Assignment 1

● Graded

Group

RAJ AGRAWAL
HRISHITA AGRAWAL
RAHUL NARAYAN
View or edit group

Total Points

40 / 50 pts

Question 1

Commands

5 / 5 pts

✔ **+ 5 pts** Specifying the correct set of commands

+ 0 pts Correct

Question 2

Cryptosystem

3 / 5 pts

✔ **+ 3 pts** The nature of the substitution cipher is not mentioned, Substitution cipher could be of Monoalphabetic or Polyalphabetic.

+ 5 pts Correct Cryptosystem

+ 0 pts Incorrect

Question 3

Analysis

20 / 25 pts

✔ **+ 10 pts** Using frequency analysis to conclude that its substitution cipher

✔ **+ 5 pts** Step by Step decryption from cipher to plain

✔ **+ 5 pts** Finding the mapping in the cryptosystem used by analyzing bigrams and trigrams (or small words)

✔ **+ 5 pts** Giving mathematical explanation for the shift in the digits (We obtained the from the plaintext after decrypting it with frequency analysis, which claims that the digits are shifted by "8" places. However, because 8 is a digit, it is obvious that 8 is also encrypted by some shifting. _Assume the number that was shifted to 8 is X. Because X is the key here, we can assert that X is shifted by X places, resulting in 8. The problem is written as follows in mathematical notation: X+X=8mod10 (mod 10 because there are 10 digits only, aka 0,1,2,3,4,5,6,7,8,9). The digits satisfying the above equation is 4 and 9. Without loss of generality, let us assume that X=9. Then the method of decryption tends to find two numbers Y and Z, such that Y+9=0mod10 and Z+9=3mod10. Therefore, leading us Y=1 and Z=4. For this case the decrypted password showed incorrect. So we tried the other value of X=4. Then the method of decryption tends to find two numbers Y and Z, such that Y+4=0mod10 and Z+4=3 mod10. Therefore, leading us as Y=6 and Z=9. For this case the decrypted password is showed correct.)

+ 0 pts incorrect/ Directly using online tool to decipher.

💬 **− 5 pts** (-3) How did you conclude that it is substitution cipher only?

(-2) Digits could have been shifted by nine as shifting '9' by nine places will generate '8'. The correct equation will be (x + x) mod 10 = 8.

Question 4

Mapping

7 / 10 pts

✔ + 3 pts Plaintext Space and cipher text space is the set of all strings containing English alphabets, numbers, punctuation marks, and spaces.

– 1 pt No mention of the existence of "digits" in the ciphertext space and plaintext space

✔ – 1 pt No mention of the existence of "punctuation marks" in the ciphertext space and plaintext spcae

✔ + 7 pts The mapping used for alphabets and numbers.

– 3 pts Mistakes or missing in mapping of alphabets

✔ – 2 pts Mistakes or missing in mapping punctuation marks

– 2 pts Mistakes or missing in mappings of numbers.

+ 0 pts Incorrect

+ 3 pts mapping only done for alphabets

Question 5

Password

5 / 5 pts

✔ + 5 pts Correct

✔ + 0 pts Incorrect

Question 6

Codes

0 / 0 pts

✔ + 0 pts Correct

Question 7

Team Name

0 / 0 pts

✔ + 0 pts Correct

+ 0 pts Incorrect

Q1 Commands
5 Points

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

1.climb
2.read
3.enter
4.read

Q2 Cryptosystem
5 Points

What cryptosystem was used at this level?

Symmetric key encryption-substitution cipher.

Q3 Analysis
25 Points

What tools and observations were used to figure out the cryptosystem?

NOTE: Failing to provide proper analysis would result in zero marks for this assignment.

We analysed the frequencies of different letters used in the cipher text and according to that we mapped the most frequent letters of the cipher text to the known most frequent letters which are used in general English literature.That is, we did frequency analysis here. Then to get the decrypted message we used substitution cipher. For example-we replaced the most frequent letter 'y', of the cipher text by the most frequent letter 'e' of general english literature. We also replaced some common 2 and 3 letter words like-'the' in place of 'mey' as we already got 'y' replaced by 'e' and 'm' by 't', then we concluded that it has high chance that it can be 'the'.

After decrypting all the English alphabet we get a plaintext which says "This message is simple substitution cypher in which digit have been shifted by 8 places." and till now we did not decrypted the digit 8. So let's assume that each digit is shifted by x then x is also shifted by x in ciphertext and hence by above two statements we concluded that ->
x+x=8 as digit 8 is obtained by shifting x to x places
So we get x=4.
That means each digit in ciphertext need to shift 4 places backwards ,as Cyphertext obtained by shifting the digit of plaintext forward by 4 places.
So, digit '0' is replaced by digit '6'
And digit '3' is replaced by digit '9'.
And thus we get our Ciphertext totally decrypted to plaintext.

Q4 Mapping
10 Points

What is the plaintext space and ciphertext space?
What is the mapping between the elements of plaintext space and the elements of ciphertext space? (Explain in less than 100 words)

Plain text space-{t, h, i, s, e, r, n, g, o, m, a, f, u, b, c, y, v, d, w, l, p, q, 6, 9, 4}.
Cipher text space-{m, e, w, a, y, t, s, i, p, j, g, b, x, h, r, k, v, o, u, n, f, d, 0, 3, 8}.

The mapping is in such a way:

m-t; e-h; w-i; a-s; y-e; s-r; h-n; r-g; g-o; j-m; p-a; t-f; n-u; o-b; i-c; x-y; b-v; u-d; v-w; k-l; f-p; d-q; 0-6; 3-9; 8-4.

Q5 Password
5 Points

What is the final command used to clear this level?

tyRgU69diqq

Q6 Codes
0 Points

Upload any code that you have used to solve this level

No files uploaded

Q7 Team Name
0 Points

encrypted_team.