SSN Lab Assignment: Classical Crypto[*]

A. Bakker C. Dumitru J. van der Ham U. Seddigh M. Pouw[†]

Feedback deadline:
September 11, 2017 10:00 CET

1 Introduction

In this assignment you will look at encoding/decoding more closely. Update your log; give more than just an account of the questions/answers posed in this assignment. Especially during group work it should be clear from the logs who did what and why.

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:

1. Install VirtualBox on your desktop machine, version 4.3 or higher.
2. Download the `SSNLabs.ova` appliance from `http://software.os3.nl/SSN/`.
3. Start VirtualBox.
4. Import the appliance via the File menu (ignore the fact that its name does not end in .ovf)
5. Start the appliance.
6. Press right Ctrl+Del (or choose "Insert Ctrl-Alt-Del" from the Machine menu) to get a login prompt.
7. Login as Administrator with password 3*wortelV2
8. 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".

1. (a) What is Affine?
   (b) What is Atbash?

[*] Based on earlier work by E.P. Schatborn. Version September 4, 2017.
[†] mick.pouw@os3.nl,u.seddigh@uva.nl

(c) What is ADFGVX?

(d) What is Playfair?

(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.

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!