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 our the cryptosystem? (Explain in less than 100 words)

We first used the Caesar Cipher but for every possible shift, we didn't get meaningful statements. We calculated the frequency of each letter and then observed that some letters are more frequent than others. We then used frequency analysis to decode the ciphertext. We used standard English Alphabets Frequency table to substitute the letters until we get something meaningful (disregarding the position of the spaces). To find the mapping, we analyzed bigrams and trigrams like 'on', 'of', 'the' etc. After we found out the mapping we observed that the actual ciphertext is rotated. In the plain text, it was given "digits are shifted by 2 places", which means the actual shifting is by 4 digits, we tried shifting both of the digits in the password forward and backward by 4 places and then 2 places for each of them (which sum to 4). Finally, 4 places forward with modulo 10 for each digit gave us the correct password.

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 is the message which is not encrypted and can be understood when read by someone who intercepts it. While ciphertext space is the message which is obtained by encrypting Plaintext and can be understood only if we know the decryption algorithm.

Mapping :

$ciphertext \implies plaintext$
$a \implies g$
$c \implies e$
$d \implies m$
$e \implies f$
$f \implies t$
$g \implies o$
$h \implies a$
$i \implies h$
$j \implies p$
$k \implies s$
$l \implies w$
$m \implies r$
$n \implies b$
$o \implies i$
$p \implies c$
$q \implies n$
$r \implies y$
$s \implies v$
$u \implies l$
$v \implies u$
$x \implies q$
$y \implies d$

Plain Text (after adjusting space and rotation of text) - 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 2 places. The password is iRqy9U1qdgt without the quotes.

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

Cs641_INFINITY.py — Download

```
mapping = ['g', '#', 'e', 'm', 'f', 't', 'o', 'a', 'h', 'p', 's', 'w',
           'r', 'b', 'i', 'c', 'n', 'y', 'v', '#', 'l', 'u', '#', 'q', 'd', '#']

alphabets = [chr(i+ord('a')) for i in range(26)]
print(alphabets)
print(mapping)

print(len(mapping))

key = [(c[0], c[1]) for c in zip(alphabets, mapping)]
for k in key:
    print(str(k[0])+"=>" + str(k[1]))

print(key)


def decrypt(cipherText):
    cipherText = [c for c in list(cipherText.lower())]
    ans = ""
    for c in list(cipherText):
        if ord(c) <= ord('z') and ord(c) >= ord('a'):
            c = mapping[ord(c)-ord('a')]
        ans += c

    print(''.join(ans))


cipher_text = "omkf pi hdn cmgef icphsck .H krg vphqkc c,fic mco kqgf ioqag eo qfcmckf oq ficpihdncm .Kg dcgeficu hfcm pi hdn cmklo uuncdgmcoqfc mc kfoq afihqfiokgqg c!Fi cpgy cvkc yegmfio kdck kha cokh kodjuck vn k fofvfogqpojicmoqli opiyoa of kihsc nccqki oefcynr2 juhpck. Fi c jhkklgm yok oMxr9V1x yaflofigvffic xvgfck. Fio kokfice"
decrypt(cipher_text.replace(" ", ""))


cipher_adjusted_space = "Fiok ok fic eomkf pihdncm ge fic phsck .Hk rgv phq kcc,ficmc ok qgfioqa ge oqfcmckf oq fic pihdncm .Kgdc ge fic uhfcm pihdncmk louu nc dgmc oqfcmckfoqa fihq fiok gqc!Fic pgyc vkcy egm fiok dckkhac ok h kodjuc kvnkfofvfogq pojicm oq liopi yoaofk ihsc nccq kioefcy nr 2 juhpck. Fic jhkklgmy ok oMxr9V1xyaf lofigvf fic xvgfck."
decrypt(cipher_adjusted_space)

```

Q7 Team Name
0 Points

INFINITY