Q1 Team Name

0 Points

Enigma

Q2 Commands

10 Points

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

go
back
read

Q3 CryptoSystem

10 Points

What cryptosystem was used in this level?

Play-Fair Cipher
International Morse Code Chart

Q4 Analysis

20 Points

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

Tools :-
1. International morse code chart
(https://morsecode.world/international/morse2.html) and

(https://morsecode.world/international/morse2.html) and python script to break the morse code.
2. Playfair cipher algorithm (https://www.geeksforgeeks.org/playfair-cipher-with-examples/).

Observations:-
We tried multiple commands and as soon as we used the "go" command, we found a code on the screen consisting of dots and dashes, which we know from our knowledge that it was morse code, We utilised an international morse code chart and the attached python script to generate something workable; fortunately, it was simply morse code and it transformed to the phrase 'CRYPTANALYSIS'. We also noticed that the screen displayed a message in which the word "PLAY FAIR" was capitalized, we took this as a sign for the subsequent steps. We were already aware of the existence of a symmetric cryptographic system called " PLAY FAIR," and because the morse code decoded as a word, we deduced that at this level, we would need to utilize the Playfair cipher with the key CRYPTANALYSIS, which makes sense given that the "play fair" cipher uses a key to decrypt the message. The encrypted message was obtained by using the "back" and "read" commands.

The following are the observations that demonstrate that the cryptosystem in question is the Playfair Cipher system:
1. The number of alphabetic characters in the cipher are all even.
2.There are no Bigrams that are made up of the same characters as another Bigram. It is mandatory that the ciphertext have a minimum of 26 different characters.
An another observation that we made was that the text did not contain the letter 'J'. In the playfair cipher, the letters I and J are treated identically in the 5x5 matrix, which is used to insert the ciphertext according to the encipher's preference. As the ciphertext did not contain any "J," it is possible that the encryptor replaced the element I/J with I alone.

Q5 Decryption Algorithm

15 Points

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

We have used ”Play fair cipher” to decrypt the plaintext. In “play fair cipher” we generate a key table(grid of 5X5) and fill the spaces in the table (a modified Polybius square) with the letters of the keyword (dropping any duplicate letters). The key here is one that was recovered from morse code and was identified as "CRYPTANALYSIS" using a morse chart. Then, in order, fill in the remaining spaces with the rest of the alphabet's letters (typically eliminating "J" as we only have 25 slots in the table and 26 alphabets). Punctuation marks are preserved in their original state. The text is then divided into Bigrams (pairs of letters) and follow the rules below based on the letter’s position in the matrix:

1. If the two letters are on the same row, replace them with the ones to their left (loop to the right if the grid is an edge),
2. If the two letters are on the same column, replace them with the ones directly above (loop to the bottom of the top of the grid is reached),
3. If the letters are not on the same row, replace them with the ones that form a rectangle with the original pair.

Using the above rules the plaintext was decrypted and the text we received was. BEWARY OF THE NEXT CHAMBER THERE IS VERY LITTLE IOY THERE SPEAK OUT X THE PASSWORD ABRACADABRA TO GO THROUGH MAY YOU HAVE THE STRENGTH FOR THE NEXT CHAMBER TO FIND THE EXIT YOU FIRST WILXLNEXED TO UTTER MAGIC WORDS THERE.

Now we can consider "I" to be "J" after this decryption and

Now we can consider "I" to be "J" after this decryption and disregard "X" if it appears between two similar letters. After doing the mentioned corrections the final decrypted text becomes BE WARY OF THE NEXT CHAMBER, THERE IS VERY LITTLE JOY THERE. SPEAK OUT THE PASSWORD "ABRACADABRA" 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?

ABRACADABRA

Q7 Code

0 Points

Upload any code that you have used to solve this level

morse_code_converter.py Download

```
vocab = {'A':'.-', 'B':'-...',\
                    'C':'-.-.', 'D':'-..', 'E':'.',\
                    'F':'..-.', 'G':'--.', 'H':'....',\
                    'I':'..', 'J':'.---', 'K':'-.-',\
                    'L':'.-..', 'M':'--', 'N':'-.',\
                    'O':'---', 'P':'.--.', 'Q':'--.-',\
                    'R':'.-.', 'S':'...', 'T':'-',\
                    'U':'..-', 'V':'...-', 'W':'.--',\
                    'X':'-..-', 'Y':'-.--', 'Z':'--..',\
-..',\
          '1':'.----', '2':'..---', '3':'...--',\
          '4':'....-', '5':'.....', '6':'-....',\
          '7':'--...', '8':'---..', '9':'----.',\
          '0':'-----', ', ':'--..--', '.':'.-.-.-',\
          '?':'..--..', '/':'-..-.', '-':'-....-',\
          '(':'-.--.', ')':'-.--.-'}
new_vocab = {v:k for k,v in vocab.items()}
mc = '-.-. .-. -.-- .--. - .- -. .- .-.. -.-- ... .. ...'
mc = mc.split(' ')
out = ''
for i in mc:
    out +=new_vocab[i]
print(out)# your code goes here
```

play_fair.py

Download

```
key = 'CRYPTANALYSIS'
mat = [['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'],]

def play_fair(mat, cipher):
    for i in mat:
        if cipher[0] in i:
            row1 = mat.index(i)
            column1 = i.index(cipher[0])
    for i in mat:
        if cipher[1] in i:
            row2 = mat.index(i)
            column2 = i.index(cipher[1])

    #Case1: Same row
    if row1 == row2:
        if column1 == 0 and column2 != 0:
            cipher = mat[row1][4]+mat[row1][column2-1]
        elif column1 != 0 and column2 == 0:
            cipher = mat[row1][column1-1]+mat[row1]
            cipher = mat[row1][column1-1]+mat[row1][4]
        elif column1 == 0 and column2 == 0:
            cipher = mat[row1][4]+mat[row1][4]
        else:
            cipher = mat[row1][column1-1]+mat[row1][column2-1]

    #Case 2: Same columnumn
    elif column1 == column2:
        if row1 == 0 and row2 != 0:
            cipher = mat[4][column1]+mat[row2-1][column1]
        elif row1 != 0 and row2 == 0:
            cipher = mat[row1-1][column1]+mat[4][column1]
        elif row1 == 0 and row2 == 0:
            cipher = mat[4][column1]+mat[4][column1]
        else:
            cipher = mat[row1-1][column1]+mat[row2-1][column2]

    #Case3: Rectangle
    else:
        cipher = mat[row1][column2] + mat[row2][column1]
    return cipher



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.'
c_mo = cipher.replace(" ","").replace(",","").replace(".","").replace('"',""
ans = ''
for i in range(0,len(c_mo),2):
    bigraph = c_mo[i]+c_mo[i+1]
    c_bi = play_fair(mat,bigraph)
    ans+=c_bi[0]+c_bi[1]

print(ans)
```

Assignment 2

● GRADED

GROUP

Pranshu Sahijwani
Kajal Sethi
Gajender Sharma

View or edit group

TOTAL POINTS

59 / 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	**14** / 15 pts
QUESTION 6	Password	R **5** / 10 pts
QUESTION 7	Code	**0** / 0 pts