Q1 Commands
10 Points

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

read->ciphertext
go->counting keys

Q2 Cryptosystem
10 Points

What cryptosystem was used in this level?

Vigenere 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.

It took us some trails of different methods to finally conclude that it is a vigenere Cipher.

> we first tried with frequency analysis but could not infer anything from it.
> we failed with caeser cipher.
> After trying other methods like shuffling the word.

> this gave an idea that it is not a normal substitution cipher.
>when we get the code $\mathbf{9,2,9,2,5,5,2,2,2,1}$ when after backward shifting the ciphertext we got the plaintext.
> the observation that the ciphertext is polyalphabetic gave a hint that it is a vigenere cipher.

Q4 Decryption Algorithm
15 Points

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

****
********** The answer consists of three parts**********
[definition of vigenere cipher]-[how we decrypted the message]-[plaintext]
****

1) Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère square or Vigenère table.

>The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.

>At different points in the encryption process, the cipher uses a different alphabet from one of the rows.

>The alphabet used at each point depends on a repeating keyword.

2) We get $\mathbf{9,2,9,2,5,5,2,2,2,1}$ when we bow down and count the horizontal lines in the figure. This can be something related to the ciphertext. Trying shifting the ciphertext

forward shifting

$$\mathbf{kg\ \ fcwd\ qh\ vin\ pnzy -> ti\ oebi\ sj\ xj}$$

This does not make sense.

backward shifting

$$\mathbf{kg\ \ fcwd\ qh\ vin\ pnzy -> be\ wary\ of\ the\ next}$$

This is giving some sense and when we reach the end of the code then we have to decrypt by using cyclicity. This implies that this is a vigenere cipher with $\mathbf{9,2,9,2,5,5,2,2,2,1}$ as the key.

3)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

Q5 Password
10 Points

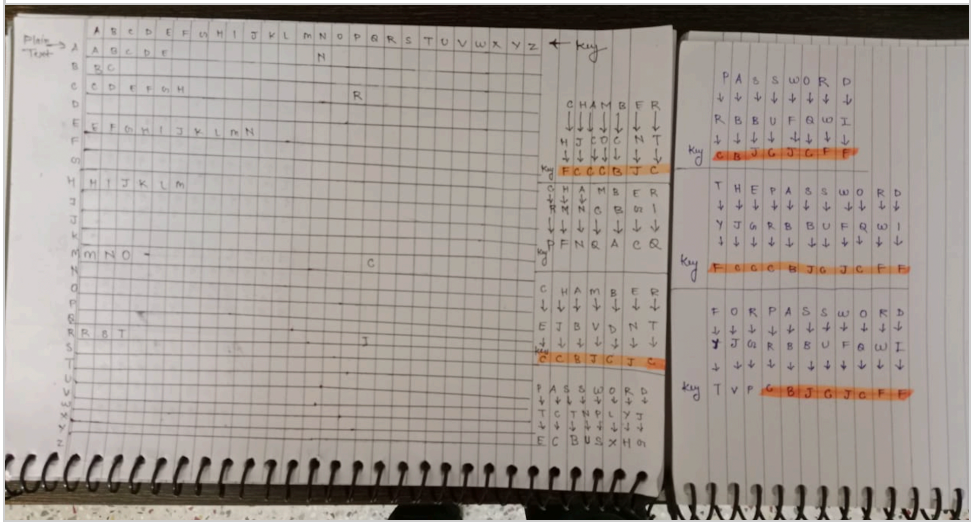
What was the final command used to clear this level?

the_cave_man_be_pleased

Q6 Codes
0 Points

Upload any code that you have used to solve this level

Screenshot 2023-02-08 at 7.46.56 PM.png Download



Q7 Team Name
0 Points

the_cryptonics

Assignment 2

Graded

Group

TANEYA SONI
ABHISHEK KUMAR PATHAK
SONAM
View or edit group

Total Points

50 / 65 pts

Question 1

Commands **10** / 10 pts

Question 2

Cryptosystem **10** / 10 pts

Question 3

Analysis R **10** / 20 pts

Question 4

Decryption Algorithm R **10** / 15 pts

Question 5

Password **10** / 10 pts

Question 6

Codes **0** / 0 pts

Question 7

Team Name **0** / 0 pts