Classical Cryptography

JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

4. Tutorial: The Enigma

(Hand in solutions on Monday, June 9th,
at the beginning of the tutorial)

As you might have guessed from the title, this tutorial focuses on the German Enigma encryption machine used during World War II. The following description of this machine is by no means complete. For more details, please refer to the lecture notes (or to Wikipedia, which offers quite a complete set of articles on the subject).

We consider here the model "M3" of the Enigma, as used by the German Army. It is composed of the following elements:

- A keyboard comprising all 26 letters from A to Z.
- A plugboard (*Steckerbrett*) with 26 pairs of sockets (one pair for each letter), allowing the operator to swap pairs of letters with the use of cross-wired cables.
- An entry stator (*Eintrittswalze*) mapping the (possibly swapped) signal from the plugboard onto 26 metal contacts placed along a circle on the left-hand side of the wheel. The contact 1 corresponds to the letter A, 2 to B, and so on. This stator is fixed (hence the name).
- Three rotors (*Walzen*) chosen among a set of five available rotors (named I, II, III, IV and V) and placed in a given order. Each rotor has 26 spring contacts on the right-hand side and 26 metal contacts on the right-hand side, allowing them to be connected to each other (and also to the entry stator) by putting them side-by-side.

  Each rotor implements a different permutation of the 26 inputs (the right-hand side) into the 26 outputs (the left-hand side) by means of internal wiring. Each rotor can be set to any of the 26 possible positions in the machine by just rotating it by the correct amount.

  An 26-letter alphabet ring is attached in the outer side of the rotor and can also be rotated to any of the 26 possible positions. In position A, the input and output pins 1 correspond to the letter A, in position B, they correspond to B, and so on. Once the alphabet ring is set, the operator is

given a letter for each rotor, and should rotate this rotor accordingly, so that the given letter appears on top of the rotor (visible through a small window).

The rotors turn with each pressing of a key. Usually, only the first (rightmost) rotor advances by one step for each key pressed. The second rotor (middle) advances by one step only when the first one is on a particular position, called the stepping position. The third rotor (rightmost) then advances when the second one in on its own stepping position. It is to be noted that in that particular case, the middle rotor also advances by one step. Each rotor has its own different stepping position which is linked to the alphabet ring (and not to the rotor itself).

- A reflector (*Umkehrwalze*), placed on the left of the three rotors, with 26 metal contacts on the right-hand side (allowing connection to the leftmost rotor). The reflector swaps pairs of positions by means of internal wiring. Each position i is mapped to another position j (which itself is mapped back to i). This reflector is fixed.
- A set of 26 lamps, one for each letter from A to Z.

Once the rotors are in place and put into the according position, the mode of operation is the following:

- The operator presses a key on the keyboard (*e.g.* C).
- This key-press advances one or several rotors by one step.
- While pressing the key, a contact is made, and "electricity" flows towards the corresponding letter of the plugboard (*e.g.* C).
- If the letter is not swapped by the plugboard, then the electric signal continues to the entry stator, in the corresponding output pin (*e.g.* 3, corresponding to C).

  If the letter is swapped with another letter (*e.g.* E), the signal reached the entry stator at the output pin corresponding to this other letter (*e.g.* 5 here).
- The signal goes through the three permutations given by the rotors, then is permuted by the reflector, and once again through the three rotors in the reverse order (note that on this way back, the permutations are also inversed!). The signal finally reaches a contact on the entry stator (*e.g.* 1).
- The signal goes back to the plugboard, where it is eventually swapped with another letter.

- It finally reaches one the lamps, which is then lit. The letter corresponding to this lamp is the encrypted letter.

The permutations of the five rotors and of the reflector are given as follows:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rotor	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
I	5	11	13	6	12	7	4	17	22	26	14	20	15	23	25	8	24	21	19	16	1	9	2	18	3	10
II	1	10	4	11	19	9	18	21	24	2	12	8	23	20	13	3	17	7	26	14	16	25	6	22	15	5
III	2	4	6	8	10	12	3	16	18	20	24	22	26	14	25	5	9	23	7	1	11	13	21	19	17	15
IV	5	19	15	22	16	26	10	1	25	17	21	9	18	8	24	12	14	6	20	7	11	4	3	13	23	2
V	22	26	2	18	7	9	20	25	21	16	19	4	14	8	12	24	1	23	13	10	17	15	6	5	3	11
Refl.	25	18	21	8	17	19	12	4	16	24	14	7	15	11	13	9	5	2	6	26	3	23	22	10	1	20

The stepping positions of rotors I, II, III, IV and V are Q, E, V, J and Z, respectively.

Exercise 4.1 (Key size and unicity distance). (12 points)

The configuration of the Enigma is given by:

- the choice of three different rotors among five;
- the initial position of these rotors in the machine;
- the stepping positions of the first two rotors (this is controlled by the position of the alphabet ring on those rotors);
- the configuration of the plugboard, which can swap up to 13 pairs of letters.

(i) Compute the number of possible choices for the rotors. 1

(ii) Compute the number of possible positions of the three rotors. 1

(iii) Compute the number of possible configurations of the stepping positions. 1

(iv) Compute the number of possible plugboard configurations when 1 pairs of letters are swapped. Then for 2, 3, ... 13 pairs of letters. 2

(v) Compute the overall number of possible plugboard configurations. 1

(vi) Compute the overall number of possible Enigma configurations. [2]

(vii) What would then be the size (in bits) of a "key" encoding all those possibilities? [2]

[2] (viii) Assuming that we use the Enigma to encrypt English or German text (whose entropy is roughly 1.5 bits per letter), what is the unicity distance of the Enigma?

Exercise 4.2 (Encryption and decryption). (14 points)

Let's first consider a simple configuration of the Enigma: rotors III, II and I (from left to right), all with their alphabet ring in position A and no cable on the plugboard. The rotors are set so that their position is AAZ (*i.e.* upon the first key-press, they will move into position AAA).

[1] (i) Starting from such a configuration, what is the encryption of the letter A? *Warning!* Describe all the steps!

[1] (ii) Starting from the same configuration, what is the encryption of the letter N?

[3] (iii) Show that in the general case (meaning, in any configuration of the rotors), encryption and decryption are equivalent.

Now, what if we add some cable on the plugbard?

[2] (iv) Give the encryptions of A and R with cables between A-C and R-X (starting from the same initial position).

[2] (v) Give he encryption of A and N with cables between A-N.

[2] (vi) Conclude. Justify your answer.

[3] (vii) Can one letter be encrypted as itself? Why?

Exercise 4.3 (Rotor stepping). (20+4 points)

We recall here the rotor stepping algorithm, which is executed at each pressing of a key:

- step the rightmost rotor;
- if the middle rotor is in its stepping position, step the middle **and** the leftmost rotor;
- if the middle rotor was not already stepped and the rightmost rotor was initially in its stepping position, step the middle rotor.

Consider now the configuration III-I-II (from left to right) with the alphabet rings in position AAA. The rotors are also set in position AAA, and the plugboard is not used.

Suppose the operator presses the key A.

(i) The rotors first advance by one step. What is the new position of the rotors? [1]

(ii) What is the index of the input pin of the first rotor which receives the signal? [1]

(iii) What is the index of the corresponding output pin of the first rotor? [1]

(iv) What is the index of the input pin of the second rotor which will then receive the signal? [1]

(v) Continue this process, and give the encryption of A. [2]

Then operator types again the key A.

(vi) What is the new position of the rotors? [1]

(vii) What is the obtained encryption of A, this time? *Warning!* Describe all the steps! [2]

The operator presses again A twice.

(viii) What are the two obtained encryptions? 2

Finally, the operator types A one last time.

(ix) What is the new position of the rotors? 2
Warning! The stepping position for rotor II is E.

2 (x) What is then the encryption of A?

Now the operator changes the position of the rotors, and set them as APD. He then proceeds to typing A four times.

3 (xi) Describe the evolution of the position of the rotors after each of these four key-strokes.

+4 (xii) Give the corresponding encryption of the typed sequence AAAA.

2 (xiii) Starting from one initial position of the rotors, how many keys does the operator need to press to end up again on the same position? (*i.e.* what is the length of the cycle?)