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?

In the game, a cryptosystem was used to reach the password which involved both substitution (mono-alphabetic) and permutation (transposition) ciphers.

1) Mono-Alphabetic Substitution mapping
The plaintext letters :
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
mapped to the ciphertext letters :
Q J E P V S G F C K M T U Y W H I N L A D B R * X *.

2) Permutation(Transposition) Cipher
In addition to substitution, a permutation cipher was also used, which rearranged the order of the ciphertext letters. Specifically, a transposition cipher using a block length of 5 was used. The encryption key for the transposition cipher was 12345, which means that the ciphertext was split into blocks of 5 letters, and the order of the letters in each block was rearranged according to the key 45213. The decryption key was also 12345, but with a different permutation, namely 43512.

Overall, the combination of substitution and permutation ciphers was used to protect the password in the game.

Q3 Analysis

30 Points

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

Ciphertext given :
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.

First of all we tried to do frequency analysis on the given ciphertext to check if it is normal substitution cipher.

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

These are the results of our frequency analysis.

Approach :

We compared these results with the frequency analysis of the English language done on a large corpus. We got the mappings for each letter by this method.
Our guessed plaintext was 'the password', so for checking the validity of our mappings we checked to substitute this word but our ciphertext was not matching the ciphertext we got from frequency analysis.
So, we came to the conclusion that this is not just a substitution cypher. There is some other cypher used here.

And also there were some words in ciphertext such as 'xxwa' which is not possible in the English language to have to letters in front common. So, we concluded that there was some kind of permutation also used in this cipher. That is how we guessed that the cipher used here is SPN network i.e. substitution and permutation cipher.

The given ciphertext consists of 284 characters from the English alphabet. To determine the likely block size used in the encryption, we need to identify the factors of 284. These factors include 2, 4, 71, and 142. Given that 2 is the least secure, and 71 and 142 are not practical, we proceeded with a block size of 4. However, analyzing the 4-grams of the ciphertext did not yield any useful information for guessing the plaintext. Therefore, we moved on to the next block size of 5.

So, checking 5-grams for guessed plaintext is :
cipher text : AFQVM LLHVQ PAWRN
plain text : **TH EPASS WORD*
where '*' symbol suggest that the letter is not known at that place.

Given the 5-gram pair "LLHVQ: EPASS", we can deduce that the plaintext letter "s" corresponds to the ciphertext letter "l" since the substring "ss" appears in the plaintext and maps to "ll" in the ciphertext. We can use this mapping to derive the permutation key for decryption, which could be either "***12" or "***21" based on the relative positions of the "s" and "l" in the 5-gram pair.

For PAWRN: WORD*, mapping can be either D:P or D: A depending on the permutation key we used either ***21 or ***12.
Using the frequency analysis, we preferred D:P mapping over D: A as A comes very frequently like 8% compared D, P which comes to around 4% in English.

From the 5-gram pair "AFQVM: ***TH" and the permutation key "***12", we can establish that "T" maps to "A" and "H" maps to "F". We also have the mapping "T: A" from the 5-gram pair "PAWRN: WORD?", which enables us to determine that the unknown character "*" in the ciphertext corresponds to "T" in the plaintext. As a result, we can decrypt the ciphertext "PAWRN: WORD?" to "PAWRN: WORDT".

The next word in the password consists of three letters and starts with "T". We find the corresponding ciphertext "lhvqpawr nqg" and consider that it may decrypt to "The". After decryption, we confirm that "The" is indeed a part of the password required to clear this level.

The 5-gram pair "PAWRN QGVFU" corresponds to the ciphertext, and "WORDT HE***" corresponds to the plain text. Given the current permutation key "***12", we are unable to map the plaintext letters "H" and "E" to the ciphertext letters "Q" and "G", respectively. However, we can map them to either "V" or "U" in the ciphertext. To determine the ideal mapping for "E", we perform a frequency analysis.

The frequency of "E" in the English language is 13%, while the frequencies of "V" and "U" in the ciphertext are 10% and 2%, respectively. Based on this information, we can map "E" to "V". With this successful mapping, we can also determine the permutation decryption key, which is "43*12" where "E: V" and "H: F". This key decrypts to "43512". We can also find the corresponding encryption permutation key, which is "12345" -> "45213" by finding the inverse of the decryption key.

The mappings we have deduced from our guessed plaintext and frequency analysis are :

{"S:L", "D:P", "T: A", "H:F", and "E:V"}

We have successfully de-permuted the ciphertext using the permutation key "43512", and the resulting 5-gram pairs are provided 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 ciphertext:

```
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
```

The De-Permuted Cipher text can be a ciphertext from a mono substitution cipher, which is the same type of cipher used in the first assignment which was solved using frequency analysis and substitution. By identifying the 5grams that correspond to the guessed text "THE PASSWORD THE" as "VQMAF VHQLL RWNPA FVUQG", we can deduce mappings for the remaining letters in the guessed plaintext, such as :
{'P: H', 'A: Q', 'W: R', 'O: W', 'R: N'}
In total, we now have 10 mappings of plaintext to ciphertext :
{ H: F, E: V, P: H, A: Q, W: R, O: W, R: N, D:P, S:L, T: A.}

Partial decrypted plain text:
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.

The given text is partially decrypted, where uppercase letters represent the cipher and lowercase letters represent the plain text. To make the decryption process easier, we can look for the most probable words and their mappings. For example, "thCs" can be "this", so we can map "I" to "C". Similarly, "Eode" can be "code", so we can map "C" to "E". We continue this process for other words such as "hoTe" being "hole", "Tess" being "less", "speaM" being "speak", and "aYd" being "and".

We can also look for longer words or phrases that make sense and help us make additional mappings. For example, "aTwaXs" can be "always" when we substitute "L" for "T", so we can map "Y" to "X". We continue this process until we have 17 mappings.

After applying these mappings, we can see that some words such as "breaker oS this code" can only be "breaker of this code", so we can map "F" to "S". We also notice that "caBe" can be "cave", "eBil" can be "evil", and "caBes" can be "caves", so we can map "V" to "B". We can also make other mappings such as "cave Uan" being "cave man", "Uagic wand" being "magic wand", "hiU" being "him" and "Uagician" being "magician".

We also notice that "sIDeaky" can be "squeaky" after mapping "Q" to "I", and "Kaffar" can be "Jaffar" after mapping "J" to "K". After making all these mappings, we have successfully decrypted the ciphertext into plain text. The final mappings include 24 substitutions they are, {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, H:F, E:V, J:K, S:L, D:P, S:L, T:A} and some mappings such as "O" and "Z" are not definite, so we can map either "X" to "O" and "Z" to "Z" or "X" to "Z" and "Z" to "O".

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 mapping found so far):
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.

It's worth noting that the last four characters of the cipher text were not permuted, but only substituted with "OUGH" in place of "WDGF". As a result, it's possible to solve the code using only the first 280 characters. The possible block sizes are 1, 2, 4, 5, 7, 8, 10, 14, 20, 28, 35, 40, 56, 70, 140, and 280. The fact that the plaintext was originally encrypted with a block size of 5 is now evident.

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

the_boys

Assignment 3

● Graded

Group

PRATIK MAHIPAL PATIL
SANKET SANJAY KALE
ADITYA SUNILKUMAR KANKRIYA
✎ 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