Q1 Commands
5 Points

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

go, read, enter, read

Q2 Cryptosystem
5 Points

What cryptosystem was used in this level?

Substitution cipher

Q3 Analysis
25 Points

What tools and observations were used to figure out the cryptosystem? (Explain in less than 100 words)

We wrote a program "count.cpp" with the help of which we counted the number of occurences of each of the alphabet in the cipher text. We then peformed frequency analysis manually and through this we found the mapping with which we were able to decrypt the cipher text.

The counts we found were as followed :-
A: 27, B: 2, C:0, D: 3, E: 22, F: 4, G: 14, H: 12, I: 9, J: 7, K: 5, L:0, M: 28, N: 7, O: 7, P: 13, Q:0, R: 5, S: 13, T: 6, U: 6, V: 4, W: 25, X: 3, Y: 36, Z:0.

(NOTE-- For count, we have not distinguished between uppercase and lowercase, so counts are irrespective of Uppercase and Lowercase.)

We observed that some of the alphabets like C, L, Q, Z do not

occur even once in the ciphertext. Another point we observed is that the punctuation marks were not encrypted and are kept as it is.
A hint is given that we have to shift the digits by 8. Now since 8 is itself a digit, so we need to shift 8 first. After shifting 8 by 8 places and considering only digits from 0-9, we find that 8 becomes 6. So the sentence becomes "shift the digits by 6". So in our password, 0 becomes 6, and 3 becomes 9.

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)

Plaintext space and ciphertext space are set of strings that are composed of symbols from a set called the alphabet of definition. Here, the alphabet of definition used is: {'a', 'b', 'c', ..., 'z', ,'A', 'B', ..., 'Z', 0, 1, 2, ..., 9}.

Plaintext space is [a-z,A-Z,0-9] and the ciphertext space is [a-z,A-Z,0-9]. This means that both the spaces consist of strings made up of lowercase and uppercase English alphabets as well as digits from 0 to 9.

The mapping is as following -

p->a , o ->b, i->c, u->d,y->e,t->f,r->g,e->h,w->i,k->l,j->m,h->n,g->o,f->p,d->q,s->r,a->s,m->t,n->u,b->v,x->y,
0->6, 3->9

We can see from above that some digits and alphabets are not mapped because they are not being used in the given cipher-text.

Q5 Password

5 Points

What was the final command used to clear this level?

tyRgU69diqq

Q6 Codes

0 Points

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

count.cpp Download

```cpp
#include<bits/stdc++.h>
using namespace std;

int main()
{
        string s= "wsam ie pjo ysgtm eyipbya .P axg niphay y, mey syw ahgm ewhrg tw hmysyam wh meyiepjo ys .Ag jygtmeyk pmys ie pjo ysavw kkoyjgsy whmy sy amwh rmephmewagh y!Me yigu ynay utg smew ajya apr ywap awjfkya no a mwmnmw ghiwfeyswhve wieuwr wm aepby oyyhae wtmy uox8 fkpiya. Me y fpaavgs uwa mxSrN03u wd dvwmegnmmey dngmya. Mew awameyt";

        map<char, int>m;  //declaring an ordered map for the purpose of hashing



        for(int i=0;i<s.length();i++)
        {
                if((s[i]>='A' and s[i]<='Z') or (s[i]>='a' and s[i]<='z') )  //since the string consists of spaces, numbers and special characters, so we dont want to
                //take them into account, for which we have used this condition
                {
                        if(s[i]>='a' and s[i]<='z')  //we should not distinguih between upper and lower case while frequency analysis.
                        m[s[i]-32]++;
                        else
                        m[s[i]]++;


                }
        }
```

```
25
26
27          int n=m.size();
28
29          cout<<n<<endl;
30
31          for(auto i:m)
32          {
33                  cout<<i.first<<": "<<(i.second)<<endl;
34          }
35
36  }
37
```

Assignment 1

● GRADED

GROUP
YASH SARASWAT
HIRAK MONDAL
MAYANK BANSAL
View or edit group

TOTAL POINTS
44 / 50 pts

QUESTION 1
Commands — **5** / 5 pts

QUESTION 2
Cryptosystem — **5** / 5 pts

QUESTION 3
Analysis — R **20** / 25 pts

QUESTION 4
Mapping — **9** / 10 pts

QUESTION 5

Password **5** / 5 pts

QUESTION 6

Codes **0** / 0 pts