[1]

CS641: THE GREAT CAVES

DEDSEC

Guntas Singh Brar 180274
Divyanshu Bhardwaj 180253
Devanshu Gupta 180233

January 22, 2020

Chapter 2 :The Caveman

Reaching the Cipher Text

- We enter the second chamber. We use "go" to see a message on a boulder that goes:
  "The spirit of Cave Man is the keeper of the chamber. To navigate through the chamber, you must pay respect to him first. Bow, and then slowly look up. Count the number of lines in horizontal dimension – they will stand in good stead."
- We proceed using "go" and then use "read" to read the message on the panel:

  "lg ccud qh urg tgay ejbwdkt, wmgtf su bgud nkudnk lrd vjfbg. Yrhfm qvd vng sfuuxytj "vkj_ecwo_ogp_ej_rnfkukf" wt iq urtuwjm. Ocz iqa jdag vio uzthsivi pqx vkj pgyd encpggt. Uy hopg yjg fhkz arz hkscv ckoq pgfn vu wwygt nkioe zttft djkth."

Cracking The Cipher Text

- We first tried simple substitution cipher. We ran frequency analysis on the text and tried to get to the key manually but got nothing.
- Then we calculated the Index of Coincidence of the cipher text. It came out to be around 0.0423 which is much less than that of English text(around 0.66). So we concluded that it must be some polyalphabetic or polygraphic cipher(As substitution ciphers have I.C. similar to English text).
- Further we calculated periodic I.C. for the text and identified peaks at regular intervals.
- These are the charecteristics of Vignere, Porta, Beaufort and Gronsfeld Ciphers. So we tried out Vigenere Cipher first.
- Running periodic I.C. analysis showed peaks at a keylength of 9, 18, 27...
- So we took the keylength as 9 and then used Chi-Squared Statistic to get the key.(Lower Chi-Squared Statistic for a text implies more similarity to English text)
- This way we got the key as **"wcgcwfccr"**. Deciphering the cipher text using this key gave the following:

  "pe wayy of dve neet chkaber, ahero ws veyy lidhle jvy thofe. splak oeh the wassgcrd "toe_cafs_man_ie_ploosed" ao go dvrounh. mai mou hhve trs strlngtr tor toe nehh chatber. dc fink the olit yvu fibgt wisl neor to uater wogic dordc hherl."

[*]

- Here we can see words "chkaber" and "chatber" which should clearly be "chamber". Hence adjusting the key accordingly to "kcgcwfccb" we get:

  "be wayy of the neet chamber, ahere is veyy little jvy there. splak out the wassword "toe_cave_man_ie_pleased" ao go throunh. may you hhve the strlngth for toe next chatber. to fink the exit yvu first wisl need to uater magic dords therl."

- Adjusting the letters, we get the correct key as "" and the deciphered text:

  "be wary of the next chamber, there is very little joy there. speak out the password "the_cave_man_be_pleased" to go through. may you have the strength for the next chamber. to find the exit you first will need to utter magic words there."

Attachments

The following codes are attached:

- **IC_analysis.py** : Calculates the Index of Coincidence of the input text
- **periodic_IC_analysis.py** : Calculates the periodic I.C. for keylengths of 2-30 for a text
- **break_vigenere.py** : Assuming vigenere cipher and given the keylength, outputs the most probable key for the cipher text using Chi-Squared Statistics