Q1 Commands
5 Points

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

1. go
2. read
3. enter
4. read

Q2 Cryptosystem
5 Points

What cryptosystem was used at this level?

Substitution Cipher

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:
1. Used Python program to check whether the given ciphertext can be decrypted with Caesar Cipher or Substitution Cipher.
2. Took reference of table showing frequencies of letters in English language from internet.

Observations:
1. First we proceeded with Caesar Cipher. We found out that none of the 26 shifts made any sense.

2. Now we proceeded with Substitution Cipher. So we calculated the frequencies of all letters in the given ciphertext.

3. After performing frequency analysis, we found the most frequently occurred letters in ciphertext as follows:

```
[(' ', 17.846),
 ('Y', 11.077),
 ('M', 8.615),
 ('A', 8.308),
 ('W', 7.692),
 ('E', 6.769),
 ('G', 4.308),
 ('S', 4.0),
 ('P', 4.0),
 ('H', 3.692),
 ('I', 2.769),
 ('N', 2.154),
 ('J', 2.154),
 ('O', 2.154),
 ('U', 1.846),
 ('T', 1.846),
 ('R', 1.538),
 ('K', 1.538),
 ('V', 1.231),
 ('.', 1.231),
 ('F', 1.231),
 ('D', 0.923),
 ('X', 0.923),
 ('B', 0.615),
 ('8', 0.308),
 ('0', 0.308),
 ('3', 0.308),
 (',', 0.308),
 ('!', 0.308)]
```

NOTE: We haven't removed spaces from ciphertext while doing our analysis, that's the reason we are getting highest frequency of spaces. But the most frequently occurred alphabetic letter in our ciphertext is 'y'.

4. Since 'y' is the most frequent letter in our ciphertext, we have substituted it with 'e' which is the most frequently occurred letter in English Language.
5. We found that 'me' is the most frequent bigram in our ciphertext(from bigram frequency analysis), so we replaced it with 'th' which is the most frequent bigram in English Vocabulary.
So till this point we are able to guess 3 letters, Y->E, M->T,E->H
After replacing above 3 letters, cipher text looks like:

```
Thwa wa the twsat ihpjoes gt the ipbea.
    Pa xgn iph aee, these wa hgthwhr gt
    whteseat wh the iepjoes. Agje gt the kptes
```

ihpjoesa vwkk oe jgse whteseatwhr thph
thwa ghe! The igue naeu tgs thwa jeaapre
wa p awjfke anoatwtntwgh iwfhes wh vhwih
uwrwta hpbe oeeh ahwtteu ox 8 fkpiea.
The fpaavgsu wa "txSrN03uwdd" vwthgnt the
dngtea

6. Now we observed that 'Thwa' is looks like 'This' so we replace 'wa' with 'is'.

At this point cipher text look like:

This is the twsat ihpjoes gt the ipbea.
Pa xgn iph aee, these is hgthwhr gt
whteseat wh the iepjoes. Agje gt the kptes
ihpjoesa vwkk oe jgse whteseatwhr thph
this ghe! The igue naeu tgs this jeaapre
is p awjfke anoatwtntwgh iwfhes wh vhwih
uwrwta hpbe oeeh ahwtteu ox 8 fkpiea.
The fpaavgsu is "txSrN03uwdd" vwthgnt the
dngtea

7. Now we try to replace 'w' with 'i' and 'a' with 's' and check is this replacement make any useful words or not.

At this point cipher text look like:

This is the tisst ihpjoes gt the ipbes.
Ps xgn iph see, these is hgthihr gt
Ihtesest ih the ihpjoes. Sgje gt the kptes
ihpjoess vikk oe jgse ihtesestihr thph
this ghe! The igue nseu tgs this jesspre
is p sijfke snostitntigh iifhes ih vhiih
uirits hpbe oeeh shitteu ox 8 fkpies.
The fpssvgsu is "txSrN03uidd" vithgnt the
dngtes

So it make some useful words like 'see'

8. Now we can see 'p' is alone so according to English dictonery only i or a is alone so here we have set of word like 'is p' so we can see 'p' is replaceable by 'a'.

At this point cipher text look like:

This is the tisst ihajoes gt the iabes.
As xgn iah see, these is hgthihr gt
Ihtesest ih the ihajoes. Sgje gt the kates
ihajoess vikk oe jgse ihtesestihr thah
this ghe! The igue nseu tgs this jessare

is a sijfke snostitntigh iifhes ih vhiih
uirits habe oeeh shitteu ox 8 fkaies.
The fassvgsu is "txSrN03uidd" vithgnt the
dngtes

9. Here we observed some words like ‘thah’, ‘ih the’ where ‘h’ can be replaced by ‘n’.
At this point cipher text look like:
This is the tisst ihajoes gt the iabes.
As xgn ian see, these is ngthinr gt
Intesest in the ihajoes. Sgje gt the kates
ihajoess vikk oe jgse intesestinr than
this gne! The igue nseu tgs this jessare
is a sijfke snostitntign iifhes in vhiih
uirits habe oeen shitteu ox 8 fkaies.
The fassvgsu is "txSrN03uidd" vithgnt the
Dngtes

10. Here word ‘ian’ should be ‘can’ so we replace ‘i’ with ‘c’.
At this point cipher text look like:
This is the tisst chajoes gt the cabes.
As xgn can see, these is ngthinr gt
Intesest in the chajoes. Sgje gt the kates
chajoess vikk oe jgse intesestinr than
this gne! The cgue nseu tgs this jessare
is a sijfke snostitntign cifhes in vhich
uirits habe oeen shitteu ox 8 fkaces.
The fassvgsu is "txSrN03uidd" vithgnt the
Dngtes

11. Now we find the word ‘oe’, here ‘e’ is fixed using the previous guess, so there are two letters possible ‘we’ and ‘be’, to remove this ambiguity we find one more word ‘oeen’, if we replace ‘o’ with ‘w’ then word becomes ‘ween’ but this is not frequently occurred word in English sentences so here only one possibility ‘been’ is possible which is frequently occur in English sentences. So we replace ‘o’ with ‘b’.
At this point cipher text look like:
This is the tisst chajbes gt the cabes.
As xgn can see, these is ngthinr gt
Intesest in the chajbes. Sgje gt the kates
chajbess vikk be jgse intesestinr than
this gne! The cgue nseu tgs this jessare
is a sijfke snbstitntign cifhes in vhich

uirits habe been shitteu bx 8 fkaces.
The fassvgsu is "txSrN03uidd" vithgnt the
Dngtes

12. From word ‘Intesest’ we can replace ‘s’ with ‘r’, from word ‘gne’ we can replace ‘g’ with ‘o’, from word ‘vhich’ we can replace ‘v’ with ‘w’.
At this point cipher text look like:
This is the tirst chajber ot the cabes.
As xon can see, there is nothinr ot
Interest in the chajber. Soje ot the kater
chajbers wikk be jore interestinr than
this one! The coue nseu tor this jessare
is a sijfke snbstitntion cifher in which
uirits habe been shitteu bx 8 fkaces.
The fassworu is "txRrN03uidd" withont the
Dnotes

13. Now word ‘tirst‘ will be ‘first’ so we replace ‘t’ with ‘f’.
Word ‘nothinr’ will ‘nothing’ so we replace ‘r’ with ‘g’,
word ‘cifher’ will ‘cipher’ so we replace ‘f’ with ‘p’,
word ‘withont’ will be ‘without’ so we replace ‘n’ with ‘u’.
At this point cipher text look like:
This is the first chajber of the cabes.
As xou can see, there is nothing of
Interest in the chajber. Soje of the kater
chajbers wikk be jore interesting than
this one! The coue useu for this jessage
is a sijpke substitution cipher in which
uigits habe been shifteu bx 8 pkaces.
The passworu is "txRgU03uidd" without the
Duotes

14. Word ‘jore’ will be ‘more’ so we replace ‘j’ with ‘m’
Word ‘xou’ will be ‘you’ so we replace ‘x’ with ‘y’
Word ‘wikk’ will be ‘will’ so we replace ‘k’ with ‘l’
Word ‘uigits’ will be ‘digits’ so we replace ‘u’ with ‘d’
At this point cipher text look like:
This is the first chamber of the cabes.
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 habe been shifted by 8 places.
The password is "tyRgU03didd" without the
Duotes

15. Word ‘habe’ will be ‘have’ so we replace ‘b’ with ‘v’
Word ‘Duotes’ will be ‘Quotes’ so we replace ‘D’ with ‘Q’
So now we get final decrypted form is :
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. After decrypting the ciphertext, we get to know that "DIGITS HAVE BEEN SHIFTED BY 8 PLACES". As per our analysis, we found that digits are encrypted using following formulae:
E(x) = (x + x) % 10
In our case E(x) = 8. So the only possible values of x are 4 and 9. So we need to shift digits by either 4 places or 9 places. Lets first assume x = 4. So we shifted digits 0 & 3 to 4 places and hence they become 6 & 9 respectively. So our decrypted text becomes "tyRgU69diqq". On submitting this decrypted text, it showed correct. So we didn't check for other value of x because we already got correct decrypted text.

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 :
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 8 places.
The password is "tyRgU69diqq" without the
Quotes.

Mapping :

A -> S
B -> V
C -> $
D -> Q
E -> H
F -> P
G -> O
H -> N
I -> C
J -> M
K -> L
L -> $
M -> T
N -> U
O -> B
P -> A
Q -> $
R -> G
S -> R
T -> F
U -> D
V -> W
W -> I
X -> Y
Y -> E
Z -> $

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

▾ cs641_assg1.ipynb Download

In [1]:

```
encrypted_text = "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."
```

SHIFT CIPHER / CAESAR CIPHER

In [2]:

```
for j in range(1,27):
    plain = ""
    for i in range(len(encrypted_text)):
        if(encrypted_text[i].isupper()):
            plain += chr(((ord(encrypted_text[i]) + j - 65) % 26) + 65)
        elif(encrypted_text[i].islower()):
            plain += chr((ord(encrypted_text[i]) + j - 97) % 26 + 97)
        else:
            plain += encrypted_text[i]
    print(plain)
    print("\n")
```

```
Nfxb xb nfz uxtbn jfqkpzt hu nfz jqczb. Qb yho jqi bzz, nfztz


Ogyc yc oga vyuco kgrlqau iv oga krdac. Rc zip krj caa, ogau


Phzd zd phb wzvdp lhsmrbv jw phb lsebd. Sd ajq lsk dbb, phb
```

Qiae ae qic xaweq mitnscw kx qic mtfce. Te bkr mtl ecc, qicw

Rjbf bf rjd ybxfr njuotdx ly rjd nugdf. Uf cls num fdd, rjdxd b

Skcg cg ske zcygs okvpuey mz ske ovheg. Vg dmt ovn gee, sk

Tldh dh tlf adzht plwqvfz na tlf pwifh. Wh enu pwo hff, tlfzf c

Umei ei umg beaiu qmxrwga ob umg qxjgi. Xi fov qxp igg, ur

Vnfj fj vnh cfbjv rnysxhb pc vnh rykhj. Yj gpw ryq jhh, vnhbl

Wogk gk woi dgckw soztyic qd woi szlik. Zk hqx szr kii, woic

Xphl hl xpj ehdlx tpauzjd re xpj tamjl. Al iry tas ljj, xpjdj hl sr

Yqim im yqk fiemy uqbvake sf yqk ubnkm. Bm jsz ubt mkk, y

Zrjn jn zrl gjfnz vrcwblf tg zrl vcoln. Cn kta vcu nll, zrlfl jn ut

Asko ko asm hkgoa wsdxcmg uh asm wdpmo. Do lub wdv om

Btlp lp btn ilhpb xteydnh vi btn xeqnp. Ep mvc xew pnn, btnh

Cumq mq cuo jmiqc yufzeoi wj cuo yfroq. Fq nwd yfx qoo, cu

Dvnr nr dvp knjrd zvgafpj xk dvp zgspr. Gr oxe zgy rpp, dvpjj

Ewos os ewq lokse awhbgqk yl ewq ahtqs. Hs pyf ahz sqq, ew

Fxpt pt fxr mpltf bxichrl zm fxr biurt. It qzg bia trr, fxrlr pt azt

Gyqu qu gys nqmug cyjdism an gys cjvsu. Ju rah cjb uss, gysr

Hzrv rv hzt ornvh dzkejtn bo hzt dkwtv. Kv sbi dkc vtt, hztnt r

Iasw sw iau psowi ealfkuo cp iau elxuw. Lw tcj eld wuu, iauor

Jbtx tx jbv qtpxj fbmglvp dq jbv fmyvx. Mx udk fme xvv, jbvp

```
Kcuy uy kcw ruqyk gcnhmwq er kcw gnzwy. Ny vel gnf yww
```

```
Ldvz vz ldx svrzl hdoinxr fs ldx hoaxz. Oz wfm hog zxx, ldxr
```

```
Mewa wa mey twsam iepjoys gt mey ipbya. Pa xgn iph ayy, m
```

FREQUENCY ANALYSIS

In [3]:

```
encrypted_text = encrypted_text.upper() #since there are small as well as capital letters in encrypted text, so for frequency analysis we converted each letter to corresponding capital letter
encrypted_text
```

Out [3]:

```
'MEWA WA MEY TWSAM IEPJOYS GT MEY IPBYA. PA X
```

In [4]:

```
l = len(encrypted_text)
unigrams = {i: round(encrypted_text.count(i) / l * 100, 3) for i in set(encrypted_text)}
```

In [5]:

```
sorted(unigrams.items(), key = lambda k: k[1], reverse = True)
```

Out [5]:

```
[(' ', 17.846),
 ('Y', 11.077),
 ('M', 8.615),
 ('A', 8.308),
 ('W', 7.692),
 ('E', 6.769),
 ('G', 4.308),
 ('P', 4.0),
 ('S', 4.0),
 ('H', 3.692),
 ('I', 2.769),
 ('N', 2.154),
 ('O', 2.154),
 ('J', 2.154),
 ('U', 1.846),
 ('T', 1.846),
 ('R', 1.538),
 ('K', 1.538),
 ('.', 1.231),
 ('V', 1.231),
 ('F', 1.231),
('D', 0.923),
('X', 0.923),
('B', 0.615),
('3', 0.308),
('0', 0.308),
('8', 0.308),
('!', 0.308),
(',', 0.308)]
```

In [6]:

```
from collections import Counter
encrypted_text = encrypted_text.replace(" ", "")
```

In [7]:

```
bigrams = Counter(encrypted_text[i : i + 2] for i in
range(len(encrypted_text) - 1))
bigrams.most_common
```

Out [7]:

```
<bound method Counter.most_common of Counter({'ME': 14,
```

Q7 Team Name
0 Points

crypt_elite

Assignment 1

● Graded

Group
SHRAWAN KUMAR
HARIS KHAN
KAPILKUMAR KISHORBHAI KATHIRIYA
✎ View or edit group

Total Points
41 / 50 pts

Question 1
Commands

5 / 5 pts

Question 2

Cryptosystem	R 3 / 5 pts
Question 3 Analysis	25 / 25 pts
Question 4 Mapping	3 / 10 pts
Question 5 Password	5 / 5 pts
Question 6 Codes	0 / 0 pts
Question 7 Team Name	0 / 0 pts