Q1 Team Name
0 Points

Lazarus

Q2 Commands
10 Points

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

list
go
back
read

Q3 CryptoSystem
10 Points

What cryptosystem was used in this level?

Playfair Cipher for text.
Morse code for encrypting Key.

Q4 Analysis
20 Points

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

After entering the "go" command, we saw a pattern of dashes and dots on the screen, and
using prior knowledge, we guessed it was morse code. Using

an image from google.

Morse Code	English Alphabets
-.-.	C
.-.	R
-.--	Y
.--.	P
-	T
.-	A
-.	N
.-..	L
...	S
..	I

-.-. .-. -.-- .--. - .- -. .- .-.. -.-- ... .
Using the above table we decrypted the above pattern to key "CRYPTANALYSIS".

In the last paragraph on the screen 'PLAY FAIR' was standing out from the rest of the text due to its font and so we thought it might be a hint.
Then we googled the "PLAY FAIR" and found out it is an encryption technique.

Then we entered the "back" command and reached the previous screen where we entered the "read" command and we saw the ciphertext;

Ciphertext:

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

First, we removed spaces, punctuation and underscore from the ciphertext as play fair cipher is only limited to alphabets so above cannot be encrypted and also it simplifies pair making.
Then we used the below-mentioned Playfair matrix to decrypt

the above ciphertext. Detailed procedure and deciphered text are mentioned in the next question's answer. There are various variations in the Playfair cipher around which letter is not included in the 5*5 grid and is replaced in plaintext at the start of the encryption process. We chose the most common one where we do not include 'J' into the matrix and also replace 'j' and 'J' with 'i' and 'I' in the plaintext respectively.

References -
Morse code - https://upload.wikimedia.org/wikipedia/commons/thumb/b/b5/International_Morse_Code.svg/390px-International_Morse_Code.svg.png

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

Q5 Decryption Algorithm

15 Points

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

Key:

```
[['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']]
```

Above is the 5x5 matrix used for encryption and decryption of messages in Playfair Cipher generated using key 'CRYPTANALYSIS'. The process of generating this matrix is first to put all unique letters from the key in order of appearance into the 5x5 matrix and then fill vacant spaces in alphabetical order with remaining alphabets except for 'J'.

The decryption method followed is to take letters in pairs of two

from left and check their position in the above matrix :

1. If both belong to the same column then add the alphabet above them in the matrix to plaintext. If a letter is at the top take the bottommost letter of the column. e.g "XO" is decrypted to "OF"

2. If both belong to the same row then add the alphabet to the left of them in the matrix to plaintext. If a letter is at the leftmost take the rightmost letter of the row. e.g "DF" is decrypted to "BE"

3. Form a rectangle with the letters at the opposite vertices and for each letter take the horizontally opposite letter in the formed rectangle e.g "UL" is decrypted to "WA"

Note: In each of the above steps, the order in which letters are added to the plaintext should be the same as the order of the pair picked from the ciphertext.

Below is the plaintext decrypted from the ciphertext.

'BEWARYOFTHENEXTCHAMBERTHEREISVERYLITTLEIOYTHERESPEAKOUTXTHEPASSWORDABRACADABRATOGOTHROUGHMAYYOUHAVETHESTRENGTHFORTHENEXTCHAMBERTOFINDTHEEXITYOUFIRSTWILXLNEXEDTOUTTERMAGICWORDSTHERE'

After Inserting spaces and removing 'X' added to separate repeated letters and replacing 'I' when it does not make proper English word with 'J'. We also add punctuations ('.' , ',' , ' "" ') and underscore('_') in the plaintext at positions from ciphertext.

'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

playfair.py Download

```
1  import numpy as np
2  cipher = 'DF ULYP XO CQD LFWC RUBHEDY, CQDYG LN XDYL EGIYIG
   LMP CQDYF. LYFNH HXPZ CQF YNILXKPB "NDCB_AN_BBHCN" PQ FQ
   CQPKZBK. OLC PMCUNUG YMB IPYDIDCQ OXY CMB LDZP AULHDFY. CX
   OALG RMB FWGI PMXBNTIP ZLSWS LFWFE PQ ZCYGY KIBAT XMNKI
   PMBYD.'
3
4  cipher2= ''
5
6  for c in cipher:
7      if ord(c) in range(65,91):
8          cipher2+=c
9
10 playmat=[]
11 added = []
12 key = 'CRYPTANALYSIS'
13
14 for s in key:
15     if s not in added:
16         playmat.append(s  if s not in ['j','J'] else 'I')
17         added.append(s)
18
19 for i in range(65,91):
20     if chr(i) not in added and chr(i)!='J':
21         playmat.append(chr(i))
22         added.append(chr(i))
23
24
25 playmat = np.array(playmat).reshape(5,5)
26
```

```
print(playmat)


plain = ''

for i in range(0,len(cipher2)-1,2):
    x1,y1 = np.where(playmat == cipher2[i])
    x2,y2 = np.where(playmat == cipher2[i+1])
    x1 = x1[0]
    x2 = x2[0]
    y1 = y1[0]
    y2 = y2[0]

    if y1 == y2:
        a = playmat[x1-1][y1] if x1>0 else playmat[4][y1]
        b = playmat[x2-1][y1] if x2>0 else playmat[4][y1]
        plain+=(a+b)

    elif x1 == x2:
        a = playmat[x1][y1-1] if y1>0 else playmat[x1][4]
        b = playmat[x1][y2-1] if y2>0 else playmat[x1][4]
        plain+=(a+b)
    else:
        plain+=playmat[x1][y2]
        plain+=playmat[x2][y1]


print('\n\n',plain)


```

Assignment 2

GRADED

GROUP

Varun Vankudre

Aditya Loth

Harsh Agarwal
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

✔	+ 5 pts	Explain keytable generation. Mention that the keyword used is "CRYPTANALYSIS".
✔	+ 2 pts	Mention Rule 1 (Letters of digraph in same row).
✔	+ 2 pts	Mention Rule 2 (Letters of digraph in same column).
✔	+ 2 pts	Mention Rule 3 (Letters of digraph form opposite corners of a rectangle).
✔	+ 1 pt	Mention about X's occurrence in the decrypted text.
✔	+ 1 pt	Explain X's occurrence due to the same letters bigram in the plaintext.
✔	+ 2 pts	Mention the final deciphered plaintext. (Full points for cases with Xs in the plaintext also)
	− 1 pts	Not mentioned and explained how I and J sharing same space in keytable happens during encryption. Also why "IOY" has been changed to "JOY" in the final plaintext.
	+ 0 pts	Unanswered or missing answer.

QUESTION 6
Password
10 / 10 pts

QUESTION 7
Code
0 / 0 pts