Assignment 3

Graded

Group

Valeti Lokesh
Himanshu Karnatak
Bikash Saha
View or edit group

Total Points

50 / 50 pts

Question 1

Commands

5 / 5 pts

✔ **+ 5 pts** Correct (go enter pluck/pick back give back back thrnxxtzy read)

+ 0 pts Incorrect

– 2 pts Unnecessary story of commands presented but not a list of commands

+ 0 pts Click here to replace this description.

Question 2

Cryptosystem

10 / 10 pts

✔ **+ 10 pts** Correct (monoalphabetic substitution and permutations cipher with block length 5)

– 2 pts Not mentioning monoalphabetic

– 2 pts Not mentioning block length

+ 0 pts Incorrect

Question 3

Analysis

Resolved **30** / 30 pts

- ✔ **+ 3 pts** Frequency analysis
- ✔ **+ 2 pts** Figured out the cryptosystem
- ✔ **+ 2 pts** Reason behind choosing block size 5
- ✔ **+ 5 pts** Identified permutation map. Permutation (Encryption) key: 43512 or 32401(when 0 is the first index) or Decryption Key: 45213.
- ✔ **+ 8 pts** Detailed cryptanalysis
- ✔ **+ 5 pts** Substitution map
- ✔ **+ 5 pts** Consider all cases, like uppercase, lower case and special characters, space etc.

+ 0 pts Wrong answer.

− 2 pts Just mentioned frequency analysis but the analysis isn't provided.

− 3 pts No mention of case of lowercase and special characters.

− 2 pts Not give a proper analysis.

Regrade Request **Submitted on: Apr 18**

Dear Sir,

Though we used Index of Coincidence along with Frequency Analysis to begin our analysis, we mentioned only Index of Coincidence, as its result (value of 0.057) is enough to determine presence of Monoalphabetic cipher. Mentioning Frequency Analysis did not seem to provide any additional information about identification of cryptosystem.

We used frequency distribution to find the mappings similar to assignment#1. This is mentioned in Point 6 where we describe:
"Frequency distribution tells us that "a -> t" is a fair possibility."

It may be our oversight to not write 'frequency analysis' explicitly, considering it implict in deciphering any monoalphabetic cipher.

In view of above kindly award +3 marks that as per rubric, were left out due to absence of Frequency Analysis.

Thank You.

Done

Reviewed on: Apr 19

Question 4

Password

5 / 5 pts

✔ **+ 5 pts** Correct (the_magic_of_wand)

+ 0 pts Incorrect

Question 5

Codes

0 / 0 pts

✔ **+ 0 pts** Correct

Question 6

Group name

0 / 0 pts

✔ **+ 0 pts** Correct

Q1 Commands
5 Points

List the commands was used in this level?

3 ,go , enter , pluck , c , c , back , give , back , back , thrnxxtzy , read

Q2 Cryptosystem
10 Points

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

In the game, a cryptographic system was employed to derive the password, utilizing a combination of both monoalphabetic substitution and permutation ciphers.

1)Mono-Alphabetic Substitution
Cipher Text to Plain Text.
a : t , b : v , c : i , d : u , e : c , f : h , g : g , h : p , i : q , j : b , k : z , l : s ,m : k , n : r , p : d , q : a , r : w , s : f , t : l , u : m , v : e, w : o , x : y , y : n

2) Permutation cipher:
Alongside the substitution cipher, a permutation technique known as a transposition cipher was employed. This method involved rearranging the order of characters within the ciphertext. Specifically, a transposition cipher with a block length of 5 was utilized. The encryption key, denoted as 12345, indicated that the ciphertext was divided into blocks of 5 characters each, and the arrangement of characters within each block was shuffled based on the sequence 45213. Similarly, for decryption, the key remained 12345, but with a different permutation sequence: 43512.

On Combining these two, Substitution and Permutation cipher is used.

Q3 Analysis
30 Points

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

1 The Given cipher text is made of letters from english language alphabets. We started with ceaser cipher with different keys but could not figure out valid words. Then we calculated the Index of coincidence for this text is 0.057, which is quite close to standard for a monoalphabetic substituion. We thought that it is monoalphabetic substitution but Cipher text also has three letter words like 'taa' and 'wwd' which do not relate to usual three letter words in the English language text. Hence, we concluded that there is a mono alphabetic substitution present in the cipher text but the letters are shuffled. Thus increasing a possibility of Substitution and Permutation Cipher.

2. Next step was to figure out the block length and sequence for permutation. With no clue at hand, we looked for a possible word in the text. The text could contain the word "password", which is an 8 letter word. There is only one 8 letter word in this cipher text "lhvqpawr". It is possible that this letter corresponds to location of substituted and permuted "password".

3. If our hypothesis is correct, then the correct inverse permutation will give same letter at the location of 'ss' in substring password. i.e. at location 2 and 3 will have same letter (substitution of 's') after inverse permutation.

4. Based on this postulate, we iterate through multiple block sizes and all possible combinations and stop when a match is found as mentioned in step 3.

5. We start finding the matches from block size =5. "vqllwrnp" and similar results by various inverse permutations match our hypothesis listed in step 3. It indicates that 'l -> s'. But it doesn't give us a unique permuation. The length of the cipher text after removing all the white spaces and puntuation is 284, So to make the size divisible by 5, we pad on letter at the end i.e x.

6. We look at the cipher text again. The word "lhvqpawr" follows three letter word "vml". Which increases a possibility of it being "vml lhvqpawr" -> "the password". We already guessed "v -> e" in our Step. Frequency distribution tells us that "a -> t" is a fair possibility. Hence we run our permutaion analysis once more so that after inverse permutation, the three letter word starts with 'a'

(being 't') and ends with 'v' (being 'e').

7. Anaysis mentioned at Step 6 reduces our possible permutations to
afvhqllrwnp (4, 3, 5, 1, 2)
afvqhllrnwp (4, 5, 3, 1, 2)
This reveals a few more substitutions 'f -> t' (making the first three letter word 'the') and 'q -> a' (As 'q' in cipher text has similar freqency of occurance as of 'a' in standard english text)

8. Hence our permutation key set is reduced to (4, 3, 5, 1, 2). Using this we now rewrite the cipher text.
"jnvqmvnwsafclewpvrcttjvjtvllvpjxafvlidvqmxlhcncanvlcpcygcyafvfwtvgwqfvqpq
ypscypqrqxwsjnvqmcygafvlhvttwyfcueqlajxafvvbctkqssqnafvlhcncawsafveqbvu
qyclqtrqxlrcafxwdscypafvuqgcerqypafqarctttvaxwdwdawsafveqbvlcarwdtpuq
mvxwdquqgcecqyywtvllafqykqssqnlhvqmafvhqllrwnpafvuqgcewsrqypawgwafn
"

9. We apply standard monoalphabetic substution cipher now as we explained in detail in level 1. The key for same comes out to be:
cipter text : Plain text
a : t ,
b : v ,
c : i ,
d : u ,
e : c ,
f : h ,
g : g ,
h : p ,
i : q ,
j : b ,
k : z ,
l : s ,
m : k ,
n : r ,
p : d ,
q : a ,
r : w ,
s : f ,
t : l ,
u : m ,

v : e,
w : o ,
x : y ,
y : n
'_':'_'
'.' : '.'
',': ',
'!': '!'

Punctuations and special symbols are neither substituted nor permuted. So thay map to themselves.

10. And the deciphered cipher text becomes:
"breakerofthiscodewillbeblessedbythesqueakyspiritresidingintheholegoaheadandfindawayofbreakingthespellonhimcastbytheevilzaffarthespiritofthecavemanisalwayswithyoufindthemagicwandthatwillletyououtofthecavesitwouldmakeyouamagiciannolessthanzaffarspeakthepasswordthemagicofwandtogothroughy"

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.

No files uploaded

Q6 Group name

0 Points

Mod3