Q1 Commands
5 Points

List the commands was used in this level?

go, put, pull, enter, pick, c, c, climb, give, back, back, thrnxxtzy, read

Q2 Cryptosystem
10 Points

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

Simple Substitution(monoalphabatic) + Permutation cipher

Q3 Analysis
30 Points

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

When we got the ciphertext we first assumed that it is substitution cipher. So we did the frequency analysis, we got nice distribution of the letters as it should be that is 3 letters had frequency about 10%(which most probably could be e,t,a). in short frequency distribution was similar to frequency distribution of a normal English paragraph. So it was clear that substitution was used, but when we did frequency analysis of bigrams and trigrams, they didn't make any sense. and we noticed that there is a word in cipher text "xxwa" but no word start with two same letter. So its not a simple substitution cipher. So we concluded that some other encryption technique is use over simple substitution.

So we assumed that permutation is used (as only substitution and permutation ciphers were discussed in class). To find the length of permutation key we did the analysis of repeated sequence (we found the spaced between repeated keyword).

we found:

Repeated sequence	spacing	possible keylenght
qmn	85	5,17
mnj	85	5,17
njv	85	5,17
flc	186	2,3,5,6
lvl	205	5,41
fvx	80	2,4,5,10
vxj	80	2,4,5,10
xja	80	2,4,5,10
qrx	70	2,5,7,10
pqq	141	3,47
fav	40	2,4,5,10
vea	60	2,3,4,5,6,10

and many more which suggest keylength is 5.

we noticed that there is word in cipher text which is "nqg_vfusr_ec_wawy" we gussed it should be the password as it have underscore. Based on previous plainetext we know that there should be a word "password" which will indicate that "nqg_vfusr_ec_wawy" is the password (known plaintext attack). We found keyword "lhvqpawr" just before "nqg_vfusr_ec_wawy" which have 8 letters. No other keyword have 8 letters close to "nqg_vfusr_ec_wawy". So keyword "lhvqpawr" has to be the password.
In "password" there should be "ss", so in place of "vq" there should be two same letters in keyword "lhvqpawr".

As the permutation key length was 5, we divided the cipher text in blocks of 5. And we located the block where "ss" should be. That block was "llhvq". As in this block "l" is two time this justify that our assumption and it is clear from here that "l" is mapped to "s".
From above we know that in place of "vq" there should be "ll", this reduce the possible no. of keys from 120 to 12. We also observed that there are single letter word "y" and "x" are used in cipher text these word could be either "a" or "i". As all the text used in the escaping the caves are in a story telling manner in which "i" can not come, so in place letter "x" and "y" there should be same letter "a". "y" is in "pqcsy" and "x" is in "quwxd" block and these should map to same letter and there is only "q" which is present in both. so we put 2 more conditions and reduced our possible no. of keys from 12 to 2.
possible keys:(1,2,3,4,5)-> (4, 5, 2, 1, 3) and (1,2,3,4,5)->(4, 5, 1, 3, 2)

Then we find two intermediate text after decrypting the permutation. And for these two text we did the frequency analysis and found the plaintext which made sense (just like we did in assignment 1). one made sense and other not. that how we finally get the password.

Permutation key:
(1,2,3,4,5)-> (4, 5, 2, 1, 3)

intermediate text after decrypting permutation:
JVNQM VWNSA FLCEW PRVCT TVJJT VLLVP JAXFV LDIVQ MLXHC NACNV LPCCY GYCAF VWFTV GQWFV QQPYP SYCPQ RXQWS JVNQM CGYAF VHLVT TYWFC UQELA JAXFV VCBTK QSSQN AVFLH

CCNAW SFAVE QVBUQ YLCQT RXQLR CFAXW DCSYP AVFUQ GECRQ YAPFQ ACRTT TAVXW
DDWAW SFAVE QVBLC AWRDT PQUMV XDWQU QCGEC QYYWT VLLAF QKYQS SNQLH VMQAF
VQHLL RNWPA FUVQG CWESR QPYAW GAWFN FXGWD

Substitution Map:
Ciphertext space: <abcdefghijklmnopqrstuvwxyz,._! >
Plaintext space: <tviuchgpqbzskrjdawflmeoynx,._! >

plaintext:
"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 zaffar. 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 zaffar! speak the password the_magic_of_wand to go thrhgyo."

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.

No files uploaded

Q6 Group name
0 Points

team_9

Assignment 3

● Graded