Q1 Commands
5 Points

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

go
read
enter
read

Q2 Cryptosystem
5 Points

What cryptosystem was used at this level?

The Substitution cipher was used at this level.

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 : We have used the frequency analysis tool available at "https://math.dartmouth.edu/~awilson/tools/frequency_analysis.html"

Observations:

First of all, we converted ciphertext in lower case(or Upper case) and then started finding the decryption pattern using frequency analysis And while finding password we kept the decrypted text in same order as it was given in

cipher text (same order means lower case character were kept as lower case and upper case character as upper case character)

1. We have found out that the most frequent character in the given cipher text is 'y' so based on frequency analysis we replaced it with 'e'.
2. Then the next frequent character is 'm' in the cipher text and in English, it is 'the' so we replaced 'm' with 't' and 'e' with 'h'.
3. After that we had a word 'These' which seems like 'There' if we replace 's' by 'r'.
4. We also observed the word 'aee' and 'oe' which seems like 'see' and 'be' by replacing 'a' by 's' and 'o' by 'b'.
5. The word 'twist' looked like 'first' if we replace 't' by 'f' and 'w' by 'i'.
6. In the word 'ihterest' , if we replace 'h' by 'n' , it becomes 'interest'.
7. In the word 'hgthinr' if we replace 'g' by 'o' and 'r' by 'g' it becomes 'nothing'.
8. If we replace 'p' by 'a' the word 'thpn' becomes 'than'
9. In the word 'kater' if we had 'l' at the first position, we would get 'later' word , so replace 'k' by 'l'.
10. The word 'simtle' looks like 'simple' so replace 't' by 'p'.
11. By replacing 'v' by 'w' and 'u' by 'd' , 'passvoru' becomes 'password'.
12. Replace 'n' by 'u' , the word 'withont' becomes 'without'.
13. The word 'duotes' looks like 'quotes' so replace 'd' by 'q'.
14. Replace 'i' by 'c' , the word 'iode' becomes 'code'.
15. The word 'cabes' looks like 'caves' so replace 'b' with 'v'.
16. The word " as xou can" looks like "as you can" if we had 'y' at 'x', so we made the changes accordingly.
17. In the deciphered text it is written that 'digits have been shifted by 8 places' but the 8 is also shifted. so we can say that all the digits in the original text are shifted by 'd' places such that digit d in the original text is mapped to a ciphertext 8 therefore the equation is $(p+d) \bmod 10 = 8$ where p is plaintext digit, and similarly we get $(p+d) \bmod 10 = 3$, $(p+d) \bmod 10 = 0$. After trying to simplify these equations we got that $d = 4$, so 8 is mapped to 4 in plaintext, 0 is mapped to 6 and 3 is mapped to 9 in plaintext. Thus the encoding used for the digit is: $(\text{plaintext} + 4) \bmod 10 = \text{ciphertext}$. Hence we found the password is

"tyRgU69diqq".
18. There weren't any changes for the special character like
(! , spaces)

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 refers to the set of all possible plaintext (or
unencrypted) messages that can be encoded and
encrypted using a given encryption algorithm.

Ciphertext space refers to the set of all possible ciphertext
(or encrypted) messages that can be produced by
encrypting all possible plaintext messages using a given
encryption algorithm.

character mapping = ['a->s', 'b->v', 'd->q', 'e->h', 'g->o', 'h-
>n', 'i->c', 'k->l', 'm->t', 'n->u', 'o->b', 'p->a', 'r->g', 's->r', 't->f',
'u->d', 'v->w', 'w->i', 'x->y', 'y->e']

digit mapping = [4->0, 5->1, 6->2, 7->3, 8->4, 9->5, 0->6, 1-
>7, 2->8, 3->9]

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.

Plaintext = 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 4

places. The password is "tyRgU69diqq" without the quotes.

Q5 Password
5 Points

What is the final command used to clear this level?

tyRgU69diqq

Q6 Codes
0 Points

Upload any code that you have used to solve this level

▼ **frequency_analysis.ipynb**   ⬇ Download

```python
In [2]:   cipher_txt = "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."
```

```python
In [4]:   frequencies = {}
          txt=cipher_txt.lower()
          #Go through the every character of ciph
          for char in txt:
              if char.isalpha():
                  #if char is present as key ther
          increment the frequency by one otherwis
          in  frequency dictionary with value as
                  if char in frequencies:
                      frequencies[char] += 1
                  else:
                      frequencies[char] = 1
          #sort the frequency dictionary
          frequencies=dict(sorted(frequencies.ite
```

```
          lambda x:x[1],reverse=True))
          print("Frequency distribution of charac
          given cipher_text:")
          for key,value in
          sorted(frequencies.items(),key= lambda
          x:x[1],reverse=True):
              print(key ,":", value)
```

```
Frequency distribution of characters in
y : 36
m : 28
a : 27
w : 25
e : 22
g : 14
s : 13
p : 13
h : 12
i : 9
j : 7
o : 7
n : 7
t : 6
u : 6
r : 5
k : 5
v : 4
f : 4
x : 3
d : 3
b : 2
```

In [ ]:

Q7 Team Name
0 Points

da_vinci

Assignment 1   ● **Graded**

Group

PRADEEP CHALOTRA

SUMIT KUMAR CHAUDHARY

ANSHUL SHARMA

✏ View or edit group

Total Points

39 / 50 pts

Question 1

Commands   **5** / 5 pts

Question 2

Cryptosystem   R   **3** / 5 pts

Question 3

Analysis   R   **20** / 25 pts

Question 4

Mapping   R   **6** / 10 pts

Question 5

Password   **5** / 5 pts

Question 6

Codes   **0** / 0 pts

Question 7

Team Name   **0** / 0 pts