Q1 Team Name

0 Points

DECODERS

Q2 Commands

10 Points

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

1. go
2. back
3. 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 300 words)

We noticed a pattern on one of the distant boulders. Then, we went closer to the boulder and found out that there was some pattern carved on it. The pattern did not contain any letters or numbers but contained a series of dots and hyphens which looked like a morse code. We decrypted this morse code and it read

"CRYPTANALYSIS". Then, we entered this word as the command but it showed that the command was invalid. Then we went back to the screen near the exit and read the text written there which read as:

DF ULYP XO CQD LFWC RUBHEDY, CQDYG LN XDYL EGIYIG LMP CQDYF. LYFNH HXPZ CQF YNILXKPB "NDCB_AN_BBHCN" PQ FQ CQPKZBK. OLC PMC UNUG YMB IPYDIDCQ OXY CMB LDZP AULHDFY. CX OALG RMB FWGI PMX BNTIP ZLSWS LFWFE PQ ZCYGY KIBAT XMNKI PMBYD.

We tried SUBSTITUTION CIPHER and PERMUTATION CIPHER for this cipher text but the frequency of the letters in the ciphertext was not matching with that of English letters . Hence we eliminated these ciphers. Then we recalled that the spirit of the caveman said to "believe in yourself and PLAY FAIR". We then anticipated that the "PLAY FAIR" the caveman was talking about was a hint that the encryption technique used in this level might be the PLAY FAIR CIPHER.

The PLAY FAIR CIPHER uses a key to encrypt a text and the same key will be used to decrypt it. We tried to decrypt this text using "CRYPTANALYSIS" as the key.

We made a 5x5 key table using this key and decrypted the text by forming a group of two letters. After applying the decryption algorithm using this key we found out that the text was transformed into a meaningful paragraph which gave us the password for the exit door as "ABRA_CA_DABRA". The deciphered paragraph is:

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.

We decrypted this text using PYTHON code in JUPYTER NOTEBOOK which is attached below. We entered the above password to get out of the chamber and cleared this level.

Q5 Decryption Algorithm

15 Points

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

After decoding the morse code we got "CRYPTANALYSIS" as the key which was used to encrypt the plain text using PLAYFAIR CIPHER. The same key is used to decrypt the cipher text.
The Playfair Cipher Decryption Algorithm:
We decrypted the message using following 2 steps:

1. Generating the 5x5 key table:
Start filling the table from the first cell and insert each unique letter from the key in the same order they appear and fill the remaining cells with the remaining letters in alphabets in the same order. Since the table contains 25 alphabets,one letter must be omitted and usually its 'J'. If the Plain text contains 'J' it is replaced by 'I'.

The Table generated is as follows:

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

2. Decrypting the message:
The ciphertext is split into pairs of two letters.
For example, "DF ULYP XO CQD LFWC RUBHEDY" is split into "DF" ,"UL" ,"YP" ,"XO" ,"CQ","DL" ,"FW" ,"CR" ,"UB", "HE", "DY".
Now, each pair of letters is decrypted using the following rules:
a) If both the letters are in the same column in the key table then, each of the letters is replaced by the letter above it in the table. For example, "UB" is replaced by "HA".
b) If both the letters are in the same row in the key table then, each of the letters is replaced by the letter to the left of it in the

table.
For example, "DF" is replaced by "BE".
c) If none of the above is true then, form a rectangle with these two letters and take the letters on the horizontal opposite corners of the rectangle.
For example, "UL" is replaced by "WA".

By using the above algorithm the plaintext we got is as follows:

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

While encryption a pair cannot contain the same letter. Then we break the letter in a single and add a bogus letter to the previous letter. Since the letter 'J' is replaced by 'I', whenever the letter 'I' appears we replace it with 'J' to check if any meaningful word is formed or not. If formed, we replace it otherwise we leave it as it is.
For example in the above plain text, "IOY" is replaced by "JOY" and whenever two same letters occur in a pair we remove the letter 'X'.
Finally, after processing the above plain text, the message looked like below:
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.

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

Play Fair cipher.ipynb

Download

In [95]:
```
key=list("CRYPTANALYSIS")
key
```

Out [95]:
```
['C', 'R', 'Y', 'P', 'T', 'A', 'N', 'A', 'L', 'Y',
```

In [96]:
```
key_squere=key
for i in range(65,91):
    if chr(i)=='J':
        continue
    key_squere.append(chr(i))
```

In [97]:
```
text=[]
for i in range(len(key_squere)):
    if key_squere[i] not in text:
        text.append(key_squere[i])
```

In [129]:
```
squere=[]
k=0
for i in range(5):
    li=[]
    for j in range(5):
        li.append(text[k])
        k+=1
    squere.append(li)
squere
```

Out [129]:
```
[['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']]
```

In [130]:
```
cipher_text="""DF ULYP XO CQD LFWC RUBHEDY,
CQDYG LN XDYL EGIYIG LMP CQDYF. LYFNH HXPZ

CQF YNILXKPB "NDCB_AN_BBHCN" PQ FQ CQPKZBK.
OLC PMC UNUG YMB IPYDIDCQ OXY CMB LDZP
```

```
AULHDFY. CX OALG RMB FWGI PMX BNTIP ZLSWS
LFWFE PQ ZCYGY KIBAT XMNKI PMBYD"""
```

In [142]:

```
cipher_text2="""DF ULYP XO CQD LFWC RUBHEDY,
CQDYG LN XDYL EGIYIG LMP CQDYF. LYFNH HXPZ
CQF YNILXKPB "NDCB_AN_BBHCN" PQ FQ CQPKZBK.
OLC PMC UNUG YMB IPYDIDCQ OXY CMB LDZP
AULHDFY. CX OALG RMB FWGI PMX BNTIP ZLSWS
LFWFE PQ ZCYGY KIBAT XMNKI PMBYD"""
```

In [143]:

```
cipher_text=cipher_text.replace(" ","")
# cipher_text.replace(".","")
```

In [144]:

```
cipher_text=cipher_text.replace(".","")
cipher_text1=[]
for i in range(len(cipher_text)):
    if ord(cipher_text[i]) not in
range(65,91):
        continue
    cipher_text1.append(cipher_text[i])
str1 = ''.join([str(elem) for elem in
cipher_text1])
str1
```

Out [144]:

```
'DFULYPXOCQDLFWCRUBHEDYCQDYGLNXDYLEGIYIGLMPCQDYFLY
```

In [145]:

```
len(str1)
```

Out [145]:

```
180
```

In [146]:

```
def ind(c):
    for i in range(5):
        for j in range(5):
            if c==squere[i][j]:
                return [i,j]
```

In [147]:

```
p_split=[]
n=len(str1)
i=0
ans=[]
while i<n:
    if ord(str1[i]) not in range(65,91):
        i+=1
        continue
#     print(str1[i])
    pair1=ind(str1[i])
#     print(pair1)
#     print(str1[i+1])
    pair2=ind(str1[i+1])
#     print(pair2)
```

```
    i+=2
    if pair1[0]==pair2[0]:
        ans.append(squere[pair1[0]]
[(pair1[1]-1)%5])
        ans.append(squere[pair2[0]]
[(pair2[1]-1)%5])
    elif pair1[1]==pair2[1]:
        ans.append(squere[(pair1[0]-1)%5]
[pair1[1]])
        ans.append(squere[(pair2[0]-1)%5]
[pair2[1]])
    else:
        ans.append(squere[pair1[0]]
[pair2[1]])
        ans.append(squere[pair2[0]]
[pair1[1]])
```

In [148]:

```
ans1 = ''.join([str(elem) for elem in ans])
ans1
```

Out [148]:

```
'BEWARYOFTHENEXTCHAMBERTHEREISVERYLITTLEIOYTHERESP
```

In [149]:

```
ans2=[]
k=0
for i in range(len(cipher_text2)):
    if ord(cipher_text2[i]) in range(65,91):
        ans2.append(ans1[k])
        k+=1
    else:
        ans2.append(cipher_text2[i])
```

In [150]:

```
ans3 = ''.join([str(elem) for elem in ans2])
ans3
```

Out [150]:

```
'BE WARY OF THE NEXT CHAMBER, THERE IS VERY LITTLE
```

Password is " ABRA_CA_DABRA"

Assignment 2

● GRADED

GROUP

Akash Gajanan Panzade
Manthan Kojage
Abhishek Dnyaneshwar Revskar

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	**15** / 15 pts
QUESTION 6	Password	**10** / 10 pts
QUESTION 7	Code	**0** / 0 pts