
CS641: THE GREAT CAVES

DEDSEC

Guntas Singh Brar
180274

Divyanshu Bhardwaj
180253

Devanshu Gupta
180233

January 30, 2020

Chapter 3 :The Holes

Reaching the Cipher Text

- We enter the third chamber. We use "go" and enter another chamber with rumbling sounds, having a small hole and a small entrance.
- We try to explore the small hole using "put" and someone bites our hand as we put it in the hole.
- We go "back" and try to explore the small entrance by typing in "enter".
- We reach a chamber. The rumbling sound is very loud here and its very sticky and smelly too. There are mushrooms on the ground. So we use "pick" and a message is displayed saying "You plucked some smelly mushrooms"
- We think of giving these mushrooms to the creature in the hole who bit us. We go "back" and type in "give". The creature eats the mushrooms and we hear a squeaky voice from the hole saying:

"Oh, thank you very much for the mushrooms! I have been hungry for so long!! I am a poor spirit trapped inside this hole by an evil man. Maybe you can help me be free ... (sigh) oh, forget it. I'll help you pass this chamber though. Note down and speak out the magic words "thrnxtzy" for the hidden door to become visible. The door lies hidden in the main chamber."

- So we go back to the main chamber and type in the magic words "thrnxtzy". A door and a glass panel appear at the front wall.
- We "read" the message on the panel that goes:

"frcpsr dy nkao lyxs autt ff stslsx fm kns lgsecpm zlarar nsiaaxqv an qks ktys. vy kcscx, qcx daxq cucy md frcspaqn vks lszt yk qab olcn fm kns swta icdedr. nkl szarna yd nsk ocwb seq ac ltuelm uanm kye. dqax nkb scvau ocqx knen utat tsm nye yne yd nsk ocwls. an ueytx bpes myc e bcvoaacq, yq tsln lkeq cidden! ry vy knryekv, lzpc nks czlluryx:"

aap_niviv_dr

Cracking The Cipher Text

- We firstly calculated the Index of Coincidence of the cipher text. It came out to be around 0.057 which is very close to that of English text(around 0.066). This indicates that it must be a simple substitution cipher.(As simple substitution ciphers have I.C. almost equal to that of English text)
- But then we saw a two letter word "ff" in the text which is not possible if it was a simple substitution cipher. However it can be possible in case of Block-Permutation Ciphers.

- But the frequency analysis indicates Substitution cipher. So it may be possible that block permutation is applied to the cipher text obtained on substituting the original message, as permutation ciphers don't change the single letter frequency characteristics of the text.
- So we thought of trying a Substitution-Permutation scheme.
- There were total 270 characters in the message. But the password has only 10 letters. So this leaves us with only two key-length possibilities, i.e, 5 or 10.
- We first tried a key-length of 5 and obtained all 5! permutations of the text. We guessed the last word to be "password" based on past assignments and applied the constraint to obtain only six permutations satisfying it.
- Further, the bigram "ff" should not occur. This leaves us with four permutations. Now we get mapping of 7 letters on placing password in the text. We substitute the rest of the text and get the following:
(This is one of the four permutations, We tried decoding other three through similar analysis which led us to know that this one is the correct permutation)

"fRsApsR Od nkaS oODs Watt fs ftsSSsD fm nks SgesApm SPaRan RsSaDaqv aq nks kOts vO AksAD AqD daqD AWAm Od fRsApaqv nks SPstt Oq kab oASn fm nks swat iAddAR nks SPaRan Od nks oAws bAq aS AtWAmS Wank mOe daqD nks bAvao WAqD nkAn Watt tsn mOe Oen Od nks oAwsS an WOetD bAps mOe A bAvaoaAq qO tsSS nkAq iAddAR nO vO nkROevk SPsAp nks PASSWORD"

- Trying "Od" = "OF" and "nks" = THE :

"fREApER OF THaS oODE Watt fe ftESSED fm THE SgeEApm SPaRaT RESaDaqv aq THE HOtE vO AHEAD AqD FaqD AWAm OF fREApaqv THE SPEtt Oq Hab oAST fm THE Ewat iAFFAR THE SPaRaT OF THE oAwE bAq aS AtWAmS WaTH mOe FaqD THE bAvao WAqD THAT Watt tET mOe OeT OF THE oAwES aT WOetD bApE mOe A bAvaoaAq qO tESS THAq iAFFAR TO vO THROevH SPEAp THE PASSWORD"

- "THas" = "THIS", "HOtE"="HOLE", "SPEAp" = "SPEAK", etc. After such obvious substitutions we decode the message:

"BREAKER OF THIS CODE WILL BE BLESSED BY THE SQUEAKY SPIRIT RESIDING IN THE HOLE. GO AHEAD AND FIND AWAY 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! TO GO THROUGH, SPEAK THE PASSWORD"

- So it was a Substitution-Permutation Cipher with permutation key (1 2 4 3 5) and substitution key "imafubqxjzh-sytcknrelwgvdp"
- We decode **"aap_niviv_dr"** using above keys to get the password **"iit_kjgjf_gr"**

Attachments

The following files are attached:

- **perm_subst.py** : Gives all the possible permutations of the text given the text and permutation key-length input. (The constraint of last word being "password" and non-occurrence of "ff" has been applied in the code so outputs only those permutations which satisfy the constraint)