CON 101 August 27, 2021

Assignment 3. Cryptanalysis of cipher texts

Due date : Sept 9, 2021

Intro – This assignment will give you an exposure to cryptanalysis techniques. Cryptanalysis is defined as the science and art of breaking codes. The study of cryptanalysis not only helps in breaking the encryption but also helps in creating better encryption techniques by studying its vulnerabilities.

Problem statement / Objective – For this assignment you are given an encrypted text message named as “cipher.txt”. The encryption technique used is Substitution cipher which is a category of traditional symmetric key cipher. In this encryption technique we substitute the characters of message with other characters to make our message unreadable. For e.g. if we substitute (a--> z, n-->p, d-->q) then words like “and” turns to “zpq”. Your task is to find such substitution rules (secret key) using which we can decrypt the given “cipher.txt”.

What to submit –

1. Explain the series of systematic deductions you employed to obtain the secret key.
2. Submit the secret key you obtained.
3. Submit the plain text you decrypted using the secret key you deduced.
4. Submit the code which you used to decrypt the cipher text to plain text.

The above submission should be in a single pdf file including code part. Please order the file as indicate above. Also, IF you have used any tools for pattern matching then write down the series of regex filter or code you applied, serial wise in code part. Name the pdf as “<Entry_num>_Assignment_3” when submitting on Turnitin .

Note : Brute forcing your way in to solution is discouraged. We study cryptanalysis so that we don’t have to try every possible permutations. Substitution ciphers have a particular weakness when used to encrypt English texts. You can find out more in books and internet and see if you can exploit the said weakness.