Q1 Commands
5 Points

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

climb
read
enter
read

Q2 Cryptosystem
5 Points

What cryptosystem was used at this level?

The cryptosystem used at this level is Substitution Cipher which is mono-alphabetic in nature.

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.

1. First, we determined whether or not shift cipher was used to encrypt the given cipher text. We discovered that none of the 26 options produced a paragraph that made sense. Shift cipher encryption was therefore ruled out as an option to decrypt the given text.

2. Then we proceeded to check whether the text has been encrypted using mono-alphabetic substitution cipher or not using frequency analysis.

3. Frequency substitution cipher is a method of encryption where letters in the plaintext are replaced by other letters based on the frequency of their occurrence in the text.

4. To perform the decryption task on the given text, the following

steps were performed: (1) Count the frequency of each letter in the cipher text. (2) Arrange the letters in descending order of their frequency. (3) Assign the most frequent letter in the cipher text to the most common letter in the English language (e.g. 'e'). (4) Assign the second most frequent letter in the cipher text to the second most common letter in the English language (e.g. 't'). (5) Continue this process for all letters in the cipher text. (6) Then Finally use the mapping obtained to decrypt the cipher text and obtain the plaintext.

5. After performing frequency analysis, we found that the most frequent letter in the given text is ‘y’ with a frequency of 36. So we replaced all occurrences of ‘y’ in the given text with ‘e’ which is the most common letter in English language and thus obtained the mapping y ->e.

6. The second most frequent letter in the text is ‘m’ with a frequency of 28. Thus it gets mapped with the second most common letter in English language which is ‘t’. After which we observed ‘Tee’ and took an educated guess that ‘e’ in the cipher text should be mapped with ‘h’ as the word ‘Tee’ closely resembles the word ‘The’. Now replace all the occurrences of ‘e’ with ‘h’ in the cipher text.

7. There is presence of only a single letter word ‘p’, so we can map it to either ‘i’ or ‘a’. We made a guess and mapped it to ‘a’. Consequently, the word ‘pa’ changes to ‘aa’. Now, the plain text word corresponding to it can be ‘as’ or ‘an’, but we made a guess and mapped it to ‘as’. Thus, ‘a’ gets mapped to ‘s’. Now replace all occurrences of ‘a’ with ‘s’ in the cipher text.

8. Now we observed the word ‘fassvgsu’ and used the concept of Hangman game and made an educated guess that should be mapped to the word ‘password’. Thus we, found the mapping such as f->p, v->w, g->o,s->r,u->d. Then replaced all occurrences of f,v,g,s,u with p,w,o,r,d.

9. After which we observed the word ‘ohe’, which looks similar to the English word ‘one’. Thus we made a well-educated guess that it should be mapped to one and obtained the mapping h->e.

10. Now we observed the word ‘ian’ and found that it closely resembles the English word ‘can’. Hence, we concluded that ‘I’ can be replaced by ‘c’ in the cipher text and obtained the mapping i->c.

11. We then considered the word ‘chajoers’ and replaced the letters ‘j’ and ‘o’ with ‘m’ and ‘b’ as it generates the English word ‘chamber’. Thus the mappings, j->m and o->b and replaced all occurrences of ‘j’ and ‘o’ with ‘m’ and ‘b’ in the given text.

12. On looking at the word ‘twrst’, we found that it closely resembles the word ‘first’ so we replaced all occurrences of ‘t’ with ‘f’ and ‘w’ with ‘i’. Thus we obtained the mappings t->f and w->i.

13. From the word ‘nsed’, we can make a well educated guess that ‘n’ should be mapped to ‘u’ as it closely resembles the English word ‘used’. Thus n is mapped to ‘u’. Similarly, from the word ‘duotes’ we can obtain the mapping d->q as it is closely related to the word ‘quotes’.

14. On closely observing the word ’pkaies’ and ‘xou’, we can make a well educated guess that it is related to the English word ‘places’ and ‘you’. Thus, we obtained the mapping k->l, x->yand i->c and replaced all occurrences of ‘k’ , ‘x’ and ‘I’ with ‘i’, ‘y’ and ‘c’ in the given text. From words like 'nothinr' and 'habe' we can easily obtain the mapping r->g and b->v as on replacing r with g and b with v we can easily obtain the English words 'nothing' and 'have'. Now replace all occurrences of 'r' with 'g' and 'b' with 'v'.

15. Thus we obtained the following mapping:

a'->'s','b'->'v','d'->'q','e'->'h','f'->'p','g'->'o','h'->'n','i'->'c','j'->'m','k'->'i','m'->'t',
'n'->'u','o'->'b','p'->'a','r'->'g','s'->'r','t'->'f','u'->'d','v'->'w','w'->'i','x'->'y','y'->'e'

Using this mapping we decrypt the entire given text and obtained the plain text as given below using the python code CipherTxt_to_PlainTxt.py:
'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 8 places. the password is “tyRgU03diqq” without the quotes.'

16. On decrypting the text, we could see that the password mentioned is "tyRgU03diqq". However, it is also mentioned in the text that each digit has been shifted by 8 places. Now, 8 itself is a

digit. Thus, 8 gets shifted by 8 places and we obtained 16. But we performed mod 10 operation on 16 which results in 6. Thus the digit 8 gets mapped to 6. So we concluded that each digit be shifted by 6 places. Thus the digits in the password 0 and 3 would get mapped to 6 and 9 when shifted by 6 places.

17. Thus the final password that we would obtain is “tyRgU69diqq”.

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)

The set of all potential plaintext messages that can be encrypted is known as the plaintext space, and the set of all possible ciphertext messages that can be created by encrypting plaintext messages is known as the ciphertext space.
The chosen encryption algorithm and key determine how the elements of plaintext space and ciphertext space are mapped. Through the use of encryption, each element of the plaintext space is assigned a corresponding element in the ciphertext space.

CIPHER TEXT SPACE:

"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"

PLAIN TEXT SPACE:

"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 8 places. The password is "tyRgU03diqq" without the quotes"

The following mapping has been extracted in accordance with the explanation provided in question 3:

'a'->'s','b'->'v','d'->'q','e'->'h','f'->'p','g'->'o','h'->'n','i'->'c','j'->'m','k'->'i','m'->'t',
'n'->'u','o'->'b','p'->'a','r'->'g','s'->'r','t'->'f','u'->'d','v'->'w','w'->'i','x'->'y','y'->'e',',8'->'6',
'0'->'6','3'->'9'

On decrypting the text, we could see that the password mentioned is "tyRgU03diqq". However, it is also mentioned in the text that each digit has been shifted by 8 places. Now, 8 itself is a digit. Thus, 8 gets shifted by 8 places and we obtained 16. But we performed mod 10 operation on 16 which results in 6. Thus the digit 8 gets mapped to 6. So we concluded that each digit be shifted by 6 places. Thus the digits in the password 0 and 3 would get mapped to 6 and 9 when shifted by 6 places.

Thus, the final password that we would obtain is “tyRgU69diqq”.

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

▾ CipherTxT_to_PlainTxT.py Download

```
from collections import defaultdict
d = defaultdict()
d['a'] = 's'
d['b'] = 'v'
d['d'] = 'q'
d['e'] = 'h'
d['f'] = 'p'
d['g'] = 'o'
d['h'] = 'n'
d['i'] = 'c'
d['j'] = 'm'
d['k'] = 'l'
d['m'] = 't'
```

```
d['n'] = 'u'
d['o'] = 'b'
d['p'] = 'a'
d['r'] = 'g'
d['s'] = 'r'
d['t'] = 'f'
d['u'] = 'd'
d['v'] = 'w'
d['w'] = 'i'
d['x'] = 'y'
d['y'] = 'e'

St = "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.".lower()
a = ""
for i in range(len(St)):
    if St[i] in d:
        a += d[St[i]]
    else:
        a += St[i]
```

Q7 Team Name
0 Points

team_ethereum

Assignment 1

● Graded

Group
DIVYESH DEVANGKUMAR TRIPATHI
AVNISH TRIPATHI
ALLAN ROBEY
View or edit group

Total Points
48 / 50 pts

Question 1 Commands	5 / 5 pts
Question 2 Cryptosystem	5 / 5 pts
Question 3 Analysis	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