Q1 Commands
5 Points

List the commands was used in this level?

enter,enter,pick,back,give,back,back,thrnxxtzy,read,the_magic_of_wand

Q2 Cryptosystem
10 Points

What cryptosystem was used in the game to reach the password?

Monoalphabetic Substitution Permutation Cipher was the cryptosystem used in the game to reach the password with block size 5.We discovered the key to be "43512".
Cipher Position: 1 2 3 4 5
Actual Position: 4 3 5 1 2

Q3 Analysis
30 Points

What tools and observations were used to figure out the cryptosystem and the password? (Explain in less than 1000 lines)

Identifying the cipher that was used to encrypt the cipher text is the first step of the assignment. Here are the procedures we took to figure out which encryption was being used:

1)Index of Coincidence: If a monoalphabetic substitution cipher or a polyalphabetic substitution cipher was used to encrypt the text, this can be determined by computing the Index of Coincidence (IC) of the ciphertext. A monoalphabetic substitution cipher is suggested by an IC close to 0.065, whereas a polyalphabetic substitution cipher is suggested by a higher IC. Our encrypted text's IC score of 0.0573 indicates the adoption of a monoalphabetic cipher.

2) Substitution cipher ,vigenere cipher, playfair cipher, permutation cipher etc. are some common monoalphabatic ciphers.

3) Frequency analysis is the most used method for cracking monoalphabatic ciphers. Following are the letters with the highest

frequency determined through frequency analysis:

q-7%
v-7%
a-5%
c-5%

We can see that substitution cipher is being utilised by looking at the frequency. q or v were swapped out for the most common English letter, "e." but nothing significant comes of it. Thus, we concluded that the monoalphabatic substitution cipher is not employed in this assignment.

4) In a next step, we examined the encrypted text's bigram and trigram patterns. Bigram trigram, as the name suggests, is a mixture of many ciphers and we are aware that a letter's permutation will change the bigram trigram frequency. As a result, we deduced that permutation cipher/transposition cipher is also used in this assignment.

5) We made an educated guess that the block size is 5. We may utilise the Kasiski examination to attempt and demonstrate that the block size used in the encryption of the given text is 5. To determine the length of the key used in the Kasiski exmaination, we can check for repeated letter sequences in the cipher text. By reducing the number of potential keys, this may make brute force decryption more practical. We can identify several repeating sequences in the supplied cipher text and determine their distances by using the Kasiski inspection. Here are some instances of repeating sequences and their separations:

"qmnjv": appears at positions 1, 18, 56, 96, 116, 142, 162

"fv": appears at positions 30, 39, 50, 76, 78, 83, 86, 94, 98, 100, 109, 110, 126, 131, 148, 153, 156, 165

The distances between these repeated patterns can then be determined. The separations between the "qmnjv" sequences, for instance, are: 17, 38, 40, 20, 26, 20

The factors of these distances can then be found by looking for them, and they are as follows: 1, 2, 3,4, 5, 10, 17, 20, 34, 68

We can observe that the factor 5 is present, however the block sizes of 1, 2, and 3 are unusually small and 10, 17, 20, 34, and 68 are

excessively huge. hence, 5 is the ideal block size.

6) Determining the key: Given that keys are small (5). By using the brute force method, we can discover all 5 factorial combinations and test them all. We discovered the key to be "43512," or Cipher position, after attempting all 120 combinations. 1 2 3 4 5.
Cipher Position: 1 2 3 4 5
Actual Position: 4 3 5 1 2

7) The encrypted cipher text in this assignment is mentioned below:
qmnjvsa nv wewc flct vprj tj tvvplvl fv xja vqildhc xmlnvc nacyclpa fc gyt vfvw. fv wgqyp, pqq pqcs y wsq rx qmnjvafy cgv tlvhf cw tyl aeuq fv xja tkbv cqnsqs. lhf avawnc cv eas fuqb qvq tc yllrqr xxwa cfy. psdc uqf avrqc gefq pyat trac xwv taa wwd dv eas flcbq. vd trawm vupq quw x decgqcwt, yq yafl vlqs yqklhq! snafq vml lhvqpawr nqg_vfusr_ec_wawy qp fn wgawdgf.

8) First we removed the spaces and the punctuation marks from the cipher text and then applied the transposition cipher on the cipher text with a block of block size 5.

qmnjvsanvwewcflctvprjtjtvvplvlfvxjavqildhcxmlnvcnacyclpafcgytvfv
wfvwgqyppqqpqcsywsqrxqmnjvafycgvtlvhfcwtylaeuqfvxjatkbvcqnsq
slhfavawnccveasfuqbqvqtcyllrqrxxwacfypsdcuqfavrqcgefqpyattracx
wvtaawwddveasflcbqvdtrawmvupqquwxdecgqcwtyqyaflvlqsyqklhqs
nafqvmllhvqpawrnqgvfusrecwawyqpfnwgawdgf

Divide it into block of block size 5.

qmnjv sanvw ewcfl ctvpr jtjtv vplvl fvxja vqild hcxml nvcna cyclp
afcgy tvfvw fvwgq yppqq pqcsy wsqrx qmnjv afycg vtlvh fcwty
laeuq fvxja tkbvc qnsqs lhfav awncc veasf uqbqv qtcyl lrqrx xwacf
ypsdc uqfav rqcge fqpya ttrac xwvta awwdd veasf lcbqv dtraw
mvupq quwxd ecgqc wtyqy aflvl qsyqk lhqsn afqvm llhvq pawrn
qgvfu srecw awyqp fnwga wdgf

Then we applied the transposition on it and obtained the text given below:

Jnvqmvnwsafclewpvrcttjvjtvllvpjxafvlidvqmxlhcncanvlcpcygcyafvf
wtvgwqfvqpqypscypqrqxwsjnvqmcygafvlhvttwyfcueqlajxafvvbctkqs
sqnafvlhcncawsafveqbvuqyclqtrqxlrcafxwdscypafvuqgcerqypafqarctt
tvaxwdwdawsafveqbvlcarwdtpuqmvxwdquqgcecqyywtvllafqykqssqn

lhvqmafvhqllrwnpafvuqgcewsrqypawgwafnwdgf

The above text is obtained after applying transposition cipher with block size of 5.

9) The above text is obtained after re-applying punctutation marks and proper spacing in the text obtained in the above step:

jnvqmvn ws afcl ewpv rctt jv jtvllvp jx afv lidvqmx lhcnca nvlcpcyg cy afv fwtv. gw qfvqp, qyp scyp q rqx ws jnvqmcyg afv lhvtt wy fcu eqla jx afv vbct kqssqn. afv lhcnca ws afv eqbv uqy cl qtrqxl rcaf xwd. scyp afv uqgce rqyp afqa rctt tva xwd wda ws afv eqbvl. ca rwdtp uqmv xwd q uqgcecqy, yw tvll afqy kqssqn! lhvqm afv hqllrwnp afv_uqgce_ws_rqyp aw gw afnwdgf.

10) Now, we have to apply the frequency analysis on the above text in order to get the decrypted text.

In this paragraph, we find a single letter which is 'q', then we made an intelligent guess that it can be mapped to 'i' or 'a'. Then we found out that 'q' is mapped to 'a'.

=> 'q'=>'a' : jnvamvn ws afcl ewpv rctt jv jtvllvp jx afv lidvamx lhcnca nvlcpcyg cy afv fwtv. gw afvap, ayp scyp a rax ws jnvamcyg afv lhvtt wy fcu eala jx afv vbct kassan. afv lhcnca ws afv eabv uay cl atraxl rcaf xwd. scyp afv uagce rayp afaa rctt tva xwd wda ws afv eabvl. ca rwdtp uamv xwd a uagcecay, yw tvll afay kassan! lhvam afv hallrwnp afv_uagce_ws_rayp aw gw afnwdgf.

11) After that we determined that 'v' is the most frequent letter in the encrypted text so we mapped 'v' to 'e'

=> 'v' => 'e' : jneamen ws afcl ewpe rctt je jtellep jx afe lideamx lhcnca nelcpcyg cy afe fwte. gw afeap, ayp scyp a rax ws jneamcyg afe lhett wy fcu eala jx afe ebct kassan. afe lhcnca ws afe eabe uay cl atraxl rcaf xwd. scyp afe uagce rayp afaa rctt tea xwd wda ws afe eabel. ca rwdtp uame xwd a uagcecay, yw tell afay kassan! lheam afe hallrwnp afe_uagce_ws_rayp aw gw afnwdgf.

12) Now we found that 'a' is next most frequent letter in the cipher text and in the English language letter 't' is second most frequent letter, therefore we have mapped 'a' to 't'.

=> 'a' => 't' : jneamen ws tfcl ewpe rctt je jtellep jx tfe lideamx lhcnct nelcpcyg cy tfe fwte. gw afeap, ayp scyp a rax ws jneamcyg tfe lhett wy fcu ealt jx tfe ebct kassan. tfe lhcnct ws tfe eabe uay cl atraxl rctf xwd. scyp tfe uagce rayp tfat rctt tet xwd wdt ws tfe eabel. ct rwdtp uame xwd a uagcecay, yw tell tfay kassan! lheam tfe hallrwnp tfe_uagce_ws_rayp tw gw tfnwdgf.

13) Now we found that 'tfe' in the modified cipher text, it gives us the clear evidence that it is 'the' so we have mapped 'f' to 'h'.

=> 'f' => 'h' : jneamen ws thcl ewpe rctt je jtellep jx the lideamx lhcnct nelcpcyg cy the hwte. gw aheap, ayp scyp a rax ws jneamcyg the lhett wy hcu ealt jx the ebct kassan. the lhcnct ws the eabe uay cl atraxl rcth xwd. scyp the uagce rayp that rctt tet xwd wdt ws the eabel. ct rwdtp uame xwd a uagcecay, yw tell thay kassan! lheam the hallrwnp the_uagce_ws_rayp tw gw thnwdgh.

14) Now we observed two letter words in the cipher text 'je' and 'tw', it can be easily seen that we can map 'j'=>'b' and 'w'=>'o' so that the word will become 'be' and 'to'.

'j'=>'b' and 'w'=>'o' => bneamen os thcl eope rctt be btellep bx the lideamx lhcnct nelcpcyg cy the hote. go aheap, ayp scyp a rax os bneamcyg the lhett oy hcu ealt bx the ebct kassan. the lhcnct os the eabe uay cl atraxl rcth xod. scyp the uagce rayp that rctt tet xod odt os the eabel. ct rodtp uame xod a uagcecay, yo tell thay kassan! lheam the hallronp the_uagce_os_rayp to go thnodgh.

15) Now we found two letter words in the cipher text 'oy' and 'yo' , it can be easily seen that we can map 'y'=>'n' so that the word will become 'no'.
'y' => 'n' : bneamen os thcl eope rctt be btellep bx the lideamx lhcnct nelcpcng cn the hote. go aheap, anp scnp a rax os bneamcng the lhett on hcu ealt bx the ebct kassan. the lhcnct os the eabe uan cl atraxl rcth xod. scnp the uagce ranp that rctt tet xod odt os the eabel. ct rodtp uame xod a uagcecan, no tell than kassan! lheam the hallronp the_uagce_os_ranp to go thnodgh.

16) Now we found 'os' it can be easily seen that we can map 's'=>'f' so that the word will become 'of'.

And we found 'odt' it can be easily seen that we can map 'd'=>'u' so that the word will become 'out'.

'd'=>'u' : bneamen of thcl eope rctt be btellep bx the liueamx lhcnct nelcpcng cn the hote. go aheap, anp fcnp a rax of bneamcng the lhett on hcu ealt bx the ebct kaffan. the lhcnct of the eabe uan cl atraxl rcth xou. fcnp the uagce ranp that rctt tet xou out of the eabel. ct routp uame xou a uagcecan, no tell than kaffan! lheam the hallronp the_uagce_of_ranp to go thnough.

17) Now we found two letter words in the cipher text 'xou' and 'bx', it can be easily seen that we can map 'x'=>'y' so that the word will become 'you' and 'by'.
'x'=>'y' : bneamen of thcl eope rctt be btellep by the liueamy lhcnct nelcpcng cn the hote. go aheap, anp fcnp a ray of bneamcng the lhett on hcu ealt by the ebct kaffan. the lhcnct of the eabe uan cl atrayl rcth you. fcnp the uagce ranp that rctt tet you out of the eabel. ct routp uame you a uagcecan, no tell than kaffan! lheam the hallronp the_uagce_of_ranp to go thnough.

18) now we found two letter words in the cipher text 'aheap' and 'anp', it can be easily seen that we can map 'P'=>'D' so that the word will become 'AHEAD' and 'AND'.
'p' => 'd' : bneamen of thcl eode rctt be btelled by the liueamy lhcnct nelcdcng cn the hote. go ahead, and fcnd a ray of bneamcng the lhett on hcu ealt by the ebct kaffan. the lhcnct of the eabe uan cl atrayl rcth you. fcnd the uagce rand that rctt tet you out of the eabel. ct routd uame you a uagcecan, no tell than kaffan! lheam the hallrond the_uagce_of_rand to go thnough.

19) now we found two letter words in the cipher text 'ct' and 'thnough' , it can be easily seen that we can map 'c'=>'i' and 'n'=>'r' so that the word will become 'it' and 'through'.

'c'=>'i' and 'n'=>'r' : breamer of thil eode ritt be btelled by the liueamy lhirit reliding in the hote. go ahead, and find a ray of breaming the lhett on hiu ealt by the ebit kaffar. the lhirit of the eabe uan il atrayl rith you. find the uagie rand that ritt tet you out of the eabel. it routd uame you a uagieian, no tell than kaffar! lheam the hallrord the_uagie_of_rand to go through.

20) Now we found one letter word in the cipher text 'breamer', it can be easily seen that we can map 'm'=>'k' and it becomes 'breaker'.

21) Now we found one letter word in the cipher text 'thil', it can be easily seen that we can map 'l'=>'s' and it becomes 'this'.

22) Now we found one letter word in the cipher text 'atrays', it can be easily seen that we can map 't'=>'l' and 'r'=>'w' and it becomes 'always'.

23) Now we found one letter word in the cipher text 'breamer', it can be easily seen that we can map 'm'=>'k' and it becomes 'breaker'.

24) now we found words in the cipher text 'hassword' , 'breaking', 'ebil', 'eave' it can be easily seen that we can map 'h'=>'p' , 'g'=>'g' , 'e'=>'c' and it becomes 'password' , 'breaking', 'evil' , 'cave'.

25) Now we found the words in the cipher text 'uagic', 'uake', it can be easily seen that we can map 'm'=>'k' and it becomes 'magic', 'make'.

26) Mappings obtained:
Mapping = {'a': 't', 'b': 'v', 'c': 'i', 'd': 'u', 'e': 'c', 'f': 'h', 'g': 'g', 'h': 'p', 'i': 'q', 'j': 'b', 'l': 's', 'm': 'k', 'n': 'r', 'p': 'd', 'q': 'a', 'r': 'w', 's': 'f', 't': 'l', 'u': 'm', 'v': 'e', 'w': 'o', 'x': 'y', 'y': 'n','k':'j','0':'0','1':'1','2':'2','3':'3','4':'4','5':'5','6':'6','7':'7','8':'8','9':'9','!':'!','@':'@','#':'#','$':'$','%':'%','*':'*','(':'(',')':')','-':'-','_':'_'}

27) Therefore, the decrypted plaintext is :

breaker of this code will be blessed by the squeaky spirit residing in the hole. go ahead, and find a way of breaking the spell on him cast by the evil jaffar. the spirit of the cave man is always with you. find the magic wand that will let you out of the caves. it would make you a magician, no less than jaffar! speak the password the_magic_of_wand to go through.

28) Finally, this way we have determined the password which is "the_magic_of_wand".

Q4 Password
5 Points

What was the final command used to clear this level?

the_magic_of_wand

Q5 Codes
0 Points

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

▾ assignment3.ipynb Download

In [1]:
```
cipher_text = "qmnjvsa nv wewc flct vprj tj
tvvplvl fv xja vqildhc xmlnvc nacyclpa fc gyt
vfvw. fv wgqyp, pqq pqcs y wsq rx qmnjvafy
cgv tlvhf cw tyl aeuq fv xja tkbv cqnsqs. lhf
avawnc cv eas fuqb qvq tc yllrqr xxwa cfy.
psdc uqf avrqc gefq pyat trac xwv taa wwd dv
eas flcbq. vd trawm vupq quw x decgqcwt, yq
yafl vlqs yqklhq! snafq vml lhvqpawr
nqg_vfusr_ec_wawy qp fn wgawdgf."

punctuations =
set(['!','@','#','$','%','^','&','(',')','_','-
','+','=','{','}',';',':','/','?','|','.',' ',',','~','`','[',']','-
','1','2','3','4','5','6','7','8','9','0',','])

# removing space and special characters

temp = ""

for i in cipher_text :
    if i not in punctuations:
        temp += i.lower()
```

In [2]:
```
temp  #encrpted text after space and special
char removal
```

Out [2]:
```
'qmnjvsanvwewcflctvprjtjtvvplvlfvxjavqildhcxmlnvc
```

In [3]:
```
# decoding the permutation - [4,3,5,1,2]
permutated_text = ""
for i in range(len(temp)//5):    # to handle case
if len is not divisible by 5
    permutated_text += temp[i*5+4-1]
    permutated_text += temp[i*5+3-1]
    permutated_text += temp[i*5+5-1]
    permutated_text += temp[i*5+1-1]
    permutated_text += temp[i*5+2-1]
```

```
x = temp[-(len(temp)%5):] # adding remaining string as it is because padding is not used. (giving wrong result when we solved considering it)
permutated_text += x
```

In [4]:
```
permutated_text  #de-permutated_text
```

Out [4]:
```
'jnvqmvnwsafclewpvrcttjvjtvllvpjxafvlidvqmxlhcnca
```

In [5]:
```
# decoding substitution
# mapping
key = {'a': 't', 'b': 'v', 'c': 'i', 'd': 'u', 'e': 'c', 'f': 'h', 'g': 'g', 'q', 'j': 'b', 'l': 's', 'm': 'k', 'n': 'r', 'p': 'd', 'q': 'a', 'r': 'w', 's': 'u': 'm', 'v': 'e', 'w': 'o', 'x': 'y', 'y': 'n','k':'j','0':'0','1':'1','2':'2','3':'3','4':'4','5':'5','6':'6','7':'7', ':':'-','_':'_'}
clean_text = ""
for i in permutated_text:
    clean_text += key[i]
```

In [6]:
```
clean_text
```

Out [6]:
```
'breakerofthiscodewillbeblessedbythesqueakyspiritre
```

In [7]:
```
# adding removed punctuations
perm_text = ""
j = 0
for i in range(len(cipher_text)):
    if cipher_text[i] in punctuations:
        perm_text += cipher_text[i]
    else:
        perm_text += clean_text[j]
        j+= 1
```

In [9]:
```
perm_text  #encrypted_text
```

Out [9]:
```
'breaker of this code will be blessed by the squeaky s
```

In [ ]:
```
```

Q6 Group name

0 Points

team_ethereum

Assignment 3

● Graded

Group
ALLAN ROBEY
AVNISH TRIPATHI
DIVYESH DEVANGKUMAR TRIPATHI
View or edit group

Total Points
50 / 50 pts

Question 1 Commands	5 / 5 pts
Question 2 Cryptosystem	10 / 10 pts
Question 3 Analysis	30 / 30 pts
Question 4 Password	5 / 5 pts
Question 5 Codes	0 / 0 pts
Question 6 Group name	0 / 0 pts