Q1 Team Name

0 Points

The_Kryptonians

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?

Morse Code encryption was used for the key and
Playfair Cipher was used for the final message.

Q4 Analysis

20 Points

What tools and observations were used to figure out the cryptosystem? (Explain in less than 300 words)

The second screen contained a code consisting of only "_" and "." which gave a clue that it might be Morse Code. Morse code can be viewed like a substitution cipher, because each letter, number and some punctuation marks are replaced by a series of dots and dashes, and it has a fixed standard key. On evaluating that based on the standard key for morse code available, one gets the word "CRYPTANALYSIS".

It also contained the word "PLAY FAIR" and nothing else in capital letters, which gave the hint that the playfair cipher could be used in further decryption. Since no option for chosen/given plaintext or ciphertext attack was available, to find the key, one went for the word "CRYPTANALYSIS" obtained through morse code.

Key Square was formed by omitting the letter J. The initial letters of the key square are the unique alphabets that appear in the key, followed by the general order of the remaining alphabets.

The Key Square was:

C	R	Y	P	T
A	N	L	S	I
B	D	E	F	G
H	K	M	O	Q
U	V	W	X	Z

The decryption algorithm is explained in the next question.

The deciphered plaintext was:

BEWARYOFTHENEXTCHAMBERTHEREISVERYLITTLEIOYTHERESPEAKOUTXTHEPASSWORDABRACADABRATOGOTHROUGHMAYYOUHAVETHESTRENGTHFORTHENEXTCHAMBERTOFINDTHEEXITYOUFIRSTWILXLNEXEDTOUTTERMAGICWORDSTHERE

Websites Referred:

https://www.geeksforgeeks.org/playfair-cipher-with-examples/

https://en.m.wikipedia.org/wiki/Morse_code

Q5 Decryption Algorithm

15 Points

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

The Playfair Cipher is a type of substitution cipher which uses a literal diagram. It is a manual symmetric encryption technique.

The Playfair Cipher Decryption Algorithm consists of 2 steps:

For the first step, the key is used to generate a key square. The key square is a grid of 25 unique letters that are used to encrypt the plaintext. The only letter that is omitted from the grid is the letter J. The initial letters of the key square are the unique alphabets that appear in the key, followed by the general order of the remaining alphabets.

The next step is the decryption of the ciphertext. First, we removed all the characters like spaces, full stops or any other punctuations. Then, the ciphertext was divided into pairs of two alphabets and one of the three below mentioned substitutions was done.

1. If both the letters are in the same row, replace them with the letters to their immediate left. Going around to the rightmost letter if at the leftmost position.
2. If both the letters are in the same column, replace them with the letters to their immediate above. Going around to the bottommost letter if at the topmost position.
3. If both the letters are in different rows and columns, form a rectangle with these two letters and replace the letters on the horizontal opposite corner of the rectangle.

The deciphered text was transformed a little to get the correct plaintext which was :

BE WARY OF THE NEXT CHAMBER, THERE IS VERY LITTLE JOY THERE. SPEAK OUT THE PASSWORD "ABRA_CA_DABRA" 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.

Here I of IOY was replaced by J to form JOY to get the meaningful word. Also, some double letters were separated by X because every pair in Playfair Cipher has unique letters, so these occurrences of X were removed to form meaningful words.

Q6 Password

10 Points

What was the final command used to clear this level?

ABRA_CA_DABRA

Q7 Code

0 Points

Upload any code that you have used to solve this level

▾ assn2.py

Download

```python
import numpy as np

keyword=input("enter keyword:")
keyword=keyword.lower()

ciphertext=input("Enter ciphertext:")
ciphertext=ciphertext.lower()
ciphertext=ciphertext.replace("j","i")
ciphertext=list(ciphertext)

st=list()

for i in ciphertext:
    if i.isalpha():
        s.append(i)

l=len(st)

if(l%2!=0):
    st.append("z")
    l+=1


b=list()
e=list()

for i in range(97,123):
    if(chr(i)!="j"):
        e.append(chr(i))

m=0
n=0
d={}
for i in range(5):
    c=[]
    while(len(c)!=5):
        if(n!=len(keyword)):
            if keyword[n] not in d:
                c.append(keyword[n])
                d[keyword[n]]=1
            n+=1
        else:
            if e[m] not in d:
                c.append(e[m])
                d[e[m]]=1
            m+=1

    b.append(c)

key=np.array(t)

r=np.where(key=="r")

pt=[]

for i in range(0,le,2):
    r1=np.argwhere(key==s[i])
    r2=np.argwhere(key==s[i+1])

    if(r1[0][1] == r2[0][1]):
        if(r1[0][0]!=0):
            pt.append(key[r1[0][0]-1][r1[0][1]])
        elif(r1[0][0]==0):
            pt.append(key[4][r1[0][1]])

        if(r2[0][0]!=0):
            pt.append(key[r2[0][0]-1][r2[0][1]])
        elif(r2[0][0]==0):
            pt.append(key[4][r2[0][1]])
    elif(r1[0][0]==r2[0][0]):
        if(r1[0][1]!=0):
            pt.append(key[r1[0][0]][r1[0][1]-1])
        elif(r1[0][1]==0):
            pt.append(key[r1[0][0]][4])
        if(r2[0][1]!=0):
            pt.append(key[r2[0][0]][r2[0][1]-1])
        elif(r2[0][1]==0):
            pt.append(key[r2[0][0]][4])

    else:
        pt.append(key[r1[0][0]][r2[0][1]])
        pt.append(key[r2[0][0]][r1[0][1]])

plaintext=str()
for i in range(len(res)):
    plaintext+=pt[i]
```

```

print()
print(plaintext)
```

Assignment 2

● GRADED

GROUP

Pranshu Gaur
Maulik Singhal
Maryam Raza Khan
View or edit group

TOTAL POINTS

65 / 65 pts

QUESTION 1

Team Name **0** / 0 pts

QUESTION 2

Commands **10** / 10 pts

QUESTION 3

CryptoSystem **10** / 10 pts

QUESTION 4

Analysis **20** / 20 pts

QUESTION 5

Decryption Algorithm R **15** / 15 pts

QUESTION 6

Password **10** / 10 pts

QUESTION 7

Code **0** / 0 pts