Q1 Commands
5 Points

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

1. "climb" to ascend the mountain
2. "read" to read what was written on the rock
3. "enter" to enter into the chamber
4. "read" to read what is written on the glass panel near the door

And the first ciphertext is visible on the screen.

Q2 Cryptosystem
5 Points

What cryptosystem was used at this level?

In this level, the cipher that was used to decrypt the writing that was on the glass panel was a "substitution cipher". While shift cipher was also used on the digits in the password, to get the final password.

Q3 Analysis
25 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 Used:
(i) Python script was used to determine if the provided ciphertext is encrypted using "SHIFT CIPHER (CAESAR CIPHER)" or not.
(ii) Used the Python script (provided in question 6) to determine the frequency of each letter and bigram inside the ciphertext.

(iii) Used a table displaying letter frequencies (unigram, letter-pair) in the English language gleaned from course presentations and the internet.

1. We used a Python script to determine whether or not the ciphertext was encrypted with shift cypher. None of the 26 alternatives resulted in a text with significant content. Therefore, the prospect of utilising shift cypher for encryption was ruled out.

2. Then, we use frequency analysis to determine if it is encrypted with a substitution cypher. The key for a mono-alphabetic substitution cypher defines a map from each letter of the plaintext alphabet to a (single) letter of the ciphertext alphabet, where the map can be arbitrary as long as it is one-to-one such that decryption is achievable. As a result, the key space contains all bijections and permutations of the alphabet. The key Space for the English alphabet has a size of 26!=26*25..*1 or around 288, making brute-force attacks difficult. Therefore, we employ frequency analysis, which utilises the statistical patterns of English alphabets.

3. Because y appears in this ciphertext substantially more frequently than any other character, we may assume that d k(y) equals E. "ME" occurs most frequently, followed by "EY", according to the frequency analysis of letter pairs. We hypothesise that d k(ME)=TH and d k(EY)=HE, given that the most frequent letter-pairs in English are "TH" and "HE".

4. As "mey" appears repeatedly in the ciphertext, we deciphered it as "the." "wa" was deciphered to be "is." Then we determined that "mewa" will be "this." "gt" corresponds to "of."

5. Since we know the partial mapping, i.e. m->t, e->h, y->e, w->i, a->s, g->o, and t->f, we may proceed. In "meysy", "the' 'e" is evident. Therefore, we hypothesized that the word may be "these" or "there." Based on additional evidence and testing, we concluded that the object is "there." "than" will replace "meph". By slowly iterating over the whole ciphertext and employing the frequency analysis approach, we were able to completely decode it.

6. Moreover, the attack works by tabulating the frequency distribution of letters in the ciphertext, i.e., noting that 'a' occurred 26 times, 'b' appeared 2 times, etc. Then, these frequencies are compared to the known frequency of letters in standard English text. We then made educated guesses for portions of the mapping based on the observed frequencies. Since 'e' is the most common letter in English, we assumed that the most common character in the ciphertext corresponded to 'e' in the plaintext, and so on. Some of the guesses were incorrect, but sufficient guesses were right to permit reasonably speedy decryption (particularly when combined with other English information, such as the fact that 'u' typically follows 'q' and 'h' is likely to come between 't' and 'e').

7. The last decipherment reveals "This is the first chamber of the caves. As you can see, there is nothing of interest in the chamber. Some of the later chambers will be more interesting than this one! The code used for this message is a simple substitution cipher in which digits have been shifted by 6 places. The password is "tyRgU69diqq" without the quotes."

8. Using frequency analysis, we deciphered the plaintext above, which indicated that the digits are displaced by "8" places. Nevertheless, given that 8 is a number, it is apparent that 8 is also encoded by shifting. Consider the integer shifted to 8 to be X. Since X is the critical variable, one may argue that X is displaced by X places, yielding 8. The issue is represented as follows in mathematical notation: X+X=8mod10. 4 and 9 are the integers that satisfy the following equation. Consider the case when X = 4. The decryption method then commonly identifies two integers Y and Z such that Y+4=0mod10 and Z+4=3mod10. Consequently, Y = 6 and Z = 9 In this case, the decrypted password is "tyRgU69diqq." It was demonstrated upon submission that the password was legitimate. Consequently, we discard X's alternative value.

Q4 Mapping

10 Points

What is the plaintext space and ciphertext space?
What is the mapping between the elements of plaintext space and the elements of ciphertext space? (Explain in less than 100 words)

Plaintext space and ciphertext space are strings made up of uppercase and lowercase English letters, numbers, spaces, and punctuation.

Ciphertext Space is:
"Mewa wa mey twsam iepjoys gt mey ipbya. Pa xgn iph ayy, meysy wa hgmewhr gt whmysyam wh mey iepjoys. Agjy gt mey kpmys iepjoysa vwkk oy jgsy whmysyamwhr meph mewa ghy! Mey iguy nayu tgs mewa jyaapry wa p awjfky anoamwmnmwgh iwfeys wh vewie uwrwma epby oyyh aewtmyu ox 8 fkpiya. Mey fpaavgsu wa "mxSrN03uwdd" vwmegnm mey dngmya."

Plaintext Space is:
"This is the first chamber of the caves. As you can see, there is nothing of interest in the chamber. Some of the later chambers will be more interesting than this one! The code used for this message is a simple substitution cipher in which digits have been shifted by 6 places. The password is "tyRgU69diqq" without the quotes."

The mapping between the elements of plaintext space and the elements of ciphertext space is as follows:
a->s, b->v, c->k, d->q, e->h, f->p, g->o, h->n, i->c, j->m, k->l, l->j, m->t, n->u, o->b, p->a, q->x, r->g, s->r, t->f, u->d, v->w, w->i, x->y, y->e, z->z, 8->6, 0->6, 3->9

Q5 Password
5 Points

What is the final command used to clear this level?

"tyRgU69diqq" is the final command that was used to clear this level.

Q6 Codes

0 Points

Upload any code that you have used to solve this level

Modern_Cryptology1.ipynb Download

Shift Cipher: Trying to check whether shift cipher is meaningful or not

In [10]:
```
def
bruteforce_shift_cipher(ciphertext):
    for i in range(1, 26):
        plaintext = ""
        for char in ciphertext:
            if char.isalpha():
                char_code =
ord(char)
                if char.isupper():
                    char_code -= i
                    if char_code <
ord('A'):
                        char_code +=
26
                elif char.islower():
                    char_code -= i
                    if char_code <
ord('a'):
                        char_code +=
26
                plaintext +=
chr(char_code)
            else:
                plaintext += char
        print(f"Key: {i},
Plaintext: {plaintext}")
```

In [11]:
```
ciphertext = "Mewa wa mey twsam
iepjoys gt mey ipbya. Pa xgn iph
ayy, meysy wa hgmewhr gt whmysyam
wh mey iepjoys. Agjy gt mey kpmys
iepjoysa vwkk oy jgsy whmysyamwhr
meph mewa ghy! Mey iguy nayu tgs
mewa jyaapry wa p awjfky
anoamwmnmwgh iwfeys wh vewie uwrwma
epby oyyh aewtmyu ox 8 fkpiya. Mey
fpaavgsu wa mxSrN03uwdd vwmegnm mey
```

```
dngmya"
bruteforce_shift_cipher(ciphertext)
```

```
Key: 1, Plaintext: Ldvz vz ldx svrzl hd
Key: 2, Plaintext: Kcuy uy kcw ruqyk gc
Key: 3, Plaintext: Jbtx tx jbv qtpxj fb
Key: 4, Plaintext: Iasw sw iau psowi ea
Key: 5, Plaintext: Hzrv rv hzt ornvh dz
Key: 6, Plaintext: Gyqu qu gys nqmug cy
Key: 7, Plaintext: Fxpt pt fxr mpltf bx
Key: 8, Plaintext: Ewos os ewq lokse aw
Key: 9, Plaintext: Dvnr nr dvp knjrd zv
Key: 10, Plaintext: Cumq mq cuo jmiqc y
Key: 11, Plaintext: Btlp lp btn ilhpb x
Key: 12, Plaintext: Asko ko asm hkgoa w
Key: 13, Plaintext: Zrjn jn zrl gjfnz v
Key: 14, Plaintext: Yqim im yqk fiemy u
Key: 15, Plaintext: Xphl hl xpj ehdlx t
Key: 16, Plaintext: Wogk gk woi dgckw s
Key: 17, Plaintext: Vnfj fj vnh cfbjv r
Key: 18, Plaintext: Umei ei umg beaiu q
Key: 19, Plaintext: Tldh dh tlf adzht p
Key: 20, Plaintext: Skcg cg ske zcygs o
Key: 21, Plaintext: Rjbf bf rjd ybxfr n
Key: 22, Plaintext: Qiae ae qic xaweq m
Key: 23, Plaintext: Phzd zd phb wzvdp l
Key: 24, Plaintext: Ogyc yc oga vyuco k
Key: 25, Plaintext: Nfxb xb nfz uxtbn j
```

Frequency Analysis : Unigrams

In [27]:

```
def
frequency_analysis(ciphertext):

    freq_dict = {}
    for char in ciphertext:
        if char.isalpha():
            if char in freq_dict:
                freq_dict[char] +=
1
            else:
                freq_dict[char] =
1

    freq_dict =
dict(sorted(freq_dict.items(),
key=lambda item: item[1],
reverse=True))
```

```
    print("Frequency:", freq_dict)
```

In [28]:

```
ciphertext = "Mewa wa mey twsam
iepjoys gt mey ipbya. Pa xgn iph
ayy, meysy wa hgmewhr gt whmysyam
wh mey iepjoys. Agjy gt mey kpmys
iepjoysa vwkk oy jgsy whmysyamwhr
meph mewa ghy! Mey iguy nayu tgs
mewa jyaapry wa p awjfky
anoamwmnmwgh iwfeys wh vewie
uwrwma epby oyyh aewtmyu ox 8
fkpiya. Mey fpaavgsu wa
mxSrN03uwdd vwmegnm mey dngmya."
frequency_analysis(ciphertext)
```

```
Frequency: {'y': 36, 'a': 26, 'w': 25,
```

Letter Pair Analysis

In [29]:

```
def
letter_pair_analysis(ciphertext):

    freq_dict = {}
    for i in
range(len(ciphertext)-1):
        if ciphertext[i].isalpha()
and ciphertext[i+1].isalpha():
            letter_pair =
ciphertext[i] + ciphertext[i+1]
            if letter_pair in
freq_dict:

freq_dict[letter_pair] += 1
            else:

freq_dict[letter_pair] = 1

    freq_dict =
dict(sorted(freq_dict.items(),
key=lambda item: item[1],
reverse=True))

    print("Frequency:", freq_dict)
```

In [30]:

```
ciphertext = "Mewa wa mey twsam
iepjoys gt mey ipbya. Pa xgn iph
ayy, meysy wa hgmewhr gt whmysyam
wh mey iepjoys. Agjy gt mey kpmys
iepjoysa vwkk oy jgsy whmysyamwhr
meph mewa ghy! Mey iguy nayu tgs
mewa jyaapry wa p awjfky
anoamwmnmwgh iwfeys wh vewie
uwrwma epby oyyh aewtmyu ox 8
fkpiya. Mey fpaavgsu wa
mxSrN03uwdd vwmegnm mey dngmya."
letter_pair_analysis(ciphertext)
```

```
Frequency: {'me': 11, 'ey': 9, 'ys': 8,
```

Substitution Cipher Using frequency analysis

In [37]:

```
def ciphertext_mapping(ciphertext, key)

    mapped_ciphertext = []
    for char in ciphertext:
        if char.isalpha() :

mapped_ciphertext.append(key[char])
        else:
            mapped_ciphertext.append(ch

    mapped_ciphertext =
''.join(mapped_ciphertext)

    print("Mapped Ciphertext:",
mapped_ciphertext)

key = {'a': 's', 'b': 'v', 'c': 'k', 'c
'q', 'e': 'h', 'f': 'p', 'g': 'o', 'h':
'i': 'c', 'j': 'm', 'k': 'l', 'l': 'j',
't', 'n': 'u', 'o': 'b', 'p': 'a', 'q':
'r': 'g', 's': 'r', 't': 'f', 'u': 'd',
'w', 'w': 'i', 'x': 'y', 'y': 'e', 'z':
'z','M':'T','P':'A','A':'S','S':'R','N'
ciphertext = "Mewa wa mey twsam iepjoys
mey ipbya. Pa xgn iph ayy, meysy wa hgm
gt whmysyam wh mey iepjoys. Agjy gt mey
kpmys iepjoysa vwkk oy jgsy whmysyamwhr
mewa ghy! Mey iguy nayu tgs mewa jyaapr
p awjfky anoamwmnmwgh iwfeys wh vewie u
epby oyyh aewtmyu ox 8 fkpiya. Mey fpaa
```

```
wa mxSrN03uwdd vwmegnm mey dngmya."
ciphertext_mapping(ciphertext, key)
```

```
Mapped Ciphertext: This is the first ch
```

```
In [ ]:
```

Q7 Team Name
0 Points

d2ce09fd5842b342d5b3b66d10b6daef

Assignment 1

● Graded

Group

RAJ KUMAR
MADHAV MAHESHWARI
GUNJ MEHUL HUNDIWALA
View or edit group

Total Points

48 / 50 pts

Question 1
Commands **5** / 5 pts

Question 2
Cryptosystem R **5** / 5 pts

Question 3
Analysis R **25** / 25 pts

Question 4
Mapping **8** / 10 pts

Question 5

Password **5** / 5 pts

Question 6

Codes **0** / 0 pts

Question 7

Team Name **0** / 0 pts