Q1 Commands

5 Points

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

```
list
go
read
enter
read
```

Q2 Cryptosystem

5 Points

What cryptosystem was used in this level?

Simple Substitution Cipher

Q3 Analysis

25 Points

What tools and observations were used to figure our the cryptosystem? (Explain in less than 100 words)

First, we checked for Caeser Cipher using brute force, but none of the decrypted text made any sense.
If Permutation Cipher was used, then the frequency of alphabets in Ciphertext should be similar to the generally observed frequency of alphabets in English text, but this was not the case for given Ciphertext.
Then we calculated the Index of Coincidence, and it came out to be 0.071, which is close enough to 0.066, which is standard for Substitution Cipher.

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)

Ciphertext = ['C', 'F', 'K', 'O', 'I', 'G', 'H', 'M', 'Q', 'P', 'D', 'N', 'V', 'E', 'Y', 'A', 'U', '.', 'J', 'L', 'R', 'X', 'S', '!', ',' , '1', '2', '9']

Plaintext = ['E', 'T', 'S', 'I', 'H', 'O', 'A', 'R', 'N', 'C', 'M', 'B', 'U', 'F', 'D', 'G', 'L', '.' , 'P', 'Q', 'Y', 'Q', 'V', '!', ',' , '5', '6', '3']

Mapping:

Ciphercharacter -> Plaintext Character

C -> E , F -> T using frequency table
I -> H, for 'the' most common 3 letter word, also whitespaces are shuffled and therefore letters need to be grouped
O -> I , K -> S for 'is' and 'this'
Q -> N , M-> R , A-> G for 'interest' and 'interesting'
H -> A for 'as'
G -> O as O has high frequency and it was making sense to replace G with it
E -> F for 'of'
D -> M for 'message', 'more' etc

J -> P , U -> L for 'simple'
P -> C for 'cipher' and 'code'
N -> B for 'chamber'
Y -> D , L -> W for 'password'
S -> V for 'caves'
R -> Y for 'by'
V -> U for 'you' and 'substitution'
X -> Q for 'quotes'
2 -> 6 , 9 -> 3 , 1 - > 5

-There is no substitution for punctuations.

After decrypting the whole ciphertext, we came to know that all digits in plaintext have also been encrypted and we have not done figured this out. Ciphertext says shifted by 2 places, which means either it was by 1 in plaintext and it got shifted to 2 or it was 6 and due to circular ordering it came to 2. We first checked for 1 and got 'unknown command' so we checked for 6 spaces by trying 3 instead of 9 and 5 instead of 1 and got right password

Q5 Password

5 Points

What is the final command used to clear this level?

iRqy3U5qdgt

Q6 Codes

0 Points

Upload any code that you have used to solve this level

caesar.py Download

```
cipher = 'omkf pi hdn cmgef icphsck .H krg vphqkc c, fic mco kqgf ioqag eo qfcmckf oq ficpihdn cm .Kg dcgeficu hfcm pi hdn cmklo uuncdgmc oqfc mc kfoq afihqfiokgq c!Fi cpgy
```

```
cvkc yeg mfio kdck kha cokh kodjuck vn k fofvfo
gqpojicmoqli opiyoa of kihsc nccqki oefc ynr2 juhpck. Fi c
jhkklgm yok oMxr9V1x ya flofigvffic xvgfck. Fio kokfice'
cipher=cipher.lower()


for i in range(1,26):
    plaintext = ''
    for j in cipher:
        if ord(j) in range(97,123):
            plaintext+= chr(ord(j)+i) if ord(j)+i<123 else
chr(ord(j)+i-26)
        else:
            plaintext+=j

    print('Plaintext with key',i,':\n',plaintext,end='
\n\n\n')

```

frequency.py

Download

```

a = "omkf pi hdn cmgef icphsck .H krg vphqkc c, fic mco
kqgf ioqag eo qfcmckf oq ficpihdn cm .Kg dcgeficu hfcm pi
hdn cmklo uuncdgmc oqfc mc kfoq afihqfiokgq c!Fi cpgy cvkc
yeg mfio kdck kha cokh kodjuck vn k fofvfo gqpojicmoqli
opiyoa of kihsc nccqki oefc ynr2 juhpck. Fi c jhkklgm yok
oMxr9V1x ya flofigvffic xvgfck. Fio kokfice"
a = a.lower()
count = {}
for i in a:
    if i in count.keys():
        count[i] = count[i] + 1
    else:
        count[i] = 1

IC = 0;
total_count = 0;
for i in count.keys():
    if i.isalpha():
        IC = IC + count[i]*(count[i]-1)
        total_count = total_count + count[i]

IC = IC/(total_count*(total_count-1))
print(count)
print(IC)
```

Q7 Team Name

0 Points

Lazarus

Assignment 1

● **GRADED**

GROUP

Harsh Agarwal

Aditya Loth

Varun Vankudre

View or edit group

TOTAL POINTS

42.5 / 50 pts

QUESTION 1

Commands **5** / 5 pts

QUESTION 2

Cryptosystem **5** / 5 pts

QUESTION 3

Analysis **R** **17.5** / 25 pts

✓ **+ 10 pts** Using frequency analysis to conclude that its substitution cipher.

+ 5 pts Mentioning about rotation in the ciphertext

✓ **+ 5 pts** Finding the mapping in the cryptosystem used by analyzing bigrams and trigrams (or small words)

+ 5 pts Given mathematical explanation for the shift in the numbers

+ 0 pts Wrong answer or NA

+ 2.5 pts partial marks awarded for mathematical explanation of numbers though no proper generalization done.

Regrade Request Submitted on: **Feb 06**

For the numbers we have mentioned in the last paragraph explaining how we decrypted the numbers

1. Rotation in cipher text indicates few words rotated in the last and first sentence.
2. Mathematical explanation - requires a generalized form which can be opted to all numbers. I have given 2.5 partial marks for this already. Do be specific from next assignment.

Reviewed on: **Feb 07**

Regrade Request Submitted on: **Feb 06**

For the points which you have not awarded us marks for we have mentioned those in question 4 as there was no clear understanding of where it had to be mentioned so we mentioned those points with mapping for easy explanation and understanding.

So if you could please consider this time, we will keep this in mind for further assignments

Mention everything from the next assignment, still you haven't mentioned anything regarding rotation of the cipher text / nor the mathematical expression

Reviewed on: **Feb 06**

QUESTION 4

Mapping

10 / 10 pts

QUESTION 5

Password

5 / 5 pts

QUESTION 6

Codes

0 / 0 pts

QUESTION 7

Team Name

0 / 0 pts