Classical Cryptography

JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

5. Tutorial: Cryptanalysis of the Enigma

Exercise 5.1 (Characteristics).

Every day, all the Enigma operators would start typing each message with the same Enigma settings as specified for that particular day on a codebook. However, for better security, they would choose different message keys (rotor positions) for each message.

The mode of operation for encryption of a given message would then be the following:

- put the machine in the initial setting as specified by the codebook,
- type in a chosen message key twice (*e.g.* `BITBIT`),
- put the rotors in the position indicated by the message key (*e.g.* `BIT` here), and
- type the actual message.

A receiving operator would then:

- put the machine in the initial setting as specified by the codebook,
- receive and decrypt the first six characters, checking for correct repetition and extracting the message key (*e.g.* `BIT` in our case),
- put the rotors in the position indicated by the message key,
- decrypt the rest of the ciphertext.

However, such a scheme exhibits an extremely weak point, which we will exploit in this exercise.

We give here a table of a few encrypted message keys received on the same day (*i.e.* encrypted from the same Enigma initial setting):

ADI XSZ	HBZ GDE	LRX BTD	SWM NLG
BYZ MKE	HUR GZL	MHE HCS	TCH AEI
COG DVH	IAS FJM	MSF HGV	UNC WIA
DBB CDN	IJY FPO	NUU VZJ	VIV SXF
DEJ CAR	JAK EJX	OQL UOU	VPG SRH
EAF JJV	JTU EFJ	PVZ LME	XBT YDK
FPU IRJ	KGL ZHU	QFH RBI	YQU KOJ
GSJ PGR	LRO BTW	RIU QXJ	ZHE TCS

(i) Check that, when the letters in position i (i being 1, 2 or 3) are the same between two such enrypted message keys, then so are the letters in position $i + 3$. Explain why.
For instance, a H in position 1 always gives a G in position 4.

(ii) From this, derive the permutation σ_1 which, given a letter x in position 1, will tell us to which letter $\sigma_1(x)$ it corresponds in position 4.
For instance, $\sigma_1(\mathsf{H}) = \mathsf{G}$.

(iii) Express this permutation as a product of cyclic permutations.

(iv) Count the length of the cycles. This is called a *characteristic*.

(v) Explain why we can only have an even number of cycles of each length.

(vi) Will the characteristic change if we use a different plugboard configuration?

(vii) Can you give the permutations σ_2 (from position 2 to 5) and σ_3 (from position 3 to 6)?

(viii) Give their characteristic.

(ix) Assuming that over these six characters no stepping of the middle or leftmost rotor has occurred, devise a way to use the three characteristics to find the initial rotor order and position.