Q1 Commands

5 Points

List the commands used in the game to reach the first ciphertext.

```
climb
read
enter
read
```

Q2 Cryptosystem

5 Points

What cryptosystem was used at this level?

Substitution cipher

Q3 Analysis

25 Points

What tools and observations were used to figure out the cryptosystem?

NOTE: Failing to provide proper analysis would result in zero marks for this assignment.

I first observed that the last line (Mey fpaavgsu wa "...") could be decoded as (The password is "..."). The aa's in fpaavgsu and double quotes gave me the idea that it has to be password. This implied that 'Me' is 'Th' and 'Mewa' is 'This' so the first line becomes 'This is the'. Also there is a lone 'p' in 6th line which means it has to be 'a'. We get the following ciphertext to plaintext decoding using this analogy:-

m -> t
e -> h

y -> e
w -> i
a -> s
p -> a
Substituting these and decoding words line by line as per the current context we are able to guess more words like twsam -> first, iepjoys -> chamber, ipbya -> caves, etc. Words like 'ayy' could be either 'too' or 'see' as they have 2 repeating letters in the end. A simple logical guess could tell it has to be 'see'.
Overall doing such substitution for every work we get the following message:-
"This is the first chamber of the caves. As you can see there is nothing of interest in the chamber. Some of the later chambers will be more interesting than this one! The code used for this message is a simple substitution cipher in which digits have been shifted by 4 places. The password is "tyRgU69diqq" without the quotes."
The 4 instead of 8 was found as a result of trial and error.
There are still letters whose substitution aren't available in the given substitution cipher.

Q4 Mapping

10 Points

What is the plaintext space and ciphertext space?
What is the mapping between the elements of plaintext space and the elements of ciphertext space? (Explain in less than 100 words)

Any readable data which can be read and utilized without the need of a decryption key is called plaintext space. The decoded message (written in the above answer) is the plaintext space for this level. Ciphertext spaces are data which can't be directly read or utilized and needs to be decoded first (usually by using some form of decryption key). The text we reach after typing the commands climb, read, enter read is encoded and illegible. This is the ciphertext space.
Mapping: Plaintext -> Ciphertext (substituting ciphertext to plaintext will decode the message).

a -> p
b -> o
c -> i
d -> u
e -> y
f -> t
g -> r
h -> e
i -> w
j ->
k ->
l -> k
m -> j
n -> h
o -> g
p -> f
q -> d
r -> s
s -> a
t -> m
u -> n
v -> b
w -> v
x ->
y -> x
z ->
j, k, x and z are the 4 remaining letters from plaintext which don't require any substitution as they do not occur in plaintext.

Q5 Password

5 Points

What is the final command used to clear this level?

tyRgU69diqq

Q6 Codes

0 Points

Upload any code that you have used to solve this level

No files uploaded

Q7 Team Name

0 Points

team_7

Assignment 1

● Graded

Group

HARSH SAROHA
RASHMI BHIKAJI WAGHMARE
CHANDEKAR VIDISH VIJAY

View or edit group

Total Points

33 / 50 pts

Question 1 Commands	**5** / 5 pts
Question 2 Cryptosystem	**3** / 5 pts
Question 3 Analysis	**17** / 25 pts
Question 4 Mapping	**3** / 10 pts
Question 5 Password	**5** / 5 pts

Question 6

Codes **0** / 0 pts

Question 7

Team Name **0** / 0 pts