Assignment 2

● Graded

Group

Himanshu Karnatak
Bikash Saha
Valeti Lokesh
View or edit group

Total Points

65 / 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)Correct

+ 0 pts Incorrect

Question 2

Cryptosystem

10 / 10 pts

✔ **+ 10 pts** Correct Cryptosystem.: Vigenere Cipher

+ 0 pts Incorrect

– 2 pts Wrong Cryptosystem

Question 3

Analysis

Resolved **20** / 20 pts

✔ **+ 5 pts** Grading comment:
Proper mention about if they tried shift cipher, mono alphabetic substitution cipher etc. before concluding its poly alphabetic substitution cipher.Correct

✔ **+ 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

Regrade Request **Submitted on: Apr 08**

1. We have described the assignment A to 0, B to 1, .. Z to 25 and deduction of the key in point number 6 of this section.

Reference:
Point-6. "If we assign numerals to every alphabet such as a=0, b=1, ... z=25, the set deduced in previous step translates to the keyword: KCGCDFCCB"

Yet, +5 marks have not been awarded.

2. In point 3 of this section we have presented our result of Index of Coincidence test and used it to deduce that cryptosystem is a polyalphabetic cipher as opposed to a monoalphabetic one.

Reference:
"Point-3. Then we calculated index of conincidence for all the alphabets used in this cipher. The index of coincedence is calculated as 0.04236. This strengthens our confidence in the idea that a POLYALPHABETIC CIPHER is used to create this ciphertext."

Yet, +5 marks have not been awarded.

In view of above kindly regrade the assignment and award due marks.

Thank you.

ok

Reviewed on: Apr 08

Question 4

Decryption Algorithm

Resolved **15** / 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 Q4Correct

✔ **+ 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

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

+ 0 pts Incorrect

Regrade Request **Submitted on: Apr 08**

1. We have mentioned removal of spaces, underscores, and punctuations in point number 3.5 of this section.

Reference:
"3.5) String s = cipher.replaceAll(" ", "").replaceAll("_", "").replaceAll(",", "").replaceAll("\"", "").replaceAll("\.", "");: Removes spaces, underscores, commas, double quotes, and fullstop from the ciphered text."

Yet, due +5 marks have not been awarded

2. We have mentioned in point 3.7 that loop "ensures that values remain within the range of the English alphabet". It is also reflected in the supporting code where mod 26 (%26) operation is used to ensure the same.

Reference:

"POINT-3.7) The loop calculates the decrypted character by calculating the position of the decrypted character after considering the Vigenere cipher shift, ensuring it stays within the range of the English alphabet and then we transform the position "

CODE:LINE-10: int k=(s.charAt(i) -key.charAt(i%(key.length()))+26)% 26;

Yet, due +5 marks have not been awarded

3. Approach of breaking the ciphertext into 9 size block is clearly mentioned in point 2 of the section. The code used for decoding is also described in detail in the points that follow.

Reference:
"POINT-2. To decrypt we extract all alphabets from the cipher text and divide them into blocks of size 9. Every letter in the block is decrypted by shifting it by the number represented by corresponding letter in keyword."

we have also added the code in the code section(Q6).

Yet, due +5 marks have not been awarded

In view of above kindly regrade the assignment and award due marks.

Thank you.

I increased 5 marks but you did not give a proper analysis.

Reviewed on: Apr 10

Question 5

Password

10 / 10 pts

✔ **+ 10 pts** Correct

+ 0 pts Incorrect

Question 6

Codes

0 / 0 pts

✔ **+ 0 pts** Correct

Question 7

Team Name

0 / 0 pts

✔ **+ 0 pts** Correct

Q1 Commands
10 Points

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

2
go
back
read

Q2 Cryptosystem
10 Points

What cryptosystem was used in this level?

A symmetric key encryption cryptosystem with following components:

Encryption/Decryption Algorithm: Polyalphabetic substitution- Vigenere cipher

Encryption/Decryption Key: KCGCDFCCB

PlainText: 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.

CipherText: Lg ccud qh urg tgay ejbwdkt, wmgtf su bgud nkudnk lrd vjfbg. Yrhfm qvd vng sfuuxytj "vkj_ecwo_ogp_ej_rnfkukf" wt iq urtuwjm. Ocz iqa jdag vio uzthsivi pqx vkj pgyd encpggt. Uy hopg yjg fhkz arz hkscv ckoq pgfn vu wwygt nkioe zttft djkth.

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.

Observations and Analysis:
0. We look at the clues given in the game to deduce some information. The hint is to "Bow, and then slowly look up. Count the number of lines in horizontal dimension --". There are 9 horizontal lines in the image. And every line has some lines in it. Starting from the bottom line, if we count the number of lines in each horizontal line we get the following set: {10,2,6,2,3,5,2,2,1}. This set has 9 elements in it. This set is expected to have some valuable information.

1. Next we reach the cipher text. Cipher appears to be made of alphabets from English language. Use of punctuations and spaces is also inline with the sentence formation structure in standard English text. Our first step is to determine if a monoalphabetic or polyalphabetic cipher is used in creating this cipher.

2. We started with frequency analysis of alphabets used in the cipher. The result for some of the most frequent letters is :
'g' : 8.65 %, 'u' : 7.03 % 't' : 7.03 % 'k' : 6.49 % 'j' : 5.41 % 'd' : 4.86 % 'f' : 4.86 % 'v' : 4.86%
'c' : 3.78% 'h' : 3.78% 'y' : 3.78% 'w' : 3.78% 'n' : 3.78% 'o' : 3.78%
This distribution does not match distribution of alphabets in English language. Therefore we conclude that Monoalphabetic Cipher is NOT used to create this cipher. It increases the possiblity of it being a Polyalphabetic cipher.

3. Then we calculated index of conincidence for all the alphabets used in this cipher. The index of coincedence is calculated as 0.04236. This strengthens our confidence in the idea that a POLYALPHABETIC CIPHER is used to create this ciphertext.

4. We tried some common polyalphabetic ciphers such as AutoKey, PlayFair, and Vignere cipher next. PlayFair and Autokey did not give any useful lead. The we tried Vignere, where a the plain text is divided into same sized blocks and each letter in a block is encrypted using a ceaser cipher with a different key. Keys for all letters in a block is usually written as a KEY WORD. And each PT letter in a block is substituted by the letter obtained by applying ceaser

cipher to that PT letter. Key for this ceaser cipher is determined by the number represented by corresponding letter in the KEY WORD.

5. To decipher the text we needed the block size and the value of keys for ceaser ciphers for every letter in a block. We used the set obtained from the hint in step 0 to deduce a key.

6. If we assign numerals to every alphabet such as a=0, b=1, ... z=25, the set deduced in previous step translates to the keyword: KCGCDFCCB

7. This keyword is then used to decipher the ciphertext using a decyption algorithm for a cryptosystem of polyalphabetic cipher with block size=9 and keyword= KCGCDFCCB. This cryptosystem is also known as VIGNERE CIPHER.

Q4 Decryption Algorithm
15 Points

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

1. From our analysis, we know a possible keyword. This gives us size of a block and the key for substituting every letter in it. (For keyword KCGCDFCCB, block size = length of keyword = 9).

2. To decrypt we extract all alphabets from the cipher text and divide them into blocks of size 9. Every letter in the block is decrypted by shifting it by the number represented by corresponding letter in keyword.

3. Following is a breif description of the decryption algorithm used enclosed in section-6:

3.1) String key = "kcgcdfccb";:This is the key used for the Vigenere cipher. The key is repeated if the length of the key is shorter than the length of the ciphered text.

3.2) String original = "";: Initializes an empty string to store the decrypted text.

3.3) String Cipher = "Lg ... djkth.";: The input ciphered text that you want to decrypt.

3.4) String cipher = Cipher.toUpperCase();: Converts the entire ciphered text to uppercase for consistency in comparison.

3.5) String s = cipher.replaceAll(" ", "").replaceAll("_", "").replaceAll(",", "").replaceAll("\"", "").replaceAll("\\.", "");: Removes spaces, underscores, commas, double quotes, and fullstop from the ciphered text.

3.6) Now Forloop iterates iterates through each character in the cleaned-up ciphered text.

3.7) The loop calculates the decrypted character by calculating the position of the decrypted character after considering the Vigenere cipher shift, ensuring it stays within the range of the English alphabet and then we transform the position into ascii character by adding 'A' and appends it to the original string.

3.8) And finally it Prints the decrypted text.

4. Deciphered plain text (after adding spaces, punctuations, special symbols, and cases as per ciphertext):

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.

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

decryption.java Download

```
1  class HelloWorld {
2      public static void main(String[] args) {
3          String key = "kcgcdfccb";
4          String original = "";
5          String Cipher = "Lg ccud qh urg tgay ejbwdkt, wmgtf su bgud nkudnk lrd
   vjfbg. Yrhfm qvd vng sfuuxytj \"vkj_ecwo_ogp_ej_rnfkukf\" wt iq urtuwjm. Ocz iqa
   jdag vio uzthsivi pqx vkj pgyd encpggt. Uy hopg yjg fhkz arz hkscv ckoq pgfn vu
   wwygt nkioe zttft djkth.";
6          String cipher = Cipher.toLowerCase();
7          String s = cipher.replaceAll(" ",
   "").replaceAll("_","").replaceAll(",","").replaceAll("\"","").replaceAll("\\.", "");
8          int n= s.length();
9          for(int i =0; i<n ; i++){
10             int k=(s.charAt(i) -key.charAt(i%(key.length()))+26)% 26;
11             k+='a';
12             original+=(char)k;
13         }
14         System.out.println(original);
15     }
16 }
```

Q7 Team Name

0 Points

mod3