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 in this level?

Substitution cipher(with spaces been moved) along with rotation by 12 places to the left on plain text.

Q3 Analysis
25 Points

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

Tools used - Frequency analysis, Python , Microsoft word
Observations:

1. We ran frequency analysis on the Text . We had total 249 letter present in the text out of which 'c' appeared 35 times which is alomst 14 % of the total letters present in the text.Hence 'c ' is 'E'.

2. 'c' has appeared as single letter word , which is not possible as 'e' is not a valid

Assignment 1 — GRADED

GROUP
Jeet Sarangi
Alok Kumar Trivedi
Akshay Kumar Chittora
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

english word , hence characters in the text are rotated.

3. The two most appeared Bigram in the text are 'FI' and 'IC'. The two most appeared Bigram in English is 'TH' and 'HE' , Hence 'I' in text is actually 'H'. and as 'FI' appeared more than 5% times in the text which is considerably higher than its successor 'IC', we can conclude that 'F' = 'T'. The same way , Third most appered bigram in text is 'CM' and in english 'ER' is 4th most appeared bigram . Hence 'M' = 'R'. Again 'CK' could be equal to 'ES' as 'CK' is next most appearing bigram starting with 'C'.

4. The next most appeared biagram with 'K' at the end is 'OK' and we can observe that the next most frequently occurring bigram in English with second alphabet as 'S' is 'IS'. Therefore, 'O' is most likely to be 'I'.

5. Now if we take "eo qfcmckf" , It can be translated as "eI qTEREST"(letter in capital are already deduced). we can safely conclude that 'Q' = 'N'.

6. Now if we consider the phrase 'The rei sngt hinag ei nterest in the' it can be written as 'There is nothing of interest in the'. hence 'g' = 'o' ,'a' = 'g' and 'e' = 'f'

7. The phrase 'kodjuck vn k fofvfo gq' can be rephrased as 'siDJUes VN s titvti on' (letter in capital are not known yet). here if we put 'v' = 'u' , 'n' = 'b' ,it becomes 'substitution'. again 'kihsc nccqki oefc ynr2 juhpck' can be written as 'shHSe beensh ifte YbR2 JUHPes' , which can be rephrased as 'shave beensh iftedby2 places' . Hence 'H' = 'a', 's' = 'v', 'Y' = 'D', 'r' = 'y' , 'j' = 'p' , 'u' = 'l', 'h' = 'a' ,'p' = 'c'.

8. Again the phrase 'the passLor dis irXy9uiX dg tLithoutthe Xuotes'. we can easily deduce that 'L' = 'w' and 'x' = 'q'. similarly 'so Deof thel ater ch amb erswillbemore' gives away the identity of 'd' as 'm'.

9. Here in the decrypted text it is mentioned that digits are shifted by 2 places however the 2 mentioned itself is shifted by some digits. Lets say x is digits present in the plain text and it was shifted by x for the encryption then (x + x) = 2 mod 10 , it gives two possible value of x
as 6 and 1 . upon shifting the digits 9 and 1 by both the number for password , we got 6 as the correct value. so 9 and 1 are replaced by (9 - 6) mod 10 = 3 and (1-6) mod 10 = 5 respectively.

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 cipher text space are set of strings made up from the elements of a set c: {'a', 'b', 'c', ...'z', 'A', 'B', ...,'Z', 0 ,1 , 2,...9,} Both the spaces consist of string made up of uppercase and lower case english letters as well as digits from 0 to 9.
After analysing the letters and digits using different encodings methods we have successfully decrypted the text and got fully formed words after rotating the cipher text.

Ciphertext = " omkf pi hdn cmgef icphsck .H krg vphqk 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 "

Decrypted text = "THIS IS THE FIRST CHAMBER OF THE CAVES .AS YOU CAN S E, 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 2 PLACES. THE PASSWORD IS IRQY9U1QDGT WITHOUT THE QUOTES."

Mapping of letters from cipher text to decrypted text :
C – E, M – R , I – H , F – T, K – S , O – I , Q – N, G – O , A – G, E – F, V – U , N – B , H – A,S – V ,Y – D , R – Y, J – P , U – L , P – C , L – W , X – Q, D – M, 2 – 6, 9 – 3, 1 – 5

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

crypto_assignment1.ipynb — Download

In [1]:
```
import string
org_text = '''omkf pi hdn cmgef icphsck .H krg vphqk 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'''
```

In [2]:
```
print(org_text)
```

```
omkf pi hdn cmgef icphsck .H krg vphqk 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
```

In [3]:
```
cipher_text = org_text.upper()
print("Cipher Text is :\n")
print(cipher_text.upper())
```

```
Cipher Text is :

OMKF PI HDN CMGEF ICPHSCK .H KRG VPHQK 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
```

In [4]:
```
freq = dict.fromkeys(string.ascii_uppercase, 0)
```

```
for ch in cipher_text:
    if ch.isalpha():
        freq[ch]+=1
```

```
print("The frequency per characters is :\n")
for k,v in sorted(freq.items(),key = lambda
x:x[1],reverse=True):
    print(k,v)
```

```
The frequency per characters is :

C 35
F 28
K 27
O 25
I 22
G 14
H 13
M 13
Q 12
P 9
D 7
N 7
V 7
E 6
Y 6
A 5
U 5
J 4
L 4
R 3
X 3
S 2
B 0
T 0
W 0
Z 0
```

In [5]:

```
bigram_freq = {}
total = 0
for i in range(0,len(cipher_text)-1):
    if(cipher_text[i].isalpha() and cipher_text[i+1].isalpha()):
        temp = cipher_text[i]+cipher_text[i+1]
        bigram_freq[temp] = bigram_freq.get(temp,0)+1
        total+=1
print("Frequency Distribution of bigrams are : ")
for k,v in sorted(bigram_freq.items(),key = lambda
x:x[1],reverse=True):
    print(k,v/total)
```

```
Frequency Distribution of bigrams are :
FI 0.06153846153846154
IC 0.035897435897435895
CM 0.03076923076923077
CK 0.03076923076923077
OQ 0.02564102564102564
FC 0.02564102564102564
```

KF 0.020512820512820513
PI 0.020512820512820513
MC 0.020512820512820513
IO 0.020512820512820513
OK 0.020512820512820513
HD 0.015384615384615385
DN 0.015384615384615385
EF 0.015384615384615385
CP 0.015384615384615385
QF 0.015384615384615385
IH 0.015384615384615385
FO 0.015384615384615385
OF 0.015384615384615385
OM 0.010256410256410256
MK 0.010256410256410256
GE 0.010256410256410256
PH 0.010256410256410256
HS 0.010256410256410256
SC 0.010256410256410256
HQ 0.010256410256410256
QK 0.010256410256410256
CO 0.010256410256410256
GF 0.010256410256410256
KG 0.010256410256410256
DC 0.010256410256410256
KL 0.010256410256410256
LO 0.010256410256410256
NC 0.010256410256410256
GM 0.010256410256410256
GQ 0.010256410256410256
KH 0.010256410256410256
KO 0.010256410256410256
JU 0.010256410256410256
VF 0.010256410256410256
YO 0.010256410256410256
KI 0.010256410256410256
MG 0.005128205128205128
KR 0.005128205128205128
RG 0.005128205128205128
VP 0.005128205128205128
KQ 0.005128205128205128
QG 0.005128205128205128
QA 0.005128205128205128
AG 0.005128205128205128
EO 0.005128205128205128
CG 0.005128205128205128
CU 0.005128205128205128
HF 0.005128205128205128
UU 0.005128205128205128
UN 0.005128205128205128
CD 0.005128205128205128
DG 0.005128205128205128
AF 0.005128205128205128
PG 0.005128205128205128
GY 0.005128205128205128
CV 0.005128205128205128
VK 0.005128205128205128
KC 0.005128205128205128
YE 0.005128205128205128

```
EG 0.005128205128205128
MF 0.005128205128205128
KD 0.005128205128205128
HA 0.005128205128205128
OD 0.005128205128205128
DJ 0.005128205128205128
UC 0.005128205128205128
VN 0.005128205128205128
FV 0.005128205128205128
QP 0.005128205128205128
PO 0.005128205128205128
OJ 0.005128205128205128
JI 0.005128205128205128
MO 0.005128205128205128
QL 0.005128205128205128
LI 0.005128205128205128
OP 0.005128205128205128
IY 0.005128205128205128
OA 0.005128205128205128
CC 0.005128205128205128
CQ 0.005128205128205128
OE 0.005128205128205128
YN 0.005128205128205128
NR 0.005128205128205128
UH 0.005128205128205128
HP 0.005128205128205128
PC 0.005128205128205128
JH 0.005128205128205128
HK 0.005128205128205128
KK 0.005128205128205128
LG 0.005128205128205128
MX 0.005128205128205128
XR 0.005128205128205128
YA 0.005128205128205128
FL 0.005128205128205128
IG 0.005128205128205128
GV 0.005128205128205128
FF 0.005128205128205128
XV 0.005128205128205128
VG 0.005128205128205128
CE 0.005128205128205128
```

In [6]:

```
plain = ""

for ch in cipher_text:
    if ch.isdigit():
        ch = str((int(ch)+4)%10)
    elif ch == 'A':
        ch = 'G'
    elif ch == 'B':
        ch = 'B'
    elif ch == 'P':
        ch = 'C'
    elif ch == 'C':
        ch = 'E'
    elif ch == 'D':
        ch = 'M'
    elif ch == 'E':
```

```
        ch = 'F'
    elif ch == 'F':
        ch = 'T'
    elif ch == 'G':
        ch = 'O'
    elif ch == 'H':
        ch = 'A'
    elif ch == 'I':
        ch = 'H'
    elif ch == 'J':
        ch = 'P'
    elif ch == 'K':
        ch = 'S'
    elif ch == 'L':
        ch = 'W'
    elif ch == 'M':
        ch = 'R'
    elif ch == 'N':
        ch = 'B'
    elif ch == 'O':
        ch = 'I'
    elif ch == 'P':
        ch = 'C'
    elif ch == 'Q':
        ch = 'N'
    elif ch == 'R':
        ch = 'Y'
    elif ch == 'S':
        ch = 'V'
    elif ch == 'T':
        ch = 'T'
    elif ch == 'U':
        ch = 'L'
    elif ch == 'V':
        ch = 'U'
    elif ch == 'W':
        ch = 'W'
    elif ch == 'X':
        ch = 'Q'
    elif ch == 'Y':
        ch = 'D'
    elif ch == 'Z':
        ch = 'Z'
    plain += ch
print(plain)
```

```
IRST CH AMB EROFT HECAVES .A SYO UCANS E,
THE REI SNOT HINGO FI NTEREST IN THECHAMB
ER .SO MEOFTHEL ATER CH AMB ERSWI LLBEMORE
INTE RE STIN GTHANTHISON E!TH ECOD EUSE DFO
RTHI SMES SAG EISA SIMPLES UB S TITUTI
ONCIPHERINWH ICHDIG IT SHAVE BEENSH IFTE
DBY6 PLACES. TH E PASSWOR DIS IRQY3U5Q DG
TWITHOUTTHE QUOTES. THI SISTHEF
```

Q7 Team Name

0 Points

Goldfish