Q1 Commands
5 Points

List the commands was used in this level?

go -> enter -> pick ->back -> give ->
back -> back -> thrnxxtzy -> read

Q2 Cryptosystem
10 Points

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

Monoalphabetic Substitution - Permutation network

Q3 Analysis
30 Points

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

Cipher text: "qmnjvsa nv wewc flct vprj tj tvvplvl fv xja vqildhc xmlnvc nacyclpa fc gyt vfvw. fv wgqyp, pqq pqcs y wsqrx qmnjvafy cgv tlvhf cw tyl aeuq fv xja tkbv cqnsqs.lhf avawnc cv eas fuqb qvq tc yllrqr xxwa cfy. psdc uqfavrqc gefq pyat trac xwv taa wwd dv eas flcbq. vd trawmvupq quw x decgqcwt, yq yafl vlqs yqklhq! snafq vmllhvqpawr nqg_vfusr_ec_wawy qp fn wgawdgf"

Tools used: C++ code for transformation and frequency analysis

We can surely say that nqg_vfusr_ec_wawy is the password according to previous assignment pattern.

We have used frequency analysis to check the frequency of different characters. Frequency was different for all of the characters, which increases the probability of ciphers such as substitution cipher.

We used global letter frequency to find whether substitution cipher was used. After replacement and some changes in similar frequent letters It was observed that some pairs of letter which are too frequent in English, such as "th" and "he" were too low and also there was an observation that capital letters were not used anywhere in current cipher text which was used in previous assignments. So we thought that permutation cipher was also used. But only permutation cipher could not give any logical output so both were used.

We checked for all the block sizes for permutation cipher in which 5 was most suitable in which more frequent character pairs in same block were making some similar permutations. also there should be word "Password" around the password cipher code, which helped us in changing some substitution to proper one.

Assumptions : Only alphabets were used during permutation and substitution. space and punctuations were on their original places.

substituion mapping:
q -> a
v -> e
a -> t
c -> i
w ->o
f -> h
l -> s
y ->n
t -> l
s -> f
p -> d
n -> r
r -> w
x -> y
g -> g
e -> c
d -> u
u -> m
j -> b
m -> k
h -> p
b -> v
k -> z

i -> q
j,x were not were not used.

in block of size 5 mapping of permutations :
1 -> 4
2 -> 5
3 -> 2
4 -> 1
5 -> 3

plain text :
breaker of this code will be blessed by the squeaky spirit residing in the hole. go ahead and find away of breaking the spell on him cast by the evil zaffar, the spirit of the caveman is always with you. find the magic wand that will let you out of the caves. it would make you a magician,no less than zaffar! speak the password the_magic_of_wand to go through.

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.

1.cpp Download

```cpp
#include<bits/stdc++.h>
using namespace std;
#include <ext/pb_ds/assoc_container.hpp>
#include <ext/pb_ds/tree_policy.hpp>
using namespace __gnu_pbds;
#define ordered_set tree<int, null_type,less<int>, rb_tree_tag,tree_order_statistics_node_update>

#define ll long long
#define pb push_back
```

```
#define mp make_pair
#define all(v) v.begin(),v.end()
#define nline "\n"
const ll INF=1e18;

#ifndef ONLINE_JUDGE
#define debug(x) cerr<<#x<<" "; _print(x); cerr<<nline;
#else
#define debug(x);
#endif

void _print(ll x){cerr<<x;}
void _print(int x){cerr<<x;}
void _print(char x){cerr<<x;}
void _print(string x){cerr<<x;}
template<class T,class V> void _print(pair<T,V> p) {cerr<<"{"; _print(p.first);cerr<<","; _print(p.second);cerr<<"}";}
template<class T>void _print(vector<T> v) {cerr<<" [ "; for (T i:v){_print(i);cerr<<" ";}cerr<<"]";}
template<class T>void _print(set<T> v) {cerr<<" [ "; for (T i:v){_print(i); cerr<<" ";}cerr<<"]";}
template<class T>void _print(multiset<T> v) {cerr<< " [ "; for (T i:v){_print(i);cerr<<" ";}cerr<<"]";}
template<class T,class V>void _print(map<T, V> v) {cerr<<" [ "; for(auto i:v) {_print(i);cerr<<" ";} cerr<<"]";}


void yup(){cout << "Yes" << nline;}
void nope(){cout << "No" << nline;}

// const int limit=7+1e9;

// ------------------------------>--------------------<------------------------------

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


void solve(){
    string s="qmnjvsa nv wewc flct vprj tj tvvplvl fv xja vqildhc xmlnvc nacyclpa fc gyt vfvw. fv wgqyp, pqq pqcs y wsqrx qmnjvafy cgv tlvhf cw tyl aeuq fv xja tkbv cqnsqs.lhf avawnc cv eas fuqb qvq tc yllrqr xxwa cfy. psdc uqfavrqc gefq pyat trac xwv taa wwd dv eas flcbq. vd trawmvupq quw x decgqcwt, yq yafl vlqs yqklhq! snafq vmllhvqpawr nqg_vfusr_ec_wawy qp fn wgawdgf";

    map<char, int> freq;
    for(char c:s){
        if(c<='Z' && c>='A'){
```

```
            c+=('a'-'A');
        }
        if(is_alpha(c)){
            freq[c]++;
        }
    }
    vector<pair<int,char> >v;
    cout<<"Char  Freq\n";   // Frequency Analysis of the
ciphertext
    for(auto i:freq){
        // cout<<i.first<<"      "<<i.second<<'\n';
        v.pb({i.second,i.first});
    }
    sort(all(v));
    reverse(all(v));
    for(auto i:v){
        cout << i.second << "     " << i.first << nline;
    }
    cout << nline;
    int j=0;

    map<char,char> change;
    string freqorder="aetiohsnlfdrwygcumbkpvzqjx";
    for(auto i:v){
        change[i.second]=freqorder[j];
        j++;
    }
    for(auto &it:s){
        if(isalpha(it)){
            it=change[it];
        }
    }

    cout << s << nline << nline;

    int n=5;
    int i=0;j=0;
    for(int i=0;i<s.size();i++){
        if(isalpha(s[i])){
            s[j]=s[i];j++;
        }
    }
    s=s.substr(0,j);
    cout << s << nline << nline;
    string k;
    string ans;
    for(i=0;i<j;i++){
        k.pb(s[i]);
        if((i+1)%n==0){
            vector<int> use={4,5,2,1,3};
            vector<int> pos(5,0);
            for(int g=0;g<5;g++){
```

```
                pos[use[g]-1]=g;
            }
            string t;
            for(int v=0;v<5;v++){
                t.push_back(k[pos[v]]);
            }
            // swap(k[0],k[3]);
            // swap(k[1],k[4]);
            // swap(k[2],k[4]);
            // swap(k[0],k[1]);
            ans+=t;k.erase();
        }
    }
    ans+=k;
    cout << ans << nline;

}

int main(){
    ios::sync_with_stdio(false);
    cin.tie(NULL);
    int t;
    // cin >> t;
    t=1;
    while(t--){
        solve();
    }
    return 0;

}
```

Q6 Group name

0 Points

team_13

Assignment 3

● Graded