

Q1 Commands**10 Points**

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

go
go
read

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.

We first tried frequency analysis, but it was unsuccessful. We repeated the questions several times before counting the lines on the boulder to find the key. If we bow and look at the boulder, in addition to the horizontal lines, we will also observe vertical and diagonal lines. For instance, "-----" counted as 9. Similarly, if we count all the lines from bottom to top we would get 9,2,9,2,5,5,2,2,2,1. So, the required key is "JCJCFCCCB" to convert ciphertext to plaintext. After trying various substitution ciphers such as Playfair cipher, repeating xor cipher, and vigenere cipher, we found out that using vigenere cipher we can decrypt the ciphertext to plaintext. The key for the Vigenere cipher is a

text string. The plaintext's alphabets are shifted by converting each alphabet in the key to its corresponding numeric value. The Vigenère cipher uses a repeating key to encrypt the message, while the Playfair cipher uses a 5x5 matrix to encode pairs of letters. Also, Playfair encrypts pairs of letters but we can see single letters are encrypted so we eliminated the Playfair cipher from consideration.

Q4 Decryption Algorithm

15 Points

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

We set a numeric value of "0 to 25" for each letter of the alphabet, ranging from "a" to "z." Now, we subtracted the key values from the cipher text's numerical values.

for example:

"kg fcwd qh vin pnzy" is the ciphertext

(10,6,5,2,22,3,16,7,21,8,13,15,13,25,24). Taking the difference modulo 26 with respect to the key i.e.

(9,2,9,2,5,5,2,2,2,1,9,2,9,2,5,...), we have

(1,4,22,0,17,24,14,5,19,7,4,13,4,23,19), which is the same as "be wary of the next chamber." In this way, we got the entire plaintext which 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."

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

da_vinci

Assignment 2

● Graded

Group

ANSHUL SHARMA
SUMIT KUMAR CHAUDHARY
PRADEEP CHALOTRA

 [View or edit group](#)

Total Points

55 / 65 pts

Question 1

[Commands](#)

10 / 10 pts

Question 2

[Cryptosystem](#)

10 / 10 pts

Question 3

[Analysis](#)

R

 15 / 20 pts

Question 4

[Decryption Algorithm](#)

10 / 15 pts

Question 5

[Password](#)

10 / 10 pts

Question 6

[Codes](#)

0 / 0 pts

Question 7

[Team Name](#)

0 / 0 pts