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 was used at this level.

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.

We did the frequency analysis of the ciphertext, then we got to know that the mapping for the most frequent letter in the English language which is 'e' is 'h'. Similarly, we found the mapping for the second most frequent letter which is 't'. The mapping we found was 't' -> 'f'. From this, we got to know that the cryptoanalysis method used here was substitution cipher. Then we tried to substitute known characters into ciphertext and found semi-plaintext. From the analysis and the word knowledge of the English language, we got to know the rest of the mappings in the following way.

We observed that the password would be in double quotes. So, our observation was that the sentence containing the password would be "The password is "mxSrN03uwdd" ". Thus, we have discovered some of the mappings of letters. Then, we created a python script in which we took ciphertext as input and substituted letters for which the mappings are known and the rest of the letters are substituted by underscores '_'. This is how we got semi-plaintext and we guessed the rest of the mappings gradually. We gradually updated mappings in our code and it was easier to guess the rest of the words using the word knowledge of English knowledge.

This is how we got possible mappings. When this ciphertext is converted to plaintext we got the password and in the plaintext, it was written that digits are shifted by 8 places. So, we shifted '8' by 8 places and got '6'. It means that digits are shifted by 6 places. So, we shifted two digits in the password of the ciphertext by 6 places. We converted 0 -> 6 and 3 -> 9.

0 -> (0 + 6)%10 = 6
3 -> (3 + 6)%10 = 9

This is how we finally got the password in plaintext as "tyRgU69diqq".

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 ->
This is any text which is readable and understandable before converting to ciphertext or after decrypting from ciphertext to readable text.

Ciphertext space ->

This is any text which is encrypted using some encryption technique. It is non-readable and non-understandable until converted to plaintext using a decryption technique.

Mappings ->

```
{
	'm':'t',
	'e':'h',
	'y':'e',
	'f':'p',
	'p':'a',
	'a':'s',
	'v':'w',
	'g':'o',
	's':'r',
	'u':'d',
	'w':'i',
	't':'f',
	'i':'c',
	'j':'m',
	'o':'b',
	'b':'v',
	'h':'n',
	'r':'g',
	'n':'u',
	'k':'l',
	'd':'q',
	'x':'y'
}
```

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

asn1.py Download

```
dic = {'m':'t',
        'e':'h',
        'y':'e',
        'f':'p',
        'p':'a',
        'a':'s',
        'v':'w',
        'g':'o',
        's':'r',
        'u':'d',
        'w':'i',
        't':'f',
        'i':'c',
        'j':'m',
        'o':'b',
        'b':'v',
        'h':'n',
        'r':'g',
        'n':'u',
        'k':'l',
        'd':'q',
        'x':'y'
        }

s = str(input())
s = s.lower()
ans = ""
for i in range(len(s)):
    if s[i] in dic:
        ans += dic[s[i]]
    else:
        if(s[i].isalpha()):
            ans += '_'
        else:
            ans += s[i]
print(ans)
```

Q7 Team Name

0 Points

the_boys

Assignment 1

Graded

Group

SANKET SANJAY KALE
PRATIK MAHIPAL PATIL
ADITYA SUNILKUMAR KANKRIYA
View or edit group

Total Points

39 / 50 pts

Question 1

Commands — **5** / 5 pts

Question 2

Cryptosystem — **3** / 5 pts

Question 3

Analysis — **20** / 25 pts

Question 4

Mapping — **6** / 10 pts

Question 5

Password — **5** / 5 pts

Question 6

Codes — **0** / 0 pts

Question 7

Team Name — **0** / 0 pts