-<br>
Breaker of this code will be blessed by the squeaky spirit residing in the hole go ahead, and find a way of breaking the spell on him cast by the evil zaffar. the spirit of the caveman is always with you. find the magic wand that will let you out of the caves. it would make you a magician ,no less than zaffar!<br>
speak<br>
the password the_magic_of_wand to go through.

## Q4 Password

**5 Points**

What was the final command used to clear this level?

the_magic_of_wand

## Q5 Codes

**0 Points**

Upload any code that you have used to solve this level.

**raj8.cpp** Download

```

#include <iostream>
using namespace std;
//code for obtaining the cipher without permutation
//in this we used the decrypting key '43512' to decrypt it.
int main()
{
    int n=0;
    char a[336];
    char b[336];
    for(int i=0;i<336;i++)
    {
        cin>>a[i];
    }
    for(int i=0;i<336;i++){

        b[n+0]=a[n+3];
        b[n+1]=a[n+2];
        b[n+2]=a[n+4];
        b[n+3]=a[n+0];
        b[n+4]=a[n+1];
        n+=5;
    }

for(int i=0;i<336;i++)
    {
        cout<<b[i];
        if((i+1)%5==0){
            cout<<" ";
        }
    }
    return 0;
}
```

## Q6 Group name

**0 Points**

encrypted_team