

Q1 Commands

5 Points

List the commands was used in this level?

go, enter, pluck, back, give, back,
back, thrnxtzy, read

Q2 Cryptosystem

10 Points

What cryptosystem was used in the game to reach the password?

The cryptosystem used in this level is substitution permutation cipher.

The substitution mapping is:

Encrypted text: abcdefghijklmnopqrstuvwxyz

Original text: tviuchgpqb?skr?dawflmeoy?

Here, substitution is a mono-alphabetic substitution, and ? means unknown letter(any alphabet out of the remaining). All other special characters, punctuations(eg, '!', ',', etc) and space remain the same.

The permutation key is 43512.

Q3 Analysis

30 Points

What tools and observations were used to figure out the cryptosystem and the password? (Explain in less than 1000 lines)

After getting the cipher text by entering the above commands, we tried to decrypt it using substitution cipher, but we were not able to get any stable mapping. Then we thought that it might be a substitution-permutation network (SPN) as simple substitution was not making any sense. Since SPN networks break the text in blocks of fixed

length and the cipher text is 284, we tried to decrypt using the block length as 2,3,4,5.

As observed in the previous cipher texts, it usually contains the phrase "enter/speak the password". Keeping this assumption in mind, we observed that the following phrase in the cipher text might decode to "enter/speak the password" as the encrypted password follows it - "snafq vml lhvqpawr "

Next, we divided the entire cipher text into blocks of 5 and focused on the blocks with the above phrase. First, we tried to decrypt using "enter the password" as the plain text for the phrase "snafq vml lhvqpawr" but it didn't make any sense. Next, using "speak the password" we were able to get 11 mappings, and the permutation key as "43512". Now, using the obtained mappings and permutation in all the blocks, we found that some blocks had 3-4 letters decoded, using which we tried to make sense of the decoded text and were able to get. Finally, with the help of the obtained mappings and permutation key, we could find all the mappings mentioned above, taking all the blocks into consideration.

The analysis is explained in detail below -

Block	Cipher text	Plain text
1	lhqsn	---sp
2	afqvm	eakth
3	llhvq	epass
4	pawrn	word-

From block 1 and 3 we can say that 'l' maps to 's' and also that the first letter of the cipher text block gets permuted to the 4th position in the plain text block. Similarly, using blocks 1,2 we can say the either 'q' or 'h' maps to 'p' but on observing the 3rd block as well we come to a conclusion that 'h' maps to 'p' and the second letter of the cipher text block gets permuted to the 5th position in the plain text block.

Now, getting 2 permutation positions, we assumed that 'a' maps to 't', 'f' maps to 'h' and 'p' maps to 'd' using the above 4 blocks. These mappings were applied in the entire cipher text and on getting no inconsistency we continued

with the analysis.

Similarly, all other mappings and permutation were obtained. Further doing the analysis, we saw that the first block from the entire cipher text after getting 11 mappings and permutation key was as follows -

After Substitution - qmnjv -> akr?e

After Permutation - ?reak

We came to the conclusion that this word might be "break" and j maps to b. This assumption didn't create any inconsistency. Similarly, we were able to find other mappings as well.

Now, using the obtained mappings and permutation key we automated deciphering the whole cipher text using the code attached below.

Before using block length as 5 we also tried with block length as 2,3,4 but that didn't make any sense.

Q4 Password

5 Points

What was the final command used to clear this level?

the_magic_of_wand

Q5 Codes

0 Points

Upload any code that you have used to solve this level.

▼ spn_decoder.py

Download

```
1 # import numpy as np
2 ciphertext="qmnjvsanvwewcflctvprjtjtvpplvlfvxjavqil
3 altered_cipher = ciphertext
4 print("The cipher without any special characters
  is ")
5 print(altered_cipher)
6
```

```
7 print("The length of the cipher is
    "+str(len(altered_cipher)))
8
9 mapping = {
10     'a': 't',
11     'b': 'v',
12     'c': 'i',
13     'd': 'u',
14     'e': 'c',
15     'f': 'h',
16     'g': 'g',
17     'h': 'p',
18     'i': 'q',
19     'j': 'b',
20     'k': '?',
21     'l': 's',
22     'm': 'k',
23     'n': 'r',
24     'o': '?',
25     'p': 'd',
26     'q': 'a',
27     'r': 'w',
28     's': 'f',
29     't': 'l',
30     'u': 'm',
31     'v': 'e',
32     'w': 'o',
33     'x': 'y',
34     'y': 'n',
35     'z': '?'
36 }
37
38 temp = ""
39 for ch in altered_cipher.lower():
40     temp += mapping[ch]
41
42 print(temp)
43
44 plaintext = ""
45 for i in range(int(len(temp)/5)):
46     plaintext+=temp[i*5+3]
47     plaintext+=temp[i*5+2]
48     plaintext+=temp[i*5+4]
49     plaintext+=temp[i*5]
50     plaintext+=temp[i*5+1]
51
52
53 print("The plain text is")
54 print(plaintext+ temp[280:284])
55
56
```

Q6 Group name

0 Points

force_de_fem

Assignment 3


● Graded

Group

Srujana Sabbani

Kriti Majumdar

ASHEE JAIN

 [View or edit group](#)

Total Points

48 / 50 pts

Question 1

Commands

5 / 5 pts

Question 2

Cryptosystem

8 / 10 pts

Question 3

Analysis

R

30 / 30 pts

Question 4

Password

5 / 5 pts

Question 5

Codes

0 / 0 pts

Question 6

Group name

0 / 0 pts