Assignment 1

● Graded

Group

KUNAL SAINI
KUSHAL MAHESHWARI
SHARATH KUMAR V

View or edit group

Total Points

40 / 50 pts

Question 1

Commands

5 / 5 pts

✓ **+ 5 pts** Specifying the correct set of commands

+ 0 pts Correct

Question 2

Cryptosystem

3 / 5 pts

✓ **+ 3 pts** The nature of the substitution cipher is not mentioned, Substitution cipher could be of Monoalphabetic or Polyalphabetic.

+ 5 pts Correct Cryptosystem

+ 0 pts Incorrect

Question 3

Analysis

Resolved **20** / 25 pts

✓ **+ 10 pts** Using frequency analysis to conclude that its substitution cipher

✓ **+ 5 pts** Step by Step decryption from cipher to plain

+ 5 pts Finding the mapping in the cryptosystem used by analyzing bigrams and trigrams (or small words)

✓ **+ 5 pts** Giving mathematical explanation for the shift in the digits (We obtained the from the plaintext after decrypting it with frequency analysis, which claims that the digits are shifted by "8" places. However, because 8 is a digit, it is obvious that 8 is also encrypted by some shifting. _Assume the number that was shifted to 8 is X. Because X is the key here, we can assert that X is shifted by X places, resulting in 8. The problem is written as follows in mathematical notation: X+X=8mod10 (mod 10 because there are 10 digits only, aka 0,1,2,3,4,5,6,7,8,9). The digits satisfying the above equation is 4 and 9. Without loss of generality, let us assume that X=9. Then the method of decryption tends to find two numbers Y and Z, such that Y+9=0mod10 and Z+9=3mod10. Therefore, leading us Y=1 and Z=4. For this case the decrypted password showed incorrect. So we tried the other value of X=4. Then the method of decryption tends to find two numbers Y and Z, such that Y+4=0mod10 and Z+4=3 mod10. Therefore, leading us as Y=6 and Z=9. For this case the decrypted password is showed correct.)

+ 0 pts incorrect/ Directly using online tool to decipher.

Regrade Request **Submitted on: Feb 15**

I have used bigrams and trigrams to find the mapping in the cryptosystem, yet I have not been awarded marks for it. You can see that I have mentioned the use of the words like 'TeH', 'p', 'THwa' and 'wa' to find my mapping.

No explanation is given for why you chose to replace characters like 'e' with 'h' and 'p' with 'a'. Also, 150 words aren't enough to award 25 marks.

Reviewed on: Feb 15

Question 4

Mapping

7 / 10 pts

✓ **+ 3 pts** Plaintext Space and cipher text space is the set of all strings containing English alphabets, numbers, punctuation marks, and spaces.

− 1 pt No mention of the existence of "digits" in the ciphertext space and plaintext space

− 1 pt No mention of the existence of "punctuation marks" in the ciphertext space and plaintext spcae

✓ **+ 7 pts** The mapping used for alphabets and numbers.

✓ **− 3 pts** Mistakes or missing in mapping of alphabets

− 2 pts Mistakes or missing in mapping punctuation marks

− 2 pts Mistakes or missing in mappings of numbers.

+ 0 pts Incorrect

+ 3 pts mapping only done for alphabets

Mapping of g is missing

Question 5

Password

5 / 5 pts

✓ **+ 5 pts** Correct

+ 0 pts Incorrect

Question 6

Codes

0 / 0 pts

✓ **+ 0 pts** Correct

Question 7

Team Name

0 / 0 pts

✓ **+ 0 pts** Correct

+ 0 pts Incorrect

Q1 Commands

5 Points

List the commands used in the game to reach the first ciphertext.

climb
read
enter
read

Q2 Cryptosystem

5 Points

What cryptosystem was used at this level?

substitution cipher

Q3 Analysis

25 Points

What tools and observations were used to figure out the cryptosystem?

NOTE: Failing to provide proper analysis would result in zero marks for this assignment.

First, we started replacing the two most occurring letters 'y' and 'm' with 'e' and 't' respectively. Then we saw multiple occurrences of 'TeE' (capital letters represent replaced letters). So we replaced 'e' with 'H'. 'p' was a single-letter word, so we tried replacing it with 'a'. Then the first 2 words looked like 'THwa wa' and there was also a combination like 'wa A' the most suitable substitution for 'w' and 'a' was 'i' and 's' respectively. Then we could figure out that the word 'fASSvgsu' must be 'PASSWORD'. Most of the words were decrypted by now, similarly we decrypted the rest of the words.
The message said the digits were shifted by 8 places. This '8' must have also been coded. So we used the equation {(x+x)mod10 = 8} to find x. Which can either be 4 or 9. We used 4 to decode the message and tried it, which turns out to be the correct one.

Q4 Mapping

10 Points

What is the plaintext space and ciphertext space?
What is the mapping between the elements of plaintext space and the elements of ciphertext space? (Explain in less than 100 words)

Letters = {a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z}
Digits = {0,1,2,3,4,5,6,7,8,9}
Special Characters = {' ', '.', ',', '!', '"'}
Plaintext space: {Letters + Digits + Special Characters}*
Ciphertext space: {Letters + Digits + Special Characters}*
where, '+' operator denotes the union of two sets.

One of the possible Mapping {Ciphertext space:Plaintext space} = {a:s, b:v, c:k, d:q, e:h, f:p, q:o, h:n, i:c, j:m, k:l, l:z, m:t, n:u, o:b, p:a, q:j, r:g, s:r, t:f, u:d, v:w, w:i, x:y, y:e, z:x, 0:4, 1:5, 2:6, 3:7, 4:8, 5:9, 6:0, 7:1, 8:2, 9:3, ' ':' ', '.':'.', ',':',', '!':'!', '"':'"'}

Q5 Password

5 Points

What is the final command used to clear this level?

tyRgU69diqq

Q6 Codes

0 Points

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

Download

```cpp
#include <iostream>
#include <vector>
#include <algorithm>
using namespace std;

int main(){

    string test = "Mewa wa mey twsam iepjoys gt mey ipbya. Pa xgn iph ayy, meysy wa hgmewhr gt whmysyam wh mey iepjoys. Agjy gt mey kpmys iepjoysa vwkk oy jgsy whmysyamwhr meph mewa ghy! Mey iguy nayu tgs mewa jyaapry wa p awjfky anoamwmnmwgh iwfeys wh vewie uwrwma epby oyyh aewtmyu ox 8 fkpiya. Mey fpaavgsu wa \"mxSrN03uwdd\" vwmegnm mey dngmya.";

    string test1 = test;

    vector<int> freq(26,0);

    for(int i=0; i<test.size(); i++)
    {
        if('A'<=test[i] && test[i]<='Z')
        test[i] = test[i] - 'A' + 'a';

        freq[ test[i]-'a' ]++;
    }

    for(int i=0; i<freq.size(); i++)
    {
        char k = 'a'+i;
        cout << k << ": " << freq[i] << endl;
    }

    for(int i=0; i<test.size(); i++)
    {
        if(test[i] == 'y')
        test[i] = 'E';
        if(test[i] == 'm')
        test[i] = 'T';
        if(test[i] == 'e')
        test[i] = 'H';
        if(test[i] == 'p')
        test[i] = 'A';
        if(test[i] == 'w')
        test[i] = 'I';
        if(test[i] == 'a')
        test[i] = 'S';
        if(test[i] == 'f')
        test[i] = 'P';
        if(test[i] == 'v')
        test[i] = 'W';
        if(test[i] == 'g')
        test[i] = 'O';
        if(test[i] == 's')
        test[i] = 'R';
        if(test[i] == 'u')
        test[i] = 'D';
        if(test[i] == 't')
        test[i] = 'F';
        if(test[i] == 'n')
        test[i] = 'U';
        if(test[i] == 'd')
        test[i] = 'Q';
        if(test[i] == 'x')
        test[i] = 'Y';
        if(test[i] == 'i')
        test[i] = 'C';
        if(test[i] == 'h')
        test[i] = 'N';
        if(test[i] == 'r')
        test[i] = 'G';
        if(test[i] == 'o')
        test[i] = 'B';
        if(test[i] == 'j')
        test[i] = 'M';
        if(test[i] == 'b')
        test[i] = 'V';
        if(test[i] == 'k')
        test[i] = 'L';
        if('0'<=test[i] && test[i]<='9')
        {
            int k = test[i]-'0';
            k = ((k-4)+10)%10;
            test[i] = '0'+k;
        }

    }

    for(int i=0; i<test1.size(); i++)
    {
        if('a'<=test1[i] && test1[i]<='z')
        test[i] = test[i] - 'A' + 'a';
    }

    cout << test << endl;

    return 0;
```

```

}
```

Q7 Team Name

0 Points

hardwired