(Team details can be found at the end of the assignment)

Cipher Method: Transposition + Substitution Cipher

Passcode: ttd_qinmc_li

Justification:

- i. At the first screen we notice there is another chamber there, thus **enter** was the command.
- ii. On the next screen, we see a large and a small hole where something is shiny in the later. Thus, we use *put* command and someone bites our hand. So, we use *back*.
- iii. To go inside large hole, we use **enter** and there we find smelly mushrooms.
- iv. After a lot of tries we figured out that we should be picking these mushrooms and give to someone, otherwise no point of this screen. So, we use *pick* as the command and go *back*.
- v. We reach the previous screen and use *give* command and it takes us to a new screen where we find magic words from the main chamber: *thrnxxtzy*
- vi. On entering these from the main chamber, we get another screen which says there is a glass panel there. So, the command is *read*.
- vii. We see a cipher text which has hardly some repeating words, but still we do the frequency analysis and find that gives us following results:

Letter	Occurrence	Percentage
K	28×	10.04%
0	28×	10.04%
Е	24×	8.6%
W	23×	8.24%

- viii. So, **Substitution** is present but when we tried to work it out it didn't make sense. Thus, it's not **Monoalphabetic Substitution**. So, we calculated frequencies of bigrams and trigrams which turned out to be very low (Maximum was 2%).
 - ix. Thus, there has to be *Transposition* present.
 - x. We then removed all non-alphabetic characters and calculated length of the whole text (excluding password) which worked out to

- be 270. Also, the password is of length 10. So, the block has to be of either 2, 5 or 10 lengths. Block size of 2 didn't make sense, so we went with size 10.
- xi. Then we thought that if keys are English words then it can't end with 2 letter word. Thus, we tried word combinations of 3_2_5 and 2_3_5 but couldn't figure out anything.
- xii. Now, judging by the statement formation, last word before password was of 8 letters with a colon so it should be 'password'.
- xiii. Also, there were two two-letter words at the beginning followed by a 7 letters word, where first two words can be one of the 'go to', 'to go', 'if by' or 'to be' but as they were followed by a 7 letters word, only 'go to' made sense followed by 'through' which is a 7 letters word.
- xiv. So, we guessed the whole sentence as:
 Cipher Text: 're re ncygnrx, ykoje akj yxoprxbc'

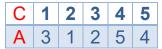
 Expected Text: 'To go through, enter the password'
- xv. With 10 letters blocks, in the last block frequency of \boldsymbol{x} in the cipher text block was $\boldsymbol{2}$ and in expected text only frequency of \boldsymbol{s} was $\boldsymbol{2}$. So, \boldsymbol{x} has to be mapped to \boldsymbol{s} . Going by numbering, position $\boldsymbol{4}$ maps to $\boldsymbol{5}$. But that wasn't the case in penultimate block. As, \boldsymbol{x} was being mapped to \boldsymbol{e} .
- xvi. So, instead of 'enter' we tried 'speak' and now the sentence became:Expected Text: 'To go through, SPEAK the password'
- xvii. Now, **x** is mapped to **s** even in the penultimate block thus the mapping was correct.
- xviii. Now, we kept on repeating the same process by using the discovered *transposition key mappings* along with *substitution mappings* as an when we discovered the same.
- xix. Following is the *transposition key mapping*:

 C Cipher Position, A Actual Position

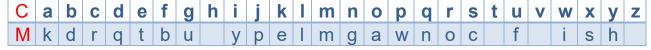
 C | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

A 3 1 2 5 4 8 6 7 10 9

- xx. As we can see the mapping repeats after position 5. Thus, *the block size is 5* and the mapping becomes:
 - C Cipher Position, A Actual Position



- xxi. The substitution mappings we found is as follows:
 - C Cipher Alphabet, M Mapped Alphabet



xxii. Now, using transposition key and the substitution key, the deciphered password becomes:

ttd_qinmc_li

Team Details:

- Ashish Pal (18111010)
- Darshit Vakil (18111013)
- o Mayank Rawat (18111040)