Q1 Commands
10 Points

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

1. go
2. back
3. 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.

Tools:
1. Used 'dcode.fr' to get the index of coincidence of ciphertext.
2. Took code reference from 'geeks for geeks' for Vigenere Cipher.

Observations:
1) First we did a frequency analysis of the given cipher and replace the most frequent letter with ‘e’ (by standard frequency table), we did the same things for more letters but we didn’t find any meaningful words, so it wasn’t a substitution cipher.
2) Second try we made is for the Vigenere cipher. We found the index of coincidence ‘I’ of the encrypted text is 0.049. Friedman’s Test says that if the index of coincidence lies between 0.038 and 0.065 then it is possibly Vigenere Cipher. The closer that ‘I’ is to 0.065, the more likely it is that we have a monoalphabetic cipher. The closer that ‘I’ is to 0.038, the more likely that we have a polyalphabetic cipher. Since in our case ‘I’ is 0.049, it is more likely to Polyalphabetic

Substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.

3) Mathematically Vigenere cipher has the following properties:

Encryption:

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

Ei = (Pi + Ki) mod 26

Decryption:

Di = (Ei - Ki + 26) mod 26

4) Then we tried to break Vigener Cipher but the key was not known to us, so we tried some other ways to decrypt.

5) We recalled the cave man which said us to bow down and count the number of lines in the Horizontal dimension. We found (9,2,9,2,5,5,2,2,2,1).

6) This Counting should definitely have something useful to decrypt the Vigenere cipher. So we tried mapping these numbers to their equivalent alphabets (i.e. "jcjcffcccb")

7) We decrypted the cipher using the above key. We used the code file to obtain the decrypted text. The Key is repeated cyclically to match the length of the ciphertext. The decrypted text we got is as follows: "BEWARYOFTHENEXTCHAMBERTHEREISVERYLITTLEJOYTHERESPEAKOUTTHEPASSWORDTHECAVEMANBEPLEASEDTOGOTHROUGHMAYYOUHAVETHESTRENGTHFORTHENEXTCHAMBERTOFINDTHEEXITYOUFIRSTWILLNEEDTOUTTERMAGICWORDSTHERE"

8) Since we had removed white spaces and all special characters from ciphertext, that's why we are getting decrypted text as above. So we manually checked both cipher text and decrypted text and put appropriate space or special characters in the decrypted text. So finally our decrypted text looks like 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."

9) So finally we get password as "the_cave_man_be_pleased". After entering this, we proceeded to the next level.

Q4 Decryption Algorithm
15 Points

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

1) Using our analysis we had already found the key as "jcjcffcccb". Vigener cipher repeats the key until its length matches the length of the ciphertext.
2) So we repeated this key in a circular manner until it matches the length of the ciphertext. This is done using generateKey function which is there in code attached here.
3) Now using Vigenere Decryption formula which is Di = (Ei - Ki + 26) mod 26, we decrypted the ciphertext, and this way we got the plain text. This is done using decryptedText function which is there in our code.
4) So we got our plain text as:
"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."
5) So finally we got password as "the_cave_man_be_pleased".

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

▾ cs641_a2.ipynb Download

In [1]:

```
def generateKey(string, key):
    key = list(key)
    if len(string) == len(key):
        return(key)
    else:
        for i in range(len(string) -
                len(key)):
            key.append(key[i % len(key)])
    return("" . join(key))
```

In [2]:

```
def decryptedText(cipher_text, key):
    orig_text = []
    for i in range(len(cipher_text)):
        x = (ord(cipher_text[i]) - ord(key[i]) + 26)
% 26
        x += ord('A')
        orig_text.append(chr(x))
    return("" . join(orig_text))
```

In [3]:

```
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.'''
#    9 2 9 2 5 5 2 2 2 1

#Removing all thins other than only letters
encrypted_text = encrypted_text.upper()
encrypted_text = encrypted_text.replace(" ",
"")
encrypted_text = encrypted_text.replace(".",
"")
encrypted_text = encrypted_text.replace(",",
"")
encrypted_text = encrypted_text.replace("""",
"")
encrypted_text = encrypted_text.replace("_",
"")
keyword = "JCJCFFCCCB"
key = generateKey(encrypted_text, keyword)
print("Decrypted Text :",
decryptedText(encrypted_text, key))
```

```
Decrypted Text : BEWARYOFTHENEXTCHAMBE
```

In [ ]:

Q7 Team Name
0 Points

crypt_elite

Assignment 2

● Graded

Group
KAPILKUMAR KISHORBHAI KATHIRIYA
SHRAWAN KUMAR
HARIS KHAN
View or edit group

Total Points
60 / 65 pts

Question 1 Commands	10 / 10 pts
Question 2 Cryptosystem	10 / 10 pts
Question 3 Analysis	20 / 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