Assignment 1

● Graded

Group

ABHAYA PRATAP SINGH
ANANYAE KUMAR BHARTARI
NAVEEN KUMAR MATHUR
View or edit group

Total Points

37 / 50 pts

Question 1

Commands

5 / 5 pts

+ 0 pts Incorrect

✔ + 5 pts Correct

Question 2

Cryptosystem

5 / 5 pts

✔ + 5 pts Correct

+ 0 pts Incorrect

Question 3

Analysis

15 / 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 Give a mathematical explanation for the shift in the numbers

+ 0 pts Wrong answer or NA

Question 4

Mapping

7 / 10 pts

✔ + 5 pts The mapping used for alphabets and numbers.

✔ + 5 pts Plaintext space and ciphertext space is the set of all strings containing English alphabets, numbers and punctuation marks.

+ 0 pts Wrong answer or NA

– 3 pts numbers mapping not correct. also not mentioned what contained in ciphertext and plaintext space example punctuation, numbers

Question 5

Password

5 / 5 pts

✔ **+ 5 pts** Correct

✔ **+ 0 pts** Incorrect

Question 6

Codes

0 / 0 pts

✔ **+ 0 pts** Correct

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

Q3 Analysis
25 Points

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

We used python 3.
Discrepancy of space:-
presence of single letter a,y implies a will be either a or i
presence of "fpaavgs" in cypher implies a word having "ii" or "aa" in 3 position which can be skiing or kraaled ran into problem while solving using these("sy" was the problem causer)
Using frequency analysis:-
"y" frequency 11.9 so has to be "e"
presence of "Me" 3-4 place in text hence tried "th" for them as " Me y fpaavgs " will become "the". and frequency of "m"-9.2 and "e"-7.3 so doable.
"Mew a" at the end used "this" a (little guess involved) therefore "fpaavgs" has double "ss" searched in the dictionary and got 3 words, happy to see "password" among the word used it and solved the 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)

Plaintext space consists of strings composed of symbols from an alphabet of definition but ciphertext space consists of strings composed of symbols from an alphabet of definition which might or might not differ from that of plaintext space.

Mapping of ciphertext with plaintext is as follows:
'y' with 'e'
'm' with 't'
'e' with 'h'
'w' with 'i'
'a' with 's'
'f' with 'p'
'p' with 'a'
'v' with 'w'
'g' with 'o'
's' with 'r'
'u' with 'd'
'n' with 'u'
'd' with 'q'
'i' with 'c'
'h' with 'n'
'k' with 'l'
'j' with 'm'
'o' with 'b'
't' with 'f'
'b' with 'v'
'x' with 'y'
'r' with 'g'
'8' with '6'
'0' with '6'
'3' with '9'

Q5 Password

5 Points

What was the final command used to clear this level?

tyRgU69diqq

Q6 Codes

0 Points

Upload any code that you have used to solve this level.

assignment1.py3 Download

```
def replac_(a,dic):
    ans=''
    for i in range(0,len(a)):
        j=a[i]
        if j in dic.keys():
            ans=ans+dic[j]
        else:
            ans=ans+j
    return ans
a=" wsam ie pjo ysgtm eyipbya .P axg niphay y,mey syw ahgm ewhrg tw hmysyam wh meyiepjoys .Ag jygtmeyk pmys ie pjo ysavw kkoyjgsywhmy sy amwh rmephmewagh y!Me yigu ynay utgsmew ajya apr ywap awjfkya no a mwmnmwghiwfeyswhve wieuwr wm aepby oyyhae wtmyuox8 fkpiya. Me y fpaavgs uwa mxSrN03u wddvwmegnmmey dngmya. Mew awameyt".lower()
c=0
d=dict()
for j in range(0,len(a)):
    i=a[j]
    c=c+1
    if i not in d.keys():
        d[i]=0
    d[i]=d[i]+1
for j in d.keys():
    if j !=" ":
        d[j]=round(d[j]*100/(c-16),1);
print(d)
print()
print()
dnew=
{"y":"e","m":"t","e":"h","w":"i","a":"s","f":"p","p":"a","v":"w","g":"o","s":"r","u":"d","n":"u",
print(len(dnew.keys()))
#dnew={"y":"a","a":"i"}
#dnew={"w":"t","s":"h","a":"i","m":"s"}
print(a)
print()
print()
print(replac_(a, dnew))
```