Q1 Commands
10 Points

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

[go, back, read] or [read]

Q2 Cryptosystem
10 Points

What cryptosystem was used in this level?

Vigenère cipher

Q3 Analysis
20 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 of all we looked at the Picture found at the command "go" it said to bow down and look up slowly and count the number of lines in horizontal dimension. So we counted the lines and formed an array and stored it. The array formed was [9, 2, 9, 2, 5, 5, 2, 2, 2, 1] of size 10. It was written that it would be of use. We figured it may be used as a key later. The next observation we did was frequency analysis. We performed it on the whole ciphertext and figured that all the characters seemed to appear nearly equal number of times. As the array we formed was of size 10 we decided to break the ciphertext into blocks of 10 and performed frequency analysis on them individually. Again we figured that all frequency are similar. We had a key now of size=10 and the frequency analysis with nearly equal frequency of characters in

blocks which referred that the cryptosystem should be "Vigenère cipher".

Q4 Decryption Algorithm
15 Points

Briefly describe the decryption algorithm used. Also mention the plaintext you deciphered. (Use less than 350 words)

For deciphering the ciphertext, we used the key taken from the pervious observation [9, 2, 9, 2, 5, 5, 2, 2, 2, 1] since it was of size 10, we used it in cyclic manner to decipher the whole text. For each alphabet, we cyclically shifted the character by the key at the corresponding index. For example the first character was reduced cyclically by 9 characters, the second by 2, the third by 9 and so on. Correspondingly the 11th character is also shifted by 9 characters.

Formally, the ith alphabet is reduced cyclically by arr[i%10] where arr is the key mentioned
above and indexes are in 0-based indexing. Firstly, we shifted only the first block of 10 alphabets and got "Be wary of th" as the first 10 characters which totally made sense as English words and started to make sense. Hence we moved on and shifted the whole ciphertext in the formal manner described above and finally got the following plaintext:

Be wary of the next chamber, there is very little joy there. Speak out the password "the_cave_man_be_pleased" to go through. May you have the strength for the next chamber. To find the exit, you first will need to utter magic words there.

Q5 Password
10 Points

What was the final command used to clear this level?

the_cave_man_be_pleased

Q6 Codes

0 Points

Upload any code that you have used to solve this level

dec.cpp Download

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

bool is_alpha(char c){
    return ((c<='Z' && c>='A')|(c<='z' && c>='a'));
}

int main(){
    int n=10;
    string s="Kg fcwd qh vin pnzy hjcocnt, cjjwg ku wnth nnyvng kxa cjjwg. Urfjm xwy yjg rbbufqwi \"vjg_djxn_ofs_dg_rmncbgi\" yq iq uqtxwlm. Oca zxw qcaj vjg tctnplyj hqs cjn pjcv ejbvdnt. Yt hkpe cjn gcnv, aqv okauy bknn ongm vt zvvgs vcpkh bqtft cjntj.";

    map<char, int> freq;
    for(char c:s){
        if(c<='Z' && c>='A'){
            c+=('a'-'A');
        }
        if(is_alpha(c)){
            freq[c]++;
        }
    }
    cout<<"Char  Freq\n";   // Frequency Analysis of the ciphertext
    for(auto i:freq){
        cout<<i.first<<"      "<<i.second<<'\n';
    }

    string cur="";
    map<char, int> tempfreq;
    for(char c:s){
        if(c<='Z' && c>='A'){
            c+=('a'-'A');
        }
        if(is_alpha(c)){
            cur+=c;
            tempfreq[c]++;
            if(cur.size()==n){
                cout<<"Char  Freq\n";       // Frequency Analysis of the blocks of size 10
                for(auto i:tempfreq){
                    cout<<i.first<<"      "<<i.second<<'\n';
                }
```

```
                tempfreq.clear();
                cur="";
            }
        }
    }
    vector<int> pp={9, 2, 9, 2, 5, 5, 2, 2, 2, 1};      // Key
pp
    int idx=0;
    for(int i=0;i<s.length();i++){
        if(is_alpha(s[i])){
            if(s[i]<='Z' && s[i]>='A'){
                s[i]=s[i]-pp[idx];
                if(s[i]<'A'){
                    s[i]+=26;
                }
            }else{
                s[i]=s[i]-pp[idx];
                if(s[i]<'a'){
                    s[i]+=26;
                }
            }
            idx=(idx+1)%n;
        }
    }
    cout<<s<<'\n';      // Output the deciphered plaintext
    return 0;
}
```

Q7 Team Name

0 Points

team_13

Assignment 2

● Graded

Group

SOLANKI KEVALKUMAR BALVANTBHAI