Assignment 3

● Graded

Group

KUSHAL MAHESHWARI
KUNAL SAINI
SHARATH KUMAR V
View or edit group

Total Points

45 / 50 pts

Question 1

Commands

Resolved **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

Regrade Request **Submitted on: Apr 04**

We have written exactly the same commands as given in the solution. I don't know why our command list is incorrect. And there is no requirement to write both pluck and pick for any team since using one if it works why will they try to find out the other one. Please re-evaluate this question and let us know if any mistake from our side.

Done.

Reviewed on: Apr 04

Question 2

Cryptosystem

10 / 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

25 / 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.

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?

go enter pluck back give back back thrnxxtzy read

Q2 Cryptosystem
10 Points

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

Substitution-Permutation Cipher. For Substitution - Monoalphabetic Substitution and for permutation - a block size of length 5 was used.

Q3 Analysis
30 Points

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

Note: 1. All capital alphabets correspond to plaintext and all small alphabets correspond to ciphertext.
2. '?' means we have not yet figured that element yet

First, we ran the frequency analysis on the cipher test through which we came to know that substitution was involved as the analysis didn't match the English dictionary. By substituting the most frequent letter with E and the 2nd most frequent letter with T, there appeared a word 'Ep' since in our context there can be no 2 letter word starting with 'E' we get to know that permutation cipher has also been used.

Now observing the ciphertext we find a pattern 'qmnjv' twice and there are 80 words between them. Similarly we can find another pattern 'fvxja' twice, which has 75 words between them. For a pattern to repeat the whole pattern should be in the same block. Let N be the block size, N = t1 + 5 + t2, where t1 is number of letters in the block before the pattern and t2 is the number of letters in the block after the pattern. Let there be k complete blocks between the repetition of the patterns. For 'qmnjv', t2 + (k*N) + t1 + 5 = 85 = p(N), Similarly for 'fvxja' 80 = q(N). Therefore N is a common divisor of 85 and 80. N can be 5 or 1. We eliminate 1 because N>1.

Now since we know N we use known-plaintext attack. We know that the word 'password' must be present at the last sentence of plaintext. So we filter all 8 letter words. In the last sentence there are two 8 letter words 'decgqcwt' and 'lhvqpwr'. We need to check for a word with a similar pattern to the password, that is a repetition of exactly one letter. Since we are permuting it might be possible that the repetitions might be separated. The block corresponding to 'lhvqpwr' are 'llhvq' and 'pawrn'. Therefore, 'lhvqpwr' is also a possible case.

Case 1: 'decgqcwt'
The blocks corresponding to 'decgqcwt' are 'quwxd', 'ecgqc' and 'wtyqy'. Since 'c' is repeating here and 's' is repeating in password we map c->S. Just before this word we have a 1 letter word 'x'. It can't be 'I' as 'I PASSWORD' doesn't make a sense in english dictionary. So we take it as 'A'. Therefore in there must be 'A' in the previous block. 'q' is the only common letter in both of these block.

Therefore we map q->A. Comparing 'ecgqc' with 'ASSWO' and 'quwxd' with'???A?' we can guess that the permutation key can be 31??2/32??1. Now comparing 'ecgqc' and 'ASSWO' there are 2 possiblities e->W,g->O and e->O,g->W. So there are 4 possible keys for permutation 31042/31402/32041/32401. Trying all these keys results in the partial decryption of 'decgqcwt' to '?ASSWOA?'. This case fails as we can't get 'PASSWORD' from '?ASSWOA?'. Therefore, we discard this case.

Case 2: 'lhvqpwr'
The block corresponding to 'lhvqpwr' are 'llhvq' and 'pawrn'. With similar analysis like case 1 we map l->S and q->A. Now compare '?PASS' with 'llhvq', we have 2 possibilities to 'P' that is 'h' or 'v'. Consider the case h->P, by comparing '?PASS' with 'llhvq' and 'quwxd' with'???A?' we the permutation key as 34102. After inverting the permutation in the ciphertext, and mapping the rest of the letters of 'PASSWORD' we find that the partially decrypted ciphertext contains a word 'OADy' which doesn't make any sense in the English dictionary. So we discard this case and take v->P. Consider the case h->P, by comparing '?PASS' with 'llhvq' and 'quwxd' with'???A?' we the permutation key as 34012. We now invert the permutation and map rest of the corresponding letters to get 'PASSWORD'. After this we decrypt rest of the ciphertext as we do in substitution cipher by analysing bigrams, trigrams and so on.

Ciphertext space = {'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', ' ', '.', ',', '!', '_'}
Plaintext space = {'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', ' ', '.', ',', '!', '_'}
Permutation key = {34012}
Mapping = [{Ciphertext:Plaintext}] = [{'a':'t'}, {'b':'v'}, {'c':'i'}, {'d':'u'}, {'e':'c'}, {'f':'h'}, {'g':'g'}, {'h':'p'}, {'i':'q'}, {'j':'b'}, {'k':'z'}, {'l':'s'}, {'m':'k'}, {'n':'r'}, {'o':'j'}, {'p':'d'}, {'q':'a'}, {'r':'w'}, {'s':'f'}, {'t':'l'}, {'u':'m'}, {'v':'e'}, {'w':'o'}, {'x':'y'}, {'y':'n'}, {'z':'x'}, {' ':' '}, {'.':'.'}, {',':','}, {'!':'!'}, {'_':'_'}]

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.

try.cpp Download

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

int main(){

    string test = "qmnjvsa nv wewc flct vprj tj tvvplvl fv xja vqildhc xmlnvc nacyclpa fc gyt vfvw. fv wgqyp, pqq pqcs y wsq rx qmnjvafy cgv tlvhf cw tyl aeuq fv xja tkbv cqnsqs. lhf avawnc cv eas fuqb qvq tc yllrqr xxwa cfy. psdc uqf avrqc gefq pyat trac xwv taa wwd dv eas flcbq. vd trawm vupq quw x decgqcwt, yq yafl vlqs yqklhq! snafq vml lhvqpawr nqg_vfusr_ec_wawy qp fn wgawdgf.";

    vector<int> freq(26,0);
    int t=0;

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

        if('a'<=test[i] && test[i]<='z')
        freq[ test[i]-'a' ]++;

    }

    string test1 = test;

    test1.erase(remove(test1.begin(),test1.end(), ' '), test1.end());
    test1.erase(remove(test1.begin(),test1.end(), '.'), test1.end());
    test1.erase(remove(test1.begin(),test1.end(), '!'), test1.end());
    test1.erase(remove(test1.begin(),test1.end(), ','), test1.end());
    test1.erase(remove(test1.begin(),test1.end(), '_'), test1.end());

    map<char,char> sub;

    sub = {{'a','T'}, {'b','V'}, {'c','I'}, {'d','U'}, {'e','C'}, {'f','H'}, {'g','G'}, {'h','P'}, {'i','Q'}, {'j','B'}, {'k','Z'}, {'l','S'}, {'m','K'}, {'n','R'}, {'o','J'}, {'p','D'}, {'q','A'}, {'r','W'}, {'s','F'}, {'t','L'}, {'u','M'}, {'v','E'}, {'w','O'}, {'x','Y'}, {'y','N'}, {'z','X'}};

    for(int i=0; i<test.size()-5; i++)
    {

        if(('a'<=test[i] && test[i]<='z') && (t+3)<test1.size())
        {
```

```
41              if(t%5==0)
42              test[i] = sub[test1[t+3]];
43              else if(t%5==1)
44              test[i] = sub[test1[t+1]];
45              else if(t%5==2)
46              test[i] = sub[test1[t+2]];
47              else if(t%5==3)
48              test[i] = sub[test1[t-3]];
49              else if(t%5==4)
50              test[i] = sub[test1[t-3]];
51
52              t++;
53          }
54
55      }
56
57      for(int i=test.size()-1; ;i--)
58      {
59          if('A'<=test[i] && test[i]<='Z')break;
60
61          if('a'<=test[i] && test[i]<='z')
62          test[i] = sub[test[i]];
63      }
64
65      cout << test << endl;
66
67      return 0;
68
69  }
```

Q6 Group name

0 Points

hardwired