Q1 Commands
5 Points

List the commands was used in this level?

go, enter, pluck, c, c, back, give, back, back, thrnxxtzy, read

Q2 Cryptosystem
10 Points

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

Substitution(Mono Alphabetic) and Permutation(Transposition) Cipher - SPN of block length 5.

Mono-Alphabetic Substitution mapping:
Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ciphertext: Q J E P V S G F C K M T U Y W H I N L A D B R % X %

Permutation(Transposition) Cipher keys:
Encryption : 12345 -> 45213
Decryption : 12345 -> 43512

Q3 Analysis
30 Points

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

Necessary Data to solve:

Given 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.

These are the results of frequency analysis on the cipher-text we got from (https://math.dartmouth.edu/~awilson/tools/frequency_analysis.html)

Q	V	A	C	F	W	L	T	Y	P	S	N	R	G	X	D	E	J	U	H	M
10%	10%	8%	7%	6%	6%	5%	4%	4%	3%	3%	3%	3%	2%	2%	2%	2%	2%	2%	1%	1%

B	K	I	O	Z
1%	0%	0%	0%	0%

These are the frequencies of english alphabet over texts (from Wikipedia)

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G
13%	9.1%	8.2%	7.5%	7%	6.7%	6.3%	6.1%	6%	4.3%	4%	2.8%	2.8%	2.4%	2.4%	2.2%	2%

Y	P	B	V	K	J	X	Q	Z
2%	1.9%	1.5%	0.98%	0.77%	0.15%	0.15%	0.095%	0.074%

Note: Format is Plaintext:Ciphertext for mapping.

Approach and Analysis:

The guessed plaintext is 'the password' for the ciphertext 'vml lhvqpawr'. but this doesn't give direct mappings for substitution. We tried using frequency analysis and meaningful substitutions, but couldn't make sense.

so its not a simple mono substitution cipher, but the distribution frequency analysis is similar to the normal english text, which means letters frequency's order is nearly same, that is simple substitution happened and along with that we suspected that a Permutation cipher was also used, so that the order has changed and so we couldn't break it using simple substitution cipher and frequency analysis.

Our approach to solve this assignment is to solve this SPN cipher using guessed plaintext to get the permutation key and length, while decryption and encryption backed by frequency analysis and then make substitutions which make sense by also using frequency analysis.

The Ciphertext is of 284 characters of english alphabet, to find the possible block size used in this cipher, we find factors of 284, which are 2, 4, 71, 142, 2 is least secure, and 71, 142 are impractical, proceed with block size 4, but from the 4grams of ciphertext didn't help with the guessed plaintext. so now we move on to the next block size 5.

For the guessed plaintext the 5gram ciphertext is as this
AFQVM LLHVQ PAWRN - Cipher
 ???TH EPASS WORD? - Plain

LLHVQ : EPASS
from this 5gram pair, for the 'ss' in plaintext we have 'll' in ciphertext i.e. we got a mapping of 'S:L'
and for now the permutation key for decryption can be ???12 or ???21, from the 'ss' and 'll'.

To find whether permutation key is ???12 or ???21, take this 5gram pair.
PAWRN : WORD?
here mapping can be D:P or D:A for permutation key ???12

and ???21 respectively.
now we use frequency analysis to choose one of these substitutions.
frequency of D in english is 4.3%, frequency of P in Ciphertext is 3% and frequency of A in Ciphertext is 8.2%, we choose the one with the same or near neighborhood frequency and makes meaningful substitutions, i.e. we choose the Permutation to be XXX12 and got the mapping 'D:P'.

Now we can make some other mappings from AFQVM : ???TH from the Permutation key ???12, the mapping found are, T:A and H:F, as we got the mapping T:A in PAWRN : WORD?, we get that '?' in plain text is 'T', i.e. PAWRN : WORDT

and now the next word to 'password' is a three letter word starting with T i.e. for "lhvqpawr nqg" in ciphertext, we thought it to be 'The', which is also a part of the password to clear this level.
so now for this guess the 5gram ciphertext is as this
PAWRN QGVFU - Cipher
WORDT HE??? - Plain
As for now the Permutation key is ???12, so we cant map H and E in guessed plaintext with Q and G in ciphertext, can map with any of V, U. Now we will find ideal mapping for E using frequency analysis.
Frequency of E in english is 13% and
Frequency of V, U in Ciphertext is 10%, 2% respectively, so we mapped 'E:V', as we have mapped successfully, now we can talk about the permutation key also, from the mappings 'E:V' and 'H:F' we can conclude that Permutation Decryption Key is 43?12 which is obviously 43512.

The Permutation key while Decryption is 12345 -> 43512 and by finding inverse, the Permutation key while Encryption is 12345 -> 45213.

and the mappings we got till now from our guess plaintext and frequency analysis are S:L, D:P, T:A, H:F, E:V.

Now we had De-Permuted the Cipher text(decryption) with Permutation key of 43512. and their 5grams are given below

5grams of Cipher-text:
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

5grams of De-Permuted (with decryption key: 4,3,5,1,2) cipher-text:
JNVQM VNWSA FCLEW PVRCT TJVJT VLLVP JXAFV LIDVQ
MXLHC NCANV LCPCY GCYAF VFWTV GWQFV QPQYP SCYPQ
RQXWS JNVQM CYGAF VLHVT TWYFC UEQLA JXAFV VBCTK
QSSQN AFVLH CNCAW SAFVE QBVUQ YCLQT RQXLR CAFXW
DSCYP AFVUQ GCERQ YPAFQ ARCTT TVAXW DWDAW SAFVE
QBVLC ARWDT PUQMV XWDQU QGCEC QYYWT VLLAF
QYKQS SQNLH VQMAF VHQLL RWNPA FVUQG CEWSR
QYPAW GWAFN WDGF

This De-Permuted Cipher text which now can be a ciphertext from a mono substitution cipher.
Now its equal to as the first assignment which was solved using frequency analysis and meaningful substitution.

In the De-permuted ciphertext the 5grams corresponding to the guessed text
"THE PASSWORD THE" is "VQMAF VHQLL RWNPA FVUQG"
???TH EPASS WORDT HE???
using this we can find mapping for remaining letters in guessed plaintext, they are 'P:H', 'A:Q', 'W:R', 'O:W', 'R:N'.

Now we have 10 mappings of Plaintext to Ciphertext they are S:L, D:P, T:A, H:F, E:V, P:H, A:Q, W:R, O:W, R:N.

Now the De-Permuted ciphertext with spacing as in cipher text is passed to a substitution cipher implementation tool on online (https://math.dartmouth.edu/~awilson/tools/frequency_analysis.html)

Partial decrypted plain text
Result at this stage is like this
(Upper case is Cipher, Lower case is Plain)

JreaMer oS thCs Eode wCTT Je JTessed JX the sIDeaMX spCrCt resCdCYG CY the hoTe Go ahead aYd SCYd a waX oS JreaMCYG the speTT oY hCU East JX the eBCT KaSSar the spCrCt oS the EaBe UaY Cs aTwaXs wCth XoD SCYd the UaGCE waYd that wCTT Tet XoD oDt oS the EaBes Ct woDTd UaMe XoD a UaGCECaY Yo Tess thaY KaSSar speaM the password the_UaGCE_oS_waYd to Go throDGh.

from this we look for most probable words to make our mapping procedure easier like
(I will choose these mappings only when it makes sense and doesn't collide with other previous mappings)
'thCs' can be 'this', so mapping 'I:C'.
'Eode' can be 'code', so mapping 'C:E'.
'Je' can be 'be', so mapping 'B:J'.
'hoTe' can be 'hole', so mapping 'L:T', also from 'Tess' ->'less'.
'speaM' can be 'speak', so mapping 'K:M'.
'aYd' can be 'and', so mapping 'N:Y'.
'aTwaXs' -> using L:T-> 'alwaXs' can be 'always', so mapping 'Y:X'.

These probable guesses were made by replacing the cipher with plain every time we get a new mapping so that the guessing gets easier on substitution by substitution.

at this moment of time the substitution mappings we have(are 17) and our partial decrypted plain text is
S:L, D:P, T:A, H:F, E:V, P:H, A:Q, W:R, O:W, R:N, I:C, C:E, B:J,

L:T, K:M, N:Y, Y:X.

Result at this stage is like this
(Upper case is Cipher, Lower case is Plain)

breaker oS this code will be blessed by the sIDeaky
spirit residinG in the hole Go ahead and Sind away
oS breakinG the spell on hiU cast by the eBil KaSSar
the spirit oS the caBe Uan is always with yoD Sind the
UaGic wand that will let yoD oDt oS the caBes it woDld
Uake yoD a UaGician no less than KaSSar speak the
password the UaGic oS wand to Go thr oDGh

'yoD' can be 'you', so mapping 'U:D'.
in 'breaker oS this code', 'oS' can only be 'of', so mapping 'F:S'.
from 'eBil', 'caBe', 'caBes' can be 'evil', 'cave', 'caves', so mapping 'V:B'.
For 'residinG', 'breakinG' the 'G' makes sense with out getting the need of substitution, so mapping 'G:G'.
Now 'hiU', 'cave Uan', 'Uagic wand', 'Uagician' can be 'him', 'cave man', 'magic wand', 'magician', so mapping 'M:U'.
for 'sIDeaky' -> 'sIueaky', alphabets remaining are J,Q,X,Z., only 'squeaky' makes sense,
so mapping 'Q:I'
for 'Kaffar' alphabets remaining are J,X,Z., 'Jaffar' makes sense(name of the villian in Alladin).
so mapping 'J:K'

Mappings found till now are(24), they are
S:L, D:P, T:A, H:F, E:V, P:H, A:Q, W:R, O:W, R:N, I:C, C:E, B:J, L:T, K:M, N:Y, Y:X, U:D, F:S, V:B, G:G, M:U, Q:I, J:K.

with these many substitutions our ciphertext has been decrypted to pure plain text as given below and mapping for O and Z of Ciphertext are not there so definite mapping cant be made,
so mapping can be {X,Z}:{O,Z} i.e., mapping of either X:O and Z:Z (or - '%') X:Z and Z:O is possible for those.

Mono-Alphabetic Substitution mapping:
Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ciphertext: Q J E P V S G F C K M T U Y W H I N L A D B R % X %

Plain-text (using the above discussed mapping):
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 CAVEMAN 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 PASS WORD T HE_MAGIC_OF_WAND TO GO THROUGH.

Point to note: The last block i.e. letter numbers 281 to 284 were not permuted but only substituted WDGF -> OUGH, i.e. this assignment can also be solved by using only first 280 letters of cipher text, then factors of 280 can be 1, 2, 4, 5, 7, 8, 10, 14, 20, 28, 35, 40, 56, 70, 140, and 280.
so having a block size 5 makes sense now from the way the plaintext was encrypted by you in first place.

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

Cryptosenpai

Assignment 3

● Graded

Group

Rumit Pingleshwar Gore
Kuruma Abhinav
VAMSEE KRISHNA KAKUMANU
View or edit group

Total Points

45 / 50 pts

Question 1 Commands	**5** / 5 pts
Question 2 Cryptosystem	**10** / 10 pts
Question 3 Analysis	**25** / 30 pts
Question 4 Password	**5** / 5 pts
Question 5 Codes	**0** / 0 pts
Question 6 Group name	**0** / 0 pts