Q1 Team Name

0 Points

flash

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?

We have used playfair cipher (to decrypt the cipher text) and Morse code (to get the key) in this level

Q4 Analysis

20 Points

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

Tools used:

1)International morse code chart from "https://morsecode.world/international/morse2.html"

2)python

Observations:

1). When we entered the 2nd level, we used the "go" command. After using this command we got a pattern which had only dots and dashes which looked like "Morse code". To decrypt it we used the morse code chart and got "CRYPTANALYSIS" which might be the key.

2). To reach the ciphertext we entered the "back" and then "read" command.

3). We tried caesar cipher and substitution cipher but the words that we were getting doesn't not make much sense. There was a sentence saying "Believe in yourself and PLAY FAIR" which gives us some hint regarding the use of Playfair cipher as an encryption algorithm.

4). The given ciphertext also doesn't contain the letter "J" so it strengthens the belief of using Playfair cipher. Thus we tried to decrypt the ciphertext using the Playfair cipher with "CRYPTANALYSIS" as the key.

5).After removing all special characters from cipher text we made the digraphs and applied the rules of this algorithm(listed in answer 4) to decrypt the ciphertext.

6). The decrypted text had some extra "X's" like "NEXED", "OUTX THE" and "WILXL". These extra X's needed to be removed to make sense of the whole text.

7). The special characters (. , " ", _) and whitespaces are likely to be un-encrypted.

Q5 Decryption Algorithm

15 Points

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

For decryption we used the following algorithm:

1). We created the key Square(5×5) . The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. We used the English language alphabets to fill the key square entries and each entry must be unique. One letter of the alphabet (usually J) is not used in the the table. If the plaintext contains J, then it is replaced by I.

2). The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabets from A to Z(that doesn't appear in the key) in order. Below is the table,

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

3) After removing the special character we start making pairs of letters known as bigrams/digraphs. If there is an odd number of characters a "Z" is added to the last character but we didn't have to add Z's.

4) For each bigram(pair) we follow the below rules:

i) if both the characters are in the same row we take the character which is left of each one. if the character is at the end we wrap around and take the letter at the other end(rightmost).

ii) If both the characters are in the same column we take the character which is above each one and if the character is at the end we wrap around and take the letter at the other end(bottommost).

iii) If neither of the rules is true then the two characters will make a rectangle and we take the characters opposite to each other horizontally.

Decrypted plaintext 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.'

After removing the extra X's and replacing the character "i" with "j"(since in place of 'IOY', 'JOY' make sense) we get final plain text i.e.,

'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

▾ decryption.ipynb Download

In [7]:

```
morse_to_eng = {
            '.-': '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',
         '.-.-.-': '.',
         '--..--': ',',
         '---...': ':',
         '..--..': '?',
         '.----.': "'",
         '-....-': '-',
         '-..-.': '/',
         '.--.-.': '@',
         '-...-': '='
        }


morse_code = "-.-. .-. -.-- .--. - .-
-. .- .-.. -.-- ... .. ..."

temp = morse_code.split(' ')
decrypted_message = ''

for c in temp:
    decrypted_message +=
morse_to_eng[c]

print("The decrypted message is :-
",decrypted_message)
```

```
The decrypted message is :- CRYPTANALYSIS
```

Assignment 2

● GRADED

GROUP

Ravi Shankar Das
Nimit Jain

Prashant Mishra

View or edit group

TOTAL POINTS

64 / 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	**10** / 10 pts
QUESTION 7	Code	**0** / 0 pts