Q1 Commands
5 Points

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

1. climb
2. read
3. enter
4. 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)

After seeing the cipher text, it looked like that one of Caesars cipher or substitution cipher was used to encrypt the text. But after applying all the 26 shifts to the letters, none of them gave us the meaningful text. Then we tried to apply frequency analysis by observing the frequencies of the letters used in the encrypted text. We calculated the frequency of each letter using a python code in Jupyter notebook. Then we matched the frequencies of the letters in the given text with that of a standard letters frequency. We noticed that the most frequent character is 'c' , so we replaced it by 'e' and the second most frequent letter 'f' was replaced by 't' then we got the word "tie" for "fic" in cipher text, so we replaced 'i' with 'h' to form "the". We tried to make several

possible matches by observing if some meaningful words were being formed or not. We came to know that the letters were not matching exactly in the order of the standard frequency table, that is why we have to try several letters with similar frequencies to replace a specific letter from the cipher text. We made an observation that the first word that was formed was "irst" which was not making any meaning ,but we observed that if the words at the end of the text were shifted to the start, a meaningful word "first " was formed and hence we shifted all the words after the fullstop in the last line to the start of the text which gave us "Thi sisthef irst". We can clearly see that the spaces are placed randomly in the text. So we tried to place the spaces at correct positions as and when a meaningful word was being formed.
For the mapping of digits, It is given in the plain text that the digits have been shifted by 2 places. If the original number before shifting is "x" then, it becomes (x+s) modulo 10 after shifting, where s is the number of digits the number has been shifted by. Since each digit is shifted, the digit 2 is also shifted. If the original digit in place of 2 before shifting is "s", after shifting the digit "s" itself, it becomes (s+s) modulo 10. That is, (2*s) modulo 10 is equal to 2. Here, only s=1 and s=6 gives (2*s) modulo 10 = 2. Which means that the digits must have been shifted by either 1 or 6. Reverse shifting the digits 9 and 1 in the password by 1 gives 8 and 0 respectively, but this password does not open the door, but reverse shifting the digits by 6 gives 3 and 5 and this opens the door. Hence the correct original digits are 6,3 and 5 in place of 2,9 and 1 in the decrypted text.Hence the password is "iRqy3U5qdgt".

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 ciphertext space is :
[F,H,K,M,V,a,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,u,v,x,y,1,2,9]
The plaintext space is :
[A,R,S,T,U,a,b,c,d,e,f,g,h,i,l,m,n,o,p,q,r,s,t,u,v,w,y,3,5,6]

The ciphertext to plaintext mapping is as follows:

c - e
f - t
k - s
o - i
i - h
g - o
h - a
m - r
q - n
p - c
v - u
n - b
d - m
y - d
e - f
v - u
a - g
j - p
l - w
x - q
r - y
s - v
F - T
H - A
K - S
M - R
V - U
1 - 5
2 - 6
9 - 3

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

frequencygenerator.ipynb Download

In [27]:
```
s="""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"""
```

In [28]:
```
s=s.lower()
```

In [29]:
```
s=list(s)
```

In [30]:
```
d={}
size=0
for i in s:
    if(i>='a'and i<='z'):
        size+=1
        if i not in d:
            d[i]=1
        else:
            d[i]+=1
```

In [31]:
```
for i in d:
    d[i]=d[i]/size*100
```

In [32]:
```
dict(sorted(d.items(), key=lambda item:
item[1],reverse=True))
```

Out [32]:
```
{'c': 13.953488372093023,
 'f': 10.852713178294573,
 'k': 10.465116279069768,
 'o': 9.689922480620156,
 'i': 8.527131782945736,
 'g': 5.426356589147287,
 'm': 5.038759689922481,
 'h': 5.038759689922481,
 'q': 4.651162790697675,
```

```
 'p': 3.488372093023256,
 'd': 2.7131782945736433,
 'n': 2.7131782945736433,
 'v': 2.7131782945736433,
 'e': 2.3255813953488373,
 'y': 2.3255813953488373,
 'a': 1.937984496124031,
 'u': 1.937984496124031,
 'l': 1.550387596899225,
 'j': 1.550387596899225,
 'r': 1.1627906976744187,
 'x': 1.1627906976744187,
 's': 0.7751937984496124}
```

In [ ]:

Q7 Team Name

0 Points

DECODERS

Assignment 1

GRADED

GROUP

Akash Gajanan Panzade
Manthan Kojage
Abhishek Dnyaneshwar Revskar
View or edit group

TOTAL POINTS

48 / 50 pts

QUESTION 1

Commands

5 / 5 pts

✔ **+ 5 pts** Correct
1. climb, read, enter, read
2. climb, enter, read
3. go, read, enter, read
4. go, enter, read

+ 0 pts Wrong or NA

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