CS641: THE GREAT CAVES

DEDSEC

Guntas Singh Brar	**Divyanshu Bhardwaj**	**Devanshu Gupta**
180274	180253	180233

January 22, 2020

Chapter 1 : The Entry

Reaching the Cipher Text

- Reading the passage, we use the command "go" and reach a door. There is some message carved on the rocks so we use the command "read"

- The message says to speak out the word "enter" to enter The Great Caves so we use the command "enter".

- We reach a chamber which has another door with a panel beside it. So we use the command "read" and we get a ciphertext:

    "yqw vpal lzelulm evl tkuje svpfclu qt evl spalj. pj gqw spz jll evlul kj zqevkzh qt kzelulje kz evl svpfclu. jqfl qt evl rpelu svpfcluj ikrr cl fqul kzeluljekzh evpz evkj qzl, k pf jlukqwj. evl sqml wjlm tqu evkj fljjphl kj p jkfdrl jwcjekewekqz skdvlu kz ivksv mkhkej vpal cllz jvktelm cg 8 drpslj. tqu evkj uqwzm dpjjiqum kj hkalz clrqi, ikevqwe evl ywqelj."

Cracking The Cipher Text

- We firstly try simple substitution cipher running a monogram frequency analysis on the cipher text.

- We then compared it with standard monogram frequency in the English text and get a key. We use this key to decode the text but didn't get anything meaningful. So we tried manual analysis.

- "l" is the most frequent letter in the cipher text so replaced it with "e".Single letter word "k" occurred in the text so it could be "i"(Substituted characters in capital):

    "gqw vpaE EzeEuEm evE tkuje svpfcEu qt evE spaEj. pj gqw spz jEE evEuE kj zqevkzh qt kzeEuEje kz evE svpfcEu. jqfE qt evE rpeEu svpfcEuj ikrr cl fquE kzeEuEjekzh evpz evkj qzE, k pf jEukqwj. evE sqmE wjEm tqu evkj fEjjphE kj p jkfdrE jwcjekewekqz skdvEu kz ivksv mkhkej vpaE cllz jvkteEm cg 8 drpsEj. tqu evkj uqwzm dpjjiqum kj hkaEz clrqi, ikevqwe evE ywqEj."

- We see that "evE" occurs very often so it could be "THE".Also we have "jEE" which can be "SEE":

    "gqw HpaE EzTEuEm THE tkuST sHpfcEu qt THE spaES. pS gqw spz SEE THEuE kS zqTHkzh qt kzTEuEST kz THE sHpfcEu. SqfE qt THE rpTEu sHpfcEuS ikrr cl fquE kzTEuESTkzh THpz THkS qzE, k pf SEukqwS. THE sqmE wSEm tqu THkS fESSphE kS p SkfdrE SwcSTkTwTkqz skdHEu kz iHksH mkhkTS HpaE cllz SHktTEm cg 8 drpsES. tqu THkS uqwzm dpSSiqum kS hkaEz clrqi, ikTHqwT THE ywqTES."

---

*

- We see "THEuE", "THkS", "HpaE"("THERE","THIS","HAVE"). Substituting, we get:

  "gqw HAVE EzTEuEm THE tIRST sHAfcER qt THE sAVES. AS gqw sAz SEE THERE IS zqTHIzh qt IzTEREST Iz THE sHAfcER. SqfE qt THE rATER sHAfcERS iIrr cl fqRE IzTER-ESTkzh THAz THIS qzE, I Af SERIqwS. THE sqmE wSEm tqR THIS fESSAhE IS A SIfdrE SwcSTITwTIqz sIdHER Iz iHIsH mIhITS HAVE cllz SHItTEm cg 8 drAsES. tqR THIS Rqwzm dASSiqum IS hIaEz cErqi, iITHqwT THE ywqTES."

- We can clearly see tIRST=FIRST, sAVES=CAVES, IzTEREST=INTEREST, SERIqwS=SERIOUS and many more. On substituting we get the decoded message:

  "YOU HAVE ENTERED 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, I AM SERIOUS. THE CODE USED FOR THIS MESSAGE IS A SIMPLE SUBSTITUTION CIPHER IN WHICH DIGITS HAVE BEEN SHIFTED BY 8 PLACES. FOR THIS ROUND PASSWORD IS GIVEN BELOW, WITHOUT THE QUOTES."

- The message says digits have been shifted by 8, so the shift in the digits will be of 4.(Say the true digit in the cipher text was "x", so all the digits are shifted by "x". therefore "2x"="8")"

- We decode "ywZr47Rzee" to get the password **"quNl03Lntt"**

Attachments

The following codes are attached:

- **monofreq_analysis.py** : Simple Monogram Frequency Analysis