Q1 Commands
10 Points

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

1.read (to read ciphertext)
2.back (to go back)
3.go (to get the key)

Q2 Cryptosystem
10 Points

What cryptosystem was used in this level?

Vigenère cipher

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.

For finding the key,

we get the following symbol on typing 'go'

We Count the number of lines in horizontal dimension - By counting lines from Top to Bottom, the no. of lines are 1-2-2-2-5-5-2-9-2-9, and Doing Bottom to Top, the no of lines are 9-2-9-2-5-5-2-2-2-1.

These numbers should definitely mean something, so we map the letters to their equivalent numbers in the English alphabet (like 0->A , 1->B, and so on). By doing this we get ('bcccffcjcj'="1-2-2-2-5-5-2-9-2-9") and ("jcjcffcccb"=9-2-9-2-5-5-2-2-2-1).

We thought these are the password to pass the level, but It was not. We thought these could be the key , so we decided to decrypt the text using both keys.

While using both 'bcccffcjcj' and 'jcjcffcccb', the key 'jcjcffcccb' gives some meaningful plain text. (it also makes sense since the instructions mentioned looking up)

So the key is = 'jcjcffcccb'.

For finding the type of cipher used,

First, we tried monoalphabetic cipher, but that did not work. We eliminated permutation cipher because the frequency of letters in ciphertext differed from the frequency of English letters.

We then moved on to polyalphabetic ciphers.

We knew there are some cipher that work on frequency of bigrams and trigrams rather than individual letters. So, we checked the frequency of bigrams and trigrams. First, we thought it was ‘Playfair Cipher’ but then Playfair has a property that either i or j appears in ciphertext not both but then our ciphertext has it so it wasn’t Playfair.

Next we thought of Vigenere cipher. We noticed repeating patterns like 'cjj' and 'cjn' at a gap of multiples of 10 (length of our key) like 20,40 etc. which also helped.

To ensure that Vigenere cipher was used, we found the index of coincidence of the ciphertext using an online tool (index of coincidence). The index of coincidence came out to be 0.04877.

Friedman’s test says that if index of coincidence lies in the range 0.0385 to 0.065, then it is possibly Vigenere cipher. Vigenere Cipher uses a simple form of polyalphabetic substitution.

Solving the cipher text, using the key 'jcjcffcccb' and decrypting using Vigenere cipher decryption algo, the plain text is
"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."

We use the password mentioned in the plain text to pass the level.

Q4 Decryption Algorithm
15 Points

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

To decrypt the text using Vigenere cipher, we use the following equation:
Decryption: Di = (Ei - Ki + 26) mod 26

We know that the key is 'jcjcffcccb'.

Explanation:
We take the first letter of the ciphertext and the first letter of the key, and subtract their value (letters have a value equal to their position in the alphabet starting from 0). If the result is negative, add 26 (26=the number of letters in the alphabet), the result gives the rank of the plain letter.

For example, Take the first letters of the given ciphertext 'k' (value = 10) and the key 'j' (value = 9) and subtract them (10-9=1), the letter of value 1 is 'b'.
Similarly, for the second letter of the ciphertext 'g' (value=6) and the second letter of the key 'c' (value=2), Di= 6-2=4 => 'e', so the next letter of the plaintext is 'e'
Continue with the next letters of the message and the next letters of the key, when arrived at the end of the key, go back the the first key of the key.

There is another method to solve the Vigenere cipher using a double entry square table.

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.

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

team_rocket

Assignment 2

Graded