

### 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 was the cryptosystem used in this level.

//

### 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.

1. We came across a figure when we first started this assignment, and we were given a tip that counting the number of lines might be helpful. The Vigenere cipher maps letters a–z to numbers between 0 and 25, therefore we determined that the hint was connected to a key for that cipher (e.g., 0 to A, 1 to B, and so on).

2. The key sequence "9292552221" was discovered by counting the lines in the graphical image starting from the bottom, which resulted in the characters "jcjffcccb."

3. Now, determining the ciphers that need a key to decrypt them is our next task.

Initially we thought of using Beaufort Cipher. For both encryption and decryption, the Beaufort cipher requires a key that is the same length as the plaintext. Thus, we can't use Beaufort cipher to decrypt the text provided in this algorithm as the key and the text provided

are of variable length.

4. Further, we thought of checking whether Playfair Cipher would be suitable to solve this assignment. However, the Playfair cipher requires a key to be a square grid of 5x5 in which each of the 25 alphabets must be distinct and one letter of the alphabet (often J) is left off the table as the table can carry only 25 alphabets. In this assignment, the key is not a grid. Thus, it is impossible for Playfair Cipher to be used to decrypt the encrypted text.

5. Then we moved on to the next approach that is the repeating key XOR decryption algorithm. Here we repeated the key until it is the same length as the cipher text. Combined each character in the repeating key with its matching character in the cipher text using the XOR algorithm. Each character in the cipher text and its corresponding character in the repeating key will be subjected to an XOR operation to produce the decrypted text. Return the text that has been decrypted to its original format, but the text is meaningless. So, in order to decode it, we must verify various algorithms.

6. Finally, we moved on to Vigenere Cipher. The Vigenere cipher translates each letters a through z into numbers between 0 and 25. (0 – A, 1 – B, 2 – C and so on). The key sequence "9292552221" was determined by counting the lines in the graphical image starting from the bottom, which resulted in the characters "jcjcffcccb" as the key sequence.

We then used a python code named "vigenere\_cipher.py" to decrypt the encrypted text. The python code has been implemented using the following logic:

Encryption-

The plaintext(P) and key(K) are added modulo 26.

$$E_i = (P_i + K_i) \bmod 26$$

Decryption-

$$D_i = (E_i - K_i + 26) \bmod 26$$

We discovered meaningful text after using the Vigenere cipher decryption technique. From this, we concluded that the Vigenere cipher has been the cryptosystem that has been used in this assignment.

Q4 Decryption Algorithm  
15 Points

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

The Vigenere cipher is a method that combines a number of interconnected Caesar ciphers to encrypt an alphabetic text. It is based on the letters in a keyword. This polyalphabetic substitution cipher serves as an illustration. This algorithm is simple to comprehend and use.

To encrypt and decrypt the text, a Vigenere table or Vigenere square is used. The tabula recta is another name for the Vigenere table.

Encrypted Text: 'Kg fcwd qh vin pnzy hjcoent, cjjwg ku wnth nnyvng kxa cjjwg Urfjm xwy yjg rbbufqwi "vjg\_djxn\_ofs\_dg\_rmncbgi" yq iq uqtxwlm. Oca zxw qcay vjg tctnplyj hqs cjn pjcv ejbvdnt. Yt hkpe cjn gcnv, aqv okauy bknn ongm vt zvvgs vcpkh bqft ejntj.'

Key: "jcjffcccb"

Step by step approach to decrypt the ciphertext using Vigenere Cipher:

1. Identify the key length: The first step is to determine the length of the key used to encrypt the message. This can be done using various techniques such as Index of Coincidence (IOC) or Kasiski examination. For this specific example, the key length is given, which is 10 characters long.

2. Repeat the key to match the length of the ciphertext: Repeat the key "jcjffcccb" until its length is equal to the length of the ciphertext. In this example, the key length is 10 characters and the ciphertext length is 100 characters, so the key needs to be repeated 10 times to match the length of the ciphertext. The repeated key will be "jcjffcccbjcjffcccb".

3. Create a Vigenere Square: A Vigenere Square is a matrix of 26x26 characters, where each row represents a different shift of the alphabet.

4. Determine the corresponding plaintext character: For each character in the ciphertext, find its corresponding character in the Vigenere Square. To do this, find the row that corresponds to the key character, and then find the column that corresponds to the ciphertext character. The intersection of that row and column is the corresponding plaintext character.

5.Repeat the process for every character in the ciphertext: Repeat the process of determining the corresponding plaintext character for every character in the ciphertext.

6. The decrypted message will now be obtained:

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.

7. A more easy implementation is mentioned below:

Encryption-

The plaintext(P) and key(K) are added modulo 26.

$$E_i = (P_i + K_i) \bmod 26$$

Decryption-

$$D_i = (E_i - K_i + 26) \bmod 26$$

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

▼ vignere\_cipher.py

 [Download](#)

```
1 key = "jcjcffcccb"
2 encrypted_text = "Kg fcwd qh vin pnzy hjcocnt cjjwg ku wnth
  nnyvng kxa cjjwg.Urfjm xwy yjg rbbufqwi
  \"vjg_djxn_ofs_dg_rmncbgi\" yq iq uqtxwlm.Oca zxw qcaj vjg
  tctnplyj hqs cjn pjcv ejbvdnt. Yt hkpe cjn gcnv,aqv okauy
  bknn ongm vt zvvgs vcpkh bqtft cjntj.";
3 decrypted_text ,j = "" , 0
4 for i in range(len(encrypted_text)):
5     if encrypted_text[i] >= 'a' and encrypted_text[i] <=
      'z':
```

```

6         diff = (ord(encrypted_text[i]) - ord(key[j]) + 26)
          % 26
7         temp = chr(ord('a')+diff)
8         j = (j+1)%len(key)
9         elif encrypted_text[i] >= 'A' and encrypted_text[i] <=
          'Z':
10            diff = (ord(encrypted_text[i].upper()) -
ord(key[j].upper()) + 26) % 26
11            temp = chr(ord('A')+diff)
12            j = (j+1)%len(key)
13        else:
14            temp = encrypted_text[i]
15        decrypted_text += temp
16    print(decrypted_text)

```

Q7 Team Name  
0 Points

team\_ethereum


//

## Assignment 2

● Graded

### Group

AVNISH TRIPATHI  
DIVYESH DEVANGKUMAR TRIPATHI  
ALLAN ROBEY

 View or edit group

### Total Points

65 / 65 pts

### Question 1

Commands

10 / 10 pts

### Question 2

Cryptosystem

10 / 10 pts

### Question 3

Analysis

20 / 20 pts

Question 4	
Decryption Algorithm	15 / 15 pts
Question 5	
Password	10 / 10 pts
Question 6	
Codes	0 / 0 pts
Question 7	
Team Name	0 / 0 pts