SSN Lab 1 Assignment

Classical Crypto

Intro

In this assignment, you will look at classical methods of encrypting/decrypting. Please keep your report clean and readable. Especially during group work it should be clear from the logs who did what and why.

For writing your report, please consider the following bullet points:

- File:
  - Filename should help to identify your report
    - (e.g. SSN-1st-Lab-YOURNAME_SURNAME).
  - File format should be HTML or PDF.
- Workstation:
  - Update the username and hostname of your machine, it will help us to recognize your screenshots.
- Structure and content:
  - It should follow the structure of the assignment - mention or follow the task numbers in order.
  - Provide the important steps which you are going through, and eventually additional interesting information and links.
  - Provide the configurations and the command lines with proof of work provide outputs (screenshots or text) for acceptance testing.
  - Label pictures and refer to them in the text by the label.
  - Don't just copy past the config file content, explain it, so we know you understand it, and the service is not running by magic.
- Format:
  - You can use any text editor/format for your lab reporting, here is an example of using HackMD online (markdown language). Link
- English:
  - One of the skills that should be obtained by you is technical writing in English.
  - Use special services to check your report before submission (f.e grammarly - but select a proper mode, it has multiple modes).
- External sources:
  - You can and should use external sources, but answers to the questions should be given in your own words, copy/paste in the answer is forbidden. That is needed to show that you understand what you have written (of course you can just paraphrase the text, but the effort is nearly equal to understanding the material and explaining it in your own words).
  - You can use quotes from external sources to reinforce your explanation, but quotation alone is not considered as an answer - answer requires your insight.

  - External sources that were used should be listed in the report. If it is not a quote, you can place them right after the answer/section (or after the report if they are relevant to the report overall). If there was a quote, the eternal source should be specified next to it.
- Discussion among students:
  - In general, assignment tasks can be discussed among students, but tasks and reports should be done individually. But be careful, there is a high level of diversity on ways how a particular task can be made, and if two students are choosing the same way and making the same mistakes it is highly suspicious.

Note: TAs might come before the deadline of the lab in order to check your lab demo.

Preparation

- Read about classical ciphers and understand some of the terms such as but not limited to:
  - Confusion
  - Diffusion
  - Permutation
  - Substitution
  - …

Task 1

1. Go to https://www.dcode.fr/tools-list#cryptography or https://cryptii.com/ crypto service website. Choose Vigenere ciphers and get familiar with it.
2. Make a team of two, encrypt an English text of at least 50 words using the Vigenere cipher, and exchange it with your fellow student.
3. Crack the encrypted text of your fellow student using the Vigenere cipher tool.
4. Go through the previous two steps again, this time using a cipher of your own choosing. Do not tell your fellow student what cipher you used!

Task 2 (bonus)

1. Read about the Enigma machine, how and why it was used?
2. Explain the mechanism of its encryption/decryption.
3. Come with some creative text and encipher/ decipher with Enigma encryption.