SSN Lab Assignment: Enigma*

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

Feedback deadline:
September 14, 2017 10:00 CET

1 Enigma

Use the Enigma simulator as installed on the VirtualBox image. Write a phrase in English, not shorter than 20 characters which states what present you want for your next birthday. Lookup the settings corresponding to your birthday in 2017 in the code book available at: `https://www.os3.nl/_media/2017-2018/courses/ssn/sne_enigma_2017.zip`, and use these to select the rotors and set the rings on the rotors. Next, follow the official German operating procedure described in `http://www.ellsbury.com/enigma3.htm` to encrypt the phrase.

Question

1. Send the non-secret information required to decrypt the message (which includes the encrypted text and your birthday) to one of your colleagues by email (make sure that you add Mick and Uraz to CC). Once you receive the corresponding message from your fellow colleague, configure your Enigma machine accordingly and decrypt the message.

2 Viola

You've just uncovered a so far unknown encryption machine called Viola which looks a bit similar to the Enigma machine. You are asked to compute the upper bound of different keys (or machine start configurations) you have to search in a brute force attack on an intercepted message.

- The Viola machine can fit 1 static reflector and 10 rotors each with 30 characters.
- There are 5 unique reflectors to select from.
- There are 50 unique (under all rotations) rotors to select from.
- The machine has a standard plugboard for all 30 characters.
- It is unknown how many plugboard cables are used so assume any number could be used.

2. How does the number of keys compare to the number of keys of a typical Enigma machine with the following specification:

*Version September 7, 2017.

†mick.pouw@os3.nl,u.seddigh@uva.nl

- The typical Enigma machine can fit 1 static reflector and 3 rotors each with 26 characters.
- There are 3 unique reflectors to select from.
- There are 5 unique (under all rotations) rotors to select from.
- The machine has a standard plugboard for all 26 characters.
- It is known the operator always uses 10 plugboard cables.