Assignment 2

● Graded

Group

HRISHITA AGRAWAL
RAHUL NARAYAN
RAJ AGRAWAL

View or edit group

Total Points

50 / 65 pts

Question 1

Commands

10 / 10 pts

✓ **+ 10 pts** commands: 1. read back go 2. go back read , 3. go go read
(answer such as for ciphertext: read and for key : go , is also correct)

+ 10 pts command : read, full marks only if the student tried to solve the assignment correctly without the provided key length

Question 2

Cryptosystem

10 / 10 pts

+ 0 pts Incorrect

✓ **+ 10 pts** Correct Cryptosystem.: Vigenere Cipher with Key jcjcffccb.

− 2 pts Wrong Key

Question 3

Analysis

Resolved **15** / 20 pts

✓ **+ 5 pts** Proper mention about if they tried shift cipher, mono alphabetic substitution cipher etc. before concluding its poly alphabetic substitution cipher.

✓ **+ 5 pts** Mention about key 9 2 9 2 5 5 2 2 2 1(jcjcffcccb), Key length 10 and working with key length 10 anywhere in Q4 or Q3

+ 5 pts Assigning them 9 2 9 2 5 5 2 2 2 1 as A to 0, B to 1, to get the key JCJCFFCCCB anywhere in Q4 or Q3 / Doing frequency analysis to for the mapping and therefore finding the key anywhere in Q4 or Q3

✓ **+ 5 pts** Use of the Kasiski test / Index of Coincidence/Repetition of same blocks to figure out the cryptosystem anywhere in Q3 and Q4

+ 0 pts Incorrect

A to mapped to 1 in mapping section, which is not true and 3rd rubric can't be mapped.

Regrade Request **Submitted on: Feb 21**

respected sir,
Sir we assigned 9292552221 as key jcjcffcccb in the qn.4 and i also write the logic that we have to assign like-(word position-1) like a to 1-1=0 and like that.
sir please check this once again.
thank you
Raj, Hrishita, Rahul

" Word position in English dictionary -1" is wrong. Don't ask for grading for writing gibberish.

Reviewed on: Feb 21

Question 4

Decryption Algorithm

Resolved **5** / 15 pts

+ 5 pts Mentioning removal of spaces/punctuation etc., or mentioning mapping of them is fixed and mentioning about "spaces" while calculating the distance of blocks anywhere in Q3 and Q4

✓ **+ 5 pts** mentioning (plaintext alphabet + key) mod 26 = cipher text alphabet or (cipher text - key) mod 26 = plaintext anywhere in Q3 or Q4

+ 5 pts Mentioning breaking the ciphertext into 10-size blocks and giving a detailed description of decoding or providing codes to get the plaintext anywhere in Q3 and Q4

✓ **+ 0 pts** Incorrect

+ 5 pts Correct answer found but explanation is not found.

No assignment specific explanation

Regrade Request **Submitted on: Feb 21**

sir we thought we have to explain the algorithm using an example so we took a plaintext and then we mentioned that we have to repeat this key and add the no. value to obtain the cipher text which is actually similar to making block of key size and then add the no. value of key to plaintext
we also mentioned that for obtaining plaintext we have to shift letters to left by key value.
and also sir we were not aware of that what to write in algorithm part as it is first assignment which asking for the algorithm, sir we will take care of that from the next time.
please regrade this question once do the needful.
Thank you
Rahul , Hrishita ,Raj

i liked your way of taking way of taking example andexplainting it , but you are supposed to answer using the ciphertext given . Considering your explanation , its only fits rubric 2, not other rubrics are not fitting . adding +5 therefore.

Reviewed on: Feb 21

Question 5

Password

10 / 10 pts

+ 0 pts Incorrect

✓ **+ 10 pts** Correct

Question 6

Codes

0 / 0 pts

✓ **+ 0 pts** Correct

Question 7

Team Name

0 / 0 pts

✓ **+ 0 pts** Correct

+ 0 pts Incorrect

Q1 Commands

10 Points

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

1. go
2. back
3. read

Q2 Cryptosystem

10 Points

What cryptosystem was used in this level?

the cryptosystem used in this level is polyalphabetic substitution cipher-Vigenere cypher.

In this we use a key and repeat it again and again and add the letter values to the plaintext letter

eg: plaintext : encrypted_team ;key =123
key repeatition : 123123123 1231
ciphertext: fpfsasugg ugdn

Q3 Analysis

20 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.

firstly we observed the frequency of the letter and then we tried to decrypt it by using frequecy analysis i.e. substitution cypher but as the frequency of letter are nearly similar so we found nothing from that. then, we observed it closely and we found that some words are repeating themselves like- cjjwg,vjg,cjn etc. so we came up with the thought that they might be the same word in plaintext as well. also we found like many words having common starting or ending like-vjg and yvg, cjn and cjntj. so then we came up with an idea that this is type of substitution cypher only.so we felt there is some more information required to solve this(like key) so we tried more commands and we found that there is another text coming up when we gave "go" command instead of "read". The text says like - we had to bow to the spirit of chamber keeper then to slowly look up and count the no. of lines in horizontal dimension so we did as it is. There is 9 lines in the last row and 2 lines in second last and we counted liked that until we reached the topmost line. We got a number like"9292552221". we thought that it has some use in decrypting the text which came upon when we gave "read" command earlier. so we went back to ciphertext and then we count the no of letters in between repeating words like "cjjwg" and we observed that the length between these words is completely divisible by the key length like-The length of " cjjwg ku wnth nnyvng kxa" is 20 and our key length is 10, as 20 is divisible by 10 the above property is satisfied. Then we got to know that it must be vigener cipher because only vigenere cipher can have this kind of property. And when we decrypted it using the above key we got our plaintext.

Q4 Decryption Algorithm

15 Points

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

For getting the plaintext we used Vigenere cypher
It actually works as follows- we are given with some key to encrypt. Then, by using that key again and again (repeatedly) we have to encrypt the plaintext and same goes for decryption also.
for ex:-plaintext="you are right" and the key ="135"
then you cyphertext is simply just adding "135' repeatedly to the plaintext.
so,
plaintext= you are right
algorithm=135 135 13513
cyphertext=zrz buj slliw
we just obtained the cyphertext by shifting letters to right by no. written below that letter.
the plaintext obtained by deciphering the cyphertext is as follows:

> Be wary of the next chamber, there is very little joy there.
> Speak out the password "the_cave_man_be_pleased" 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.

and the key used to decipher this text as follow"9292552221" we can think of this key in the form of English alphabet as follows "jcjcffcccb" ,to use this we have to simply shift the word by " " word position in English dictionary -1". like j is at 10th place, so we shift letter by 9 place.

Q5 Password

10 Points

What was the final command used to clear this level?

the_cave_man_be_pleased

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