German University in Cairo
Faculty of MET (CSEN 1001 Computer and Network Security Course)
Dr. Amr El Mougy
Reham Ayman
Abdelrahman Osama

Hacking Assignment 1 : Break Vigenère Cipher

Discussion 08/02/2020 - 12/02/2020 **Task Grade** 5%

1 Introduction

In this task you're required to implement an algorithm to break Vigenère Cipher. This can be done by following the Kasiski method explained in the lecture. The challenge in automating it appears in having a way to determine the repetitions in the given Ciphertext in order to guess the length of the key. Instead of following Kasiski method, we will implement a different algorithm that won't be as efficient as Kasiski method for long cipher texts. The algorithm requires calculating a value called Index of Coincidence, that indicate roughly the probability of two randomly selected letters being equal. You can read more about the Index of Coincidence in the following links:
`https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-IOC-Len.html`

2 Details

You are given a a starter python file containing the base implementation of the task. To compute the key length, you will apply the concept of the Index of Coincidence, you can start by dividing the Ciphertext into various cosets. And then calculating the average Index of Coincidence for this possible division of cosets. You will then have to check the average Index of Coincidence per key length and determine the most probable key length by getting the one with the highest IC.

$$IC = \frac{1}{N(N-1)} \sum_{n=1}^{26} F_i(F_i - 1)$$

You are also provided with a set of test cases S0, S1 and S2 in order to check your implementation once you are done.

You will find the source code on the MET website; "VignereCrackerStarter.py"

3 Submission

You will be required to submit your file at the end of the tutorial slot. Upload the file to the MET website in the corespondent submission link for your tutorial group. The python file should be named as $[ID]\_[TutoiralNumber]\_[Task\_Number]$ (e.g. $[37-1111]\_[T01]\_[Task1]$).

In case there was a problem in the submission through the MET website, then send an email to your TA with the title same as the name of the python file.