Q1 Commands
5 Points

List the commands was used in this level?

enter, enter, pick, back, put, back,
give, back, back, thrnxxtzy, read

Q2 Cryptosystem
10 Points

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

Substitution-Permutation Network (1 Round)

Q3 Analysis
30 Points

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

Tools:
1) Used C++ program to divide the ciphertext in the blocks of 5 letters.
2) Used C++ program to permute the ciphertext as per the mapping which is mentioned below.
3) Used 'dcode.fr' to get the index of coincidence of ciphertext.

Observations:
1) We found index of coincidence of the ciphertext to be 0.05728, which is close to monoalphabetic substitution cipher. So we started with monoalphabetic substitution cipher but we found a word 'wwd'. There are no such 3 lettered meaningful words in English vocabulary which start with two same letters. So we came to conclusion that definitely it's not entirely substitution cipher. So

it could be Substitution-Permutation Network.

2) We found length of ciphertext to be 284. So the block size could be either 2 or 4. We first tried with block size 2 but the new ciphertext too didn't make much sense. Then we tried with block size 4 but again new ciphertext didn't make any sense. So what we did was we padded one letter '*' at the end of ciphertext so that length of ciphertext is 285 now and then we assumed block size of 5.

3) We divided ciphertext into blocks of 5 using 'divide.cpp' (which is included here). So ciphertext now looks like as follows:

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*

3) Now we observed the ciphertext and found that last sentence is most probably containing the password. The first 3 words of last sentence which is "snafq vml lhvqpawr" seems most likely to be "enter/speak the password". Above words on divided with block of 5 looks like:

lhqsn afqvm llhvq pawrn
** ***th epass word*

4) The second last block above is having a common letter 'l' in the ciphertext and 's' in corresponding plaintext. This gives us mapping from 'l' to 's' and permutation for decryption to encryption is (1, 2, 3, 4, 5) -> (*, *, *, 1, 2).

5) We observed the first block and found that it is

containing 'l' which is mapped to 's' and hence we concluded that the first letter in corresponding plaintext is 'speak', not 'enter'.

lhqsn afqvm llhvq pawrn

sp eakth epass word*

6) From here we found that 'h' is mapping to 'p', so in block 'llhvq', h should be mapped to 'p' hence we found a new permutation for decryption to encryption to be (1, 2, 3, 4, 5) -> (*, 3, *, 1, 2).

7) In blocks 'afqvm' and 'llhvq', we found that 'v' is common between them and both mapped to 'e' in the corresponding plaintext block. So from here we get permutation as (1, 2, 3, 4, 5) -> (4, 3, 5, 1, 2).

8) So now using 'permute.cpp', we transformed the entire blocks of ciphertext using above mapping and hence new ciphertext after permutation looks like:

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 fg*wd

9) Now we have to do substitution for that reason we convert these 5 blocks into our original cipher text form so we include all punctuation marks and space. So now ciphertext look like:

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 afnfg*wd

10) From permutation (1,2,3,4,5)->(4,3,5,1,2), we found some mapping like
L->S, A->T, F->H, H->P, W->O, P->D, V->E, Q->A, R->W, N->R, M->K

11) Here we didn't do frequency analysis because we have enough number of mapping to see some meaningful words.

12) After replacing L,A,F to their corresponding mapped letter, ciphertext look like,
jnvqmvn ws thcs ewpv rctt jv jtvssvp jx thv sidvqmx
shcnct nvscpcyg cy thv hwtv. gw qhvqp, qyp scyp q rqx
ws jnvqmcyg thv shvtt wy hcu eqst jx thv vbct kqssqn.
thv shcnct ws thv eqbv uqy cs qtrqxs rcth xwd.
scyp thv
uqgce rqyp thqt rctt tvt xwd wdt ws thv eqbvs.
ct rwdtp
uqmv xwd q uqgcecqy, yw tvss thqy kqssqn!
shvqm thv
hqssrwnp thv_uqgce_ws_rqyp tw gw thnhg*wd

13) After replacing H,W,P to their corresponding mapped letter, ciphertext look like,
jnvqmvn os thcs eodv rctt jv jtvssvd jx thv sidvqmx
spcnct nvscdcyg cy thv hotv. go qhvqd, qyd scyd q rqx
os jnvqmcyg thv spvtt oy hcu eqst jx thv vbct kqssqn.
thv spcnct os thv eqbv uqy cs qtrqxs rcth xod.
scyd thv

uqgce rqyd thqt rctt tvt xod odt os thv eqbvs. ct rodtd
uqmv xod q uqgcecqy, yo tvss thqy kqssqn! spvqm thv
pqssrond thv_uqgce_os_rqyd to go thnhg*od

14) After replacing V,Q,R to their corresponding mapped letter ciphertext look like,
jneamen os thcs eode wctt je jtessed jx the sideamx
spcnct nescdcyg cy the hote. go ahead, ayd scyd a wax
os jneamcyg the spett oy hcu east jx the ebct kassan.
the spcnct 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 kassan! speam the
passwond the_uagce_os_wayd to go thnhg*od

15) After replacing N,M to their corresponding letter ciphertext look like,
jreaker os thcs eode wctt je jtessed jx the sideakx
spcrct rescdcyg cy the hote. go ahead, ayd scyd a wax
os jreakcyg 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
uake xod a uagcecay, yo tess thay kassar! speak the
password the_uagce_os_wayd to go thrhg*od
16) From word ‘thcs’ we can guess it is ‘this’ so we replace ‘C’ with ‘I’. From word ‘eode’ we can guess it is ‘code’ so we replace ‘E’ with ‘C’. So now Ciphertext look like :
jreaker os this code witt je jtessed jx the

sideakx
spirit residiyg iy the hote. go ahead, ayd siyd a wax
os jreakiyg the spett oy hiu cast jx the ebit kassar.
the spirit os the cabe uay is atwaxs with xod. siyd the
uagic wayd that witt tet xod odt os the cabes. it wodtd
uake xod a uagiciay, yo tess thay kassar! speak the
password the_uagic_os_wayd to go thrhg*od

17) From word ‘witt’ we can guess it is ‘will’ so we replace ‘T’ with ‘L’
From word ‘je’ we can guess it is ‘be’ so we replace ‘J’ with ‘B’. Now Cipher text look like :
breaker os this code will be blessed bx the sideakx
spirit residiyg iy the hole. go ahead, ayd siyd a wax
os breakiyg the spell oy hiu cast bx the ebil kassar.
the spirit os the cabe uay is alwaxs with xod. siyd the
uagic wayd that will let xod odt os the cabes. it wodld
uake xod a uagiciay, yo less thay kassar! speak the
password the_uagic_os_wayd to go thrhg*od

18) From word ‘bx’ we can guess it is ‘by’ so we replace ‘X’ with ‘Y’. Similarly from word ‘wodld’ we can guess it is ‘would’ so we replace ‘D’ with ‘U'. Now Cipher text look like :
breaker os this code will be blessed by the siueaky
spirit residiyg iy the hole. go ahead, ayd siyd a way
os breakiyg the spell oy hiu cast by the ebil kassar.
the spirit os the cabe uay is always with you.

siyd the
uagic wayd that will let you out os the cabes. it would
uake you a uagiciay, yo less thay kassar! speak the
password the_uagic_os_wayd to go thrhg*ou

19) From word ‘os’ we can guess it is ‘of’ so we replace ‘S’ with ‘F’. From word ‘breakiyg’ we can guess it is ‘breaking ’ so we replace ‘Y’ with ‘N’. From word ‘uagic’ we can guess it is ‘magic’ so we replace ‘U’ with ‘M’. Now Ciphertext look like :
breaker of this code will be blessed by the siueaky
spirit residing in the hole. go ahead, and find a way
of breaking the spell on him cast by the ebil kaffar.
the spirit of the cabe man is always with you. find the
magic wand that will let you out of the cabes. it would
make you a magician, no less than kaffar! speak the
password the_magic_of_wand to go thrhg*ou

20) From word ‘cabe’ we can guess it is ‘cave’ so we replace ‘B’ with ‘V’. Now Cipher text look like :
breaker of this code will be blessed by the siueaky
spirit residing in the hole. go ahead, and find a way
of breaking the spell on him cast by the evil kaffar.
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 kaffar! speak the
password the_magic_of_wand to go thrhg*ou

21) From word ‘siueaky’ we can guess it is ‘squekly’ so we replace ‘I’ with ‘Q’
Now k is remaing so it might be J because J,X,Z is remaining to be mapped so for ‘K’ we get meaningful latter J because word ‘kaffar’ become ‘jaffar’ so we replace ‘K’ with ‘J’.
And last word ‘thrhg*ou’ we can guess it is through.
So our final decrypted text look like:

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

22) So the password we get is 'the_magic_of_wand'.

23) The mapping used for breaking simple substitution cipher after we get correct permuted ciphertext is as follows:
A -> T
B -> V
C -> I
D -> U
E -> C
F -> H
G -> G
H -> P
I -> Q
J -> B
K -> J
L -> S
M -> K
N -> R
O -> $

P -> D
Q -> A
R -> W
S -> F
T -> L
U -> M
V -> E
W -> O
X -> Y
Y -> N
Z -> $
'.' -> '.'
',' -> ','
'!' -> '!'
'_' -> '_'

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.

divide.cpp Download

permute.cpp Download

Q6 Group name
0 Points

crypt_elite

Assignment 3

● Graded

Group
SHRAWAN KUMAR
KAPILKUMAR KISHORBHAI KATHIRIYA
HARIS KHAN
View or edit group

Total Points
47 / 50 pts

Question 1 Commands	5 / 5 pts
Question 2 Cryptosystem	10 / 10 pts
Question 3 Analysis	27 / 30 pts
Question 4 Password	5 / 5 pts
Question 5 Codes	0 / 0 pts
Question 6 Group name	0 / 0 pts