SSN Lab Assignment: Enigma*

Lucas Hecht Zhiyang Wang

Feedback deadline:
Thursday September 12, 2024 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 2024 in the code book available at: `http://software.os3.nl/SSN/sne_enigma_2024.zip`,

and use these to select the rotors and set the rings on the rotors. Next, follow the official German operating procedure (so with a per-operator and per-message key) described in `http://www.ellsbury.com/enigma3.htm` to encrypt the phrase. Operator errors helped crack the Enigma (see "Enigma cillies"), so please follow the procedure correctly!

Question

1. Explain the following terms:
   (a) Ringstellung (ring setting)
   (b) Grundstellung (indicator setting)
   (c) Message setting
   (d) Kenngruppen
2. 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 the lab teachers to CC). Once you receive the corresponding message from your fellow colleague, configure your Enigma machine accordingly and decrypt the message.

*Based on earlier work by C. Dumitru, J. van der Ham, P. Prjevara, U. Odyurt, A. Bakker, V. Breider, R. Vermeulen. Version September 3, 2024.

2 Violetta

You've just uncovered a so far unknown encryption machine called Violetta 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 Violetta machine can fit 1 static reflector and 12 rotors each with 32 characters.
- There are 7 unique reflectors to select from.
- There are 53 unique (under all rotations) rotors to select from.
- The machine has a standard plugboard for all 32 characters.
- It is unknown how many plugboard cables are used so assume any number could be used.

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

- 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.