Q1 Team name

0 Points

NULL

Q2 Commands

10 Points

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

go,go,read

Q3 Cryptosystem

10 Points

What cryptosystem was used in this level?

Playfair Cipher

Q4 Analysis

20 Points

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

Firstly we tried using frequency analysis on the ciphertext and observed that the frequencies are not that widely distributed and also the words formed do not make any sense. Thus we concluded that it was not substitution cipher. We tried using vigenere cipher as well but the text did not seem reasonable either.

Then we observed that if we enter "go" instead of "read" in the first prompt, we get a message with morse code which hints us to "play fair". This made us realize that the text might be using Playfair Cipher. To find the key with which it is encrypted, we decoded the morse code and got "SECURITY" as the key. We decrypted the text assuming that it is Playfair cipher with key "SEC

URITY" and found the password "OPEN_SESAME" which worke
d.

Q5 Decryption algorithm

15 Points

Briefly describe the decryption algorithm used. Also, mention the plaintext you deciphered. (Use less than 250 words)

The decryption algorithm uses a 5*5 square which is obtained
by replacing the first 8 cells(in row-major order) with letters of t
he word "security" (which is the key as mentioned in Q4), and t
he remaining cells are filled with other letters in alphabetic ord
er while skipping letter 'J'. The 5*5 square looks as follows after
construction:
S E C U R
I T Y A B
D F G H K
L M N O P
Q V W X Z
The Decryption algorithm is as follows:
1. Group the ciphertext into groups of 2 letters ignoring the pun
ctuation marks.
2. For each group of 2 letters if
(a) They are in the same row of the grid: Each of them is replac
ed by their (cyclic) precedent in the corresponding row. (the lett
er to the left of it in the row).
(b) They are in the same column of the grid: Each of them is rep
laced by their (cyclic) precedent in the corresponding column.
(the letter above it in the column).
(c) Else: Each of them is replaced with the letters on their own r
ow but at the other pair of corners of the original pair's rectangl
e.
Note: No two consecutive characters are the same in Playfair ci
phertext since Playfair cipher encryption algorithm inserts an X
between consecutive equal characters.

The text decrypted with the above algorithm is as follows:
BE WARY OF THE NEXT CHAMBER, THERE IS VERY LITTLE IO
Y THERE.
SPEAK OUT XTHE PASSWORD "OPEN_SESAME" TO GO THR
OUGH. MAY XYOU

HAVE THE STRENGTH FOR THE NEXT CHAMBER. TO FIND T
HE EXIT YOU
FIRST WILXL NEXED TO UTTER MAGIC WORDS THERE.

As we can see, there are 'X' 's inserted between consecutive e
qual characters and J replaced with I since it is not present in t
he grid. So the final decrypted text is as follows:
BE WARY OF THE NEXT CHAMBER, THERE IS VERY LITTLE JO
Y THERE.
SPEAK OUT THE PASSWORD "OPEN_SESAME" TO GO THRO
UGH. MAY YOU
HAVE THE STRENGTH FOR THE NEXT CHAMBER. TO FIND T
HE EXIT YOU
FIRST WILL NEED TO UTTER MAGIC WORDS THERE.

The code written using the above algorithm can be seen below in the code section.

Q6 Password

10 Points

What was the final command used to clear this level?

OPEN_SESAME

Q7 Code

0 Points

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

1.cpp Download

```
#include <bits/stdc++.h>

using namespace std;

int main()
{

    vector<string> a;
    string _;
    while (getline(cin, _))
    {
```

```
        a.push_back(_);
    }

    vector<string> grid(5, string(5, ' '));

    string key = "SECURITY";

    char skip = 'J';

    vector<int> row(26, -1), col(26);

    for (int i = 0; i < 8; i++)
    {
        int r = i / 5, c = i % 5;
        grid[r][c] = key[i];
        row[key[i] - 'A'] = r;
        col[key[i] - 'A'] = c;
    }

    int cur = 8;

    for (int i = 0; i < 26; i++)
    {
        if (row[i] == -1 and skip != char('A' + i))
        {
            int r = cur / 5, c = cur % 5;
            grid[r][c] = char('A' + i);
            row[i] = r;
            col[i] = c;
            cur++;
        }
    }

    string S = "";

    for (auto &s : a)
    {
        for (char c : s)
        {
            if (c >= 'A' and c <= 'Z')
            {
                S += c;
            }
        }
    }

    int N = int(S.length());
    string T = S;

    for (int i = 0; i < N; i += 2)
    {
        int x = (S[i] - 'A');
```

```
        int y = (S[i + 1] - 'A');

        if (row[x] == row[y])
        {
            int cx = col[x];
            int cy = col[y];
            int r = row[x];
            T[i] = grid[r][(cx + 4) % 5];
            T[i + 1] = grid[r][(cy + 4) % 5];
        }
        else if (col[x] == col[y])
        {
            int rx = row[x];
            int ry = row[y];
            int c = col[x];
            T[i] = grid[(rx + 4) % 5][c];
            T[i + 1] = grid[(ry + 4) % 5][c];
        }
        else
        {
            int rx = row[x], cx = col[x], ry = row[y], cy = col[y];
            T[i] = grid[rx][cy];
            T[i + 1] = grid[ry][cx];
        }
    }

    cur = 0;

    for (auto &s : a)
    {
        for (char c : s)
        {
            if (c >= 'A' and c <= 'Z')
            {
                cout << T[cur++];
            }
            else
                cout << c;
        }
        cout << endl;
    }

    return 0;
}

/*

INPUT:
TR XYCB MH AFC MUVY EOHPTCS, AFCSS TE QCSI NTYIMS TNA AFCSC.
EMRBH XAA VAFR MIUCQPUH "LMRL_CCETOT" FN HM AKUXAHK.
```

```
OTA WANA
OTXT FFU EISCWNAF HME BFU MCVA UGTOTRE. BM HYLF IFU UVTY ANE
HBSEI QYOQM OUVSF AM EAFTE PYHYS XNSKE IFUSC.

OUTPUT:
BE WARY OF THE NEXT CHAMBER, THERE IS VERY LITTLE IOY THERE.
SPEAK OUT XTHE PASSWORD "OPEN_SESAME" TO GO THROUGH. MAY XYOU
HAVE THE STRENGTH FOR THE NEXT CHAMBER. TO FIND THE EXIT YOU
FIRST WILXL NEXED TO UTTER MAGIC WORDS THERE.

*/
```

Assignment 2

UNGRADED

GROUP

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

TOTAL POINTS

- / 65 pts

QUESTION 1

Team name — 0 pts

QUESTION 2

Commands — 10 pts

QUESTION 3

Cryptosystem — 10 pts

QUESTION 4

Analysis — 20 pts

QUESTION 5

Decryption algorithm — 15 pts

QUESTION 6

Password 10 pts

QUESTION 7

Code 0 pts