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 in this level?

The substitution cipher is used in this level to decrypt the ciphertext and there is also rotation by 12(considering the space character) characters to the left.

Q3 Analysis
25 Points

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

Tools used: We have used the frequency analysis tool available at "https://math.dartmouth.edu/~awilson/tools/frequency_analysis.html" to get the idea about the substitutions that we need to perform in order to convert the ciphertext to plain text.
Observations:
1) We found that the two most frequent characters in the given ciphertext are 'c' and 'f' so we replaced them with 'e' and 't' respectively which are the two most frequent characters in english.
2) After which we observed that we had 'ti' as the most frequent bigram in the ciphertext and in English, it is 'th' so we replaced 'i' with 'h'.

3) We observed that there were many segmented words like 'th e' which looks like 'the' so we identified that there can be spaces within a word.
4) We replaced 'o' by 'i', after which we had a word like 'thi k' which looked like this so replace 'k' with 's'.
5) After which we had a word 'E iMst' which looked like first if we consider the rotation so replace 'm' by 'r' and 'e' by 'f'.
6)The word 'i Qterest' looks like interest so replaced 'q' with 'n'.
7) In the word 'nGt hinA' if we replace 'g' by 'o' and 'a' by 'g' it becomes 'nothing'.
8) The word 'so deofthe' looks like 'some of the' so we replaced 'd' by 'm'
9) In the word 'U Hter' if we had 'l' at the first position and 'a' at the second position then we will get the word 'later' so we replaced 'u' by 'l' and 'h' by 'a'.
10) In the word 'PaSes' if we had 'c' at the first position and v at the first s's position we could make 'caves' so we replaced 'p' by 'c' and 's' by 'v'.
11) The word 'a sRo V' looks like 'as you' if we had y at r's place and u at v's place so we made the changes accordingly.
12) The word 'Li llNemore' looks like 'will be more' so we replaced 'l' by 'w' and 'n' by 'b'.
13) The word 'coY e' looks like code so replace 'y' by 'd'.
14) The word 'simJle' looks like simple so replace 'j' by 'p'.
15) The word 'Xuotes' looks like quotes so replace 'x' by 'q'.
16) There weren't any changes for the special character like(! , spaces)
17) In the deciphered text it is written that 'digits have been shifted by 2 places' but the 2 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 ciphertext 2 therefore the equation is (d+d)mod10=2 this gives two possible values of d which are 6 and 1, after trying out both the choices we get 6 as the correct value. Thus the encoding used for digits is : (plaintext+6)mod10 = ciphertext.

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 space = [a-z]-{b,t,w,z} U {2,9,1} U { ,!,.} U {H,K,F,V}

plaintext space = [a-z]-{j,k,x,z} U {6,3,5} U { ,!,.} U {T,A,R,U}

Character mapping = ['a->g', 'c->e', 'd->m', 'e->f', 'g->t' ,'h->o', 'i->a', 'j->h',' k->p', 'l->s' ,'m->w', 'n->r', '0->b', 'p->i', 'q->c', 'r->n', s->y', 't->v', 'u->l', 'v->u', 'w->q', 'x->d']

Digit mapping = [2->6,9->3, 1->5]

ciphertext = "omkf pi hdn cmgef icphsck .H krg vphqkc c,fic mco kqgf ioqag eo qfcmckf oq ficpihdn cm .Kg dcgeficu hfcm pi hdn cmklo uuncdgmcoqfc 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"

plaintext = "'irst ch amb eroft hecaves .A syo ucanse e,the rei snot hingo fi nterest in thechamb er .So meofthel ater ch amb erswi llbemoreinte re stin gthanthison e!Th ecod euse dfo rthi smes sag eisa simples ub s tituti oncipherinwh ichdig it shave beensh ifte dby2 places. Th e passwor dis iRqy9U1q dg twithoutthe quotes. Thi sisthef'

original text = "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 iRqy3U5qdgt without the quotes."

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

Assignment1.ipynb Download

In [1]:
```
ciphertext = "omkf pi hdn cmgef
icphsck .H krg vphqkc c,fic mco kqgf
ioqag eo qfcmckf oq ficpihdn cm .Kg
dcgeficu hfcm pi hdn cmklo
uuncdgmcoqfc 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"
```

In [2]:
```
ciphertext_without_case =
ciphertext.lower()
```

In [3]:
```
ciphertext_without_case
```

Out [3]:
```
'omkf pi hdn cmgef icphsck .h krg vphqkc c,
```

In [4]:
```
frequency={}
for item in ciphertext_without_case:
    if item.isalpha():
        try:
            frequency[item]+=1
        except:
            frequency[item]=1

print("Frequency distribution in the given
cipher text: ")
for k,val in sorted(frequency.items(), key
= lambda x: x[1], reverse = True):
    print(k
,val/len(ciphertext_without_case)*100,sep='
= ")
```

```
Frequency distribution in the given cipher
c = 11.145510835913312
f = 8.6687306501548
k = 8.359133126934983
o = 7.739938080495357
i = 6.811145510835913
g = 4.3343653250774
m = 4.024767801857585
h = 4.024767801857585
q = 3.7151702786377707
p = 2.786377708978328
d = 2.1671826625387
n = 2.1671826625387
v = 2.1671826625387
e = 1.8575851393188854
y = 1.8575851393188854

a = 1.5479876160990713
u = 1.5479876160990713
```

```
l = 1.238390092879257
j = 1.238390092879257
r = 0.9287925696594427
x = 0.9287925696594427
s = 0.6191950464396285
```

In [5]:
```
mapping_for_lower_case = ['g','-
','e','m','f','t','o','a','h','p','s','w','
','l','u','-','q','d','-']
```

In [6]:
```
mapping_for_upper_case = ['G','-
','E','M','F','T','O','A','H','P','S','W','
','L','U','-','Q','D','-']
```

In [7]:
```
ans = ""
for item in ciphertext:
    if (ord(item)>=ord('a') and
ord(item)<=ord('z')):
        item =
mapping_for_lower_case[ord(item)-
ord('a')]
    if (ord(item)>=ord('A') and
ord(item)<=ord('Z')):
        item =
mapping_for_upper_case[ord(item)-
ord('A')]
    ans += item;
```

In [8]:
```
ans
```

Out [8]:
```
'irst ch amb eroft hecaves .A syo ucanse e,
```

In [9]:
```
d=12
```

In [10]:
```
temp1 = ans[0 : len(ans)-d]
temp2 = ans[len(ans)-d : ]
```

In [11]:
```
check = temp2 + temp1
check
```

Out [11]:
```
' Thi sisthefirst ch amb eroft hecaves .A s
```

In [12]:
```
password = "iRqy3U5qdgt"
```

Q7 Team Name

0 Points

flash

Assignment 1

GRADED

GROUP

Prashant Mishra
Nimit Jain
Ravi Shankar Das

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