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)

The punctuation of the given cipher text was incorrect. In particular, the last sentence of the cipher text was incomplete and there was '.' in the beginning of some words and there is a '!' in the middle of a word etc. We observed that shifting all the characters cyclically by 10 places made the punctuation correct. So we shifted the characters of cipher text by 10 places and then carried out frequency analysis and it turned out to be correct.

We computed the frequencies of all characters and observed that y, m are the most frequent characters and replaced them with e and t respectively.
After that replacing e with h made sense due to the formation of word "the".
p is the single letter word and it appears in the middle of a sentence. So p is replaced by a.
a is replaced with s due to the formation of "see".
w is replaced with i due to the formation of "this" and "is".
h is replaced with n due to formation of "than" and "in".
i is replaced with c due to formation of "can".

g is replaced with o due to formation of "one".
v is replaced with w due to formation of "which".
n is replaced with u due to formation of "without".
s is replaced with r due to formation of "interest".
d is replaced with q due to formation of "quotes".
j is replaced with m due to formation of "message"
t is replaced with f due to formation of "first"
k is replaced with l due to formation of "will"
f is replaced with p due to formation of "simple"
u is replaced with d due to formation of "digits"
o is replaced with b due to formation of "substitution"
b is replaced with v due to formation of "have"
x is replaced with y due to formation of "by".

After doing this, the decrypted text states that digits are shifted by 8 places. Since 8 is also in the message it would also be shif ted. So effectively the digits are shifted by 8/2 = 4 places.So we shifted the digits by 4 places to the left to obtain the password.

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)

Both Plain text space and cipher text space are set of all strings formed using the letters from [A...Z] U [a...z] U [0...9] U { ',' , '.' ,'!'} where U denotes union.
The following is the mapping from plain text space to cipher te xt space for alphabet(for both lowercase and uppercase)
A -> P
B -> O
C -> I
D -> U
E -> Y
F -> T
G -> R
H -> E
I -> W
L -> K
M -> J

N -> H
O -> G
P -> F
Q -> D
R -> S
S -> A
T -> M
U -> N
V -> B
W -> V
Y -> X
For digits the mapping is d -> (d + 4)%10
',' , '.' , '!' map to themselves in the cipher text space
Note: 4 letters are not present in cipher text. hence their mappi
ng cannot be decided.

Encrypted Text with corrected punctuation:

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.

Decrypted Text got by using the mapping above:

This is the first chamber of the caves. As
you can see, there is nothing of interest
in the chamber. Some of the later chambers
will be more interesting than this one! The
code used for this message is a simple
substitution cipher in which digits have
been shifted by 4 places. The password is
tyRgU69diqq without the quotes.

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.

1.cpp Download

```cpp
// Code used to correct the punctuation and print the frequencies

#include <bits/stdc++.h>

using namespace std;

int main()
{
    vector<string> a;
    {
        // taking the cipher text as input line by line.
        string s;
        while (getline(cin, s))
        {
            a.push_back(s);
        }
    }

    /*
        The punctuation doesn't seem to be correct for the given paragraph.
        For instance, the paragraph doesn't end with a punctuation mark(.) and there seems to be an
        incomplete sentence in the end. Also the first letter of the Paragraph is not capitalised.
        some words start with a punctuation mark and there is also an exclamation mark in the middle of a word in line 4.
        Since identification of words is important for carrying out Frequency Analysis, we need to crct these errors.
        All these errors can be corrected by cyclically shifting the paragraph by 10 places which is done by the following piece of code.
    */
```

```

    vector<string> b = a;

    int n = int(a.size());
    for (int i = 0; i < n; i++)
    {
        int m = int(a[i].length());
        for (int j = 0; j < m; j++)
        {
            if (a[i][j] == ' ')
                continue;
            int row = i, col = j;
            int cnt = 0;
            while (cnt < 10)
            {
                if (col + 1 < int(a[row].length()))
                    col++;
                else
                {
                    row = (row + 1) % n;
                    col = 0;
                }
                if (a[row][col] != ' ')
                    cnt++;
            }
            b[row][col] = a[i][j];
        }
    }

    for(auto& s:b)
        cout << s << endl;

    cout << endl
         << endl;

    {
        const int A = 26;

        vector<int> cnt(A);

        for (auto &s : b)
        {
            for (char c : s)
            {
                if (c >= 'A' and c <= 'Z')
                    cnt[c - 'A']++;
                if (c >= 'a' and c <= 'z')
                    cnt[c - 'a']++;
            }
        }

        vector<int> ord(A);
```

```
        iota(ord.begin(), ord.end(), 0);
        sort(ord.begin(), ord.end(), [&](int x, int y) { return cnt[x] > cnt[y]; });

        cout << setprecision(3) << fixed;

        int tot = accumulate(cnt.begin(), cnt.end(), 0);

        for (int i : ord)
        {
            cout << char('A' + i) << "  " << cnt[i] << "  " << double(cnt[i] * 100) / tot << endl;
        }
    }

    return 0;
}

/*
INPUT:

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

*/

/*
OUTPUT:

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.


Y  36  13.953
M  28  10.853
A  27  10.465
W  25  9.690
E  22  8.527
G  14  5.426
```

```
P  13  5.039
S  13  5.039
H  12  4.651
I  9  3.488
J  7  2.713
O  7  2.713
N  7  2.713
T  6  2.326
U  6  2.326
K  5  1.938
R  5  1.938
V  4  1.550
F  4  1.550
X  3  1.163
D  3  1.163
B  2  0.775
Q  0  0.000
L  0  0.000
C  0  0.000
Z  0  0.000

*/

/*

DECRYPTED TEXT:

This is the first chamber of the caves. As
you can see, there is nothing of interest
in the chamber. Some of the later chambers
will be more interesting than this one! The
code used for this message is a simple
substitution cipher in which digits have
been shifted by 4 places. The password is
tyRgU69diqq without the quotes.

*/
```

Assignment 1

UNGRADED

GROUP

AJAY PRAJAPATI

A5 - SURYADEVARA SAI KRISHNA
A11 - GARIMELLA MOHAN RAGHU
View or edit group

TOTAL POINTS

- / 50 pts

QUESTION 1

Commands 5 pts

QUESTION 2

Cryptosystem 5 pts

QUESTION 3

Analysis 25 pts

QUESTION 4

Mapping 10 pts

QUESTION 5

Password 5 pts

QUESTION 6

Codes 0 pts