SSN Lab Assignment: Classical Crypto[*]

Zhiyang Wang Lucas Hecht[†]

Feedback deadline:
Monday September 9, 2024 10:00 CEST
Final deadline:
Sunday October 27, 2024 23:59 CET

1 Introduction

In this assignment you will look at encrypting and decrypting more closely. You are to keep a log of your progress on your part of the Wiki. You can find this by going to `https://www.os3.nl/2024-2025/start` and scrolling to the list of students at the bottom of the page, and clicking your name. Please use the template structure provided there, and have one Wiki page per assignment.

On this Wiki page document your progress, including choices or assumptions made, problems encountered and answers to the questions posed in this assignment. Please make an effort to explain the methods and steps using your own words, instead of pasting text from a source directly as an answer. Always provide references to your sources. During group work it should be especially clear from the logs who did what and why.

Your answers will be graded by the lab teachers after the end of the block (Sunday October 27th 2024), which is the official, final deadline for the assignment. Your assignments need to be graded “sufficient” after the block for your exam grade to count.

However, the lab teachers can give you intermediate feedback if you place your answers on your Wiki page before the `feedback deadline` stated above each assignment (Monday September 9, 2024, in this case). Within a week after the feedback deadline you will receive an email from the lab teachers with the feedback (usually). You are expected to process this feedback before the final deadline. [1]

Because of the cosy number of students this year, we will not provide you with feedback on all answers. You must, however, answer all questions on your Wiki. Be curious and investigate - do these labs to better yourself, not just to ”pass”. If you want feedback on a particular answer, you can always ask us during lab time or by email.

On `https://www.os3.nl/2024-2025/courses/ssn/labs` you will find DokuWiki templates for the questions in this document. Please copy them to your Wiki tree and add your answers to make grading easier.

2 Installing the VirtualBox Appliance

For this assignment you need the Simon Singh Codebook CD-ROM which we make available via a VirtualBox Appliance running Windows 2003. Install the appliance as follows:

[*] Based on earlier work by E.P. Schatborn, C. Dumitru, J. van der Ham, A. Bakker, P. Prjevara, U. Odyurt. Version September 2, 2024.

[†] lucas@os3.nl, yang@os3.nl, teachers.ssn@os3.nl

[1] Be aware that the final deadline is in the weekend the clock reverts back from savings time.

1. Check if Secure Boot in your desktop's BIOS has been disabled by pressing F2 on startup and selecting "Secure Boot" from the list. It should be disabled by default. If not, tick "Disable"
2. Install VirtualBox on your desktop machine, version 4.3 or higher.
3. Download the `SSNLabs.ova` appliance from `http://software.os3.nl/SSN/`.
4. Start VirtualBox.
5. Import the appliance via the File menu (ignore the fact that its name does not end in .ovf)
6. Start the appliance.
7. Press right Ctrl+Del (or choose "Insert Ctrl-Alt-Del" from the Machine menu) to get a login prompt.
8. Login as Administrator with password `3*wortelV2`
9. Start the Codebook CDROM via the link in the "SSN Lab 1" folder on the desktop.

3 Crypto

Go through the Codebook CD-ROM. We will look at everything upto and including Vigenere ciphers. Choose "Main Contents" and go through the first three chapters of the "Birth of cryptography" upto and including "Mechanising secrecy".

Please ensure that you provide a detailed example with your answers, not just explanation of the workings of the algorithm.

1. (a) What is Atbash?
   (b) What is Affine?
   (c) What is Playfair?
   (d) What is ADFGVX?
   (e) What is Pigpen?
2. Encrypt an English text of at least 80 words using the Vigenere cipher and exchange it with one of your fellow students (also forward it to your lab TA). Do not share the key!
3. Crack the crypted 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!