Computer Assignment 1

Deadline: Jan 30, 2023, 11:59 PM

Winter 2024

(Upload it to Gradescope.)

Project Description

The goal of this assignment is to learn the basics of traditional encryption mechanisms, which are now considered insecure. There are 6 steps for this assignment, and you need to complete each step one by one.

The description of each step and some hints are provided in the Jupyter notebook, which can be found in this folder. Please follow the instructions and make sure to provide both the code and a description of how your code works.

The project itself is quite straightforward. You might need to spend a bit of time learning how to use Jupyter/Python if you are not familiar with it (it is worth learning, though!). If you are already familiar with it, then you should be able to solve all the steps in a few hours. Please plan accordingly based on your background.

Alternatively, if you don't really want to use Jupyter, you can submit your code in any other language that you want. Make sure that your code is well commented. You should create a Jupiter-style report if you are choosing this route (i.e., put everything in one single PDF: description of your code, code snippet, and the output of your code using screenshots for each step).

What to Submit

Submit your notebook and your report in one PDF (you need to export your notebook as a PDF). Make sure that it includes all the steps, and make sure within each step you are putting: the description, code, and screenshot of the output.

Notes

- If you have any questions, post them on Campuswire. If you know the answer to a question, please answer!
- There might be slight changes/updates to the code, so make sure that you are using the most updated version!
- Sharing is considered cheating! The project is quite simple and it is mostly an opportunity for you to get some minimal hands-on experience, so please do it yourself without seeking help from anyone and/or the internet.