Summerschool crypt@b-it 2008

JÉRÉMIE DETREY, DANIEL LOEBENBERGER

Exercise sheet Enigma

In this tutorial we are going to explore the Enigma in greater detail. To start download the Enigma simulator from the tutorial's web page and unpack it on your computer. The simulator we will use is named `m3bp.exe`.

Exercise 1 (From the lecture).

(i) *Find a formula for the number of possible settings of n plugboard connections $(n = 0, 1, 2, \ldots, 13)$.*

(ii) *"Cribs" are stereotypical parts of a message. E. g.*
`WETTERBERICHT` (weather report)
`OBERKOMMANDO` (high command)
`KEINEBESONDERENVORKOMMNISSE` (no notable events)
If the ciphertext started with `GBDQQBHNWZTA`, the message can start with only one of the above cribs. Which one?

(iii) *Assume that the starting position of the Enigma is `RLU`. Suppose furthermore, that the middle and the left rotor advances if the letter `Z` is displayed either from the right or from the middle rotor. Determine all positions which cannot appear in the sequel. From this, calculate the period of the Enigma, that is the number of key strokes, until the Enigma is in position `RLU` again.*

Exercise 2 (Playing with the Enigma).

(i) *Translate the string `crypt@b-it 2008` into an Enigma readable format.*

(ii) *Encrypt the resulting message using the Enigma's initial settings provided in the codebook page. Use `CPT` for the message key.*

(iii) *Describe in detail the way the letter `A` is processed by the Enigma when using the same key as in part (ii).*

(iv) *Use the provided codebook page to decrypt the message*

```
CRYPTABIT 01.08.2008 09:00 = 4 = WMSMUG =

WWHOR TGQTF NXPUM ADMAF PIDQF
```

Exercise 3 (Cryptanalysing Enigma the Polish way).
*We place ourselves before September 1938, when the German operators sent an enciphered message key (entered twice). At that time, only three rotors (I, II and III) and reflector B were in use. In the following, we assume that the alphabet ring positions are 1-1-1 (*i.e. *the letter* A *corresponds to pin 1,* B *to pin 2, and so on). The following table gives their internal wiring:*

	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
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

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

APN VIS	GBD PEE	NCK QZW	TMJ FJM
CDX MBK	GOU PFQ	NVE QGO	UGX RCK
CKC MLV	HCI IZD	OCT JZF	VAN COS
DEY NRX	HDA IBJ	OHV JPC	VXP CVL
DGF NCY	ISO YDH	QOJ XFM	WXU UVQ
EVT TGF	KVU ZGQ	QUW XKZ	XPD BIE
EZG TWN	LMS AJA	SJI OYD	YTL EAU
FLI GXD	MWV SUC	TAE FOO	ZYY LMX

We denote by σ_1, σ_2 and σ_3 the three permutations mapping the first letter to the fourth, the second to the fifth and the third to the sixth, respectively. For instance: $\sigma_1(\mathsf{A}) = \mathsf{V}$, $\sigma_2(\mathsf{A}) = \mathsf{O}$ *and* $\sigma_3(\mathsf{A}) = \mathsf{J}$.

(i) *Recall the general property on the lengths of the cycles in each permutation σ_1, σ_2 and σ_3.*

(ii) *Using the 32 doubly enciphered keys, give the complete cycle decomposition of the three permutations σ_1, σ_2 and σ_3. What is the characteristic of the day?* (i.e. *the lengths of the cycles)*

(iii) *Assuming that the letters* RIZ *are the first three letters of a doubly enciphered message key intercepted on the same day, give the following three letters $\sigma_1(\mathsf{R})$, $\sigma_2(\mathsf{I})$ and $\sigma_3(\mathsf{Z})$.*

The following table is an excerpt of the characteristic tables as built by Rejewski with help of his Cyclometer. It corresponds to rotor positions III-II-I (from left to right). We assume the rotor settings of the day to be contained in this table.

Rotor position	Characteristic	Permutation (without plugboard)
...	...	...
BIR	13, 13	(AEJHNTCSUFMLY) (BRGXZOKWVQPID)
BIS	12, 12, 1, 1	(ATKEGXFLYHUD) (BONVICRQSZMJ) (P) (W)
BIT	13, 13	(AHFUBZKIGLNVP) (CTXORMWYDQESJ)
BIU	12, 12, 1, 1	(BNSPIMZKXRJE) (CHTDLYGOFVWU) (A) (Q)
BIV	13, 13	(AVRMSTJWUCKZL) (BHIPEOFGYDNQX)
BIW	9, 9, 3, 3, 1, 1	(ATFSDBECO) (GRZWUKLXV) (HYI) (JPM) (N) (Q)
BIX	11, 11, 2, 2	(AJMIDETHGNS) (FPXKWZYLUQO) (BC) (RV)
BIY	13, 13	(AULOITYHGRWVB) (CJXPQZNEDSKMF)
BIZ	8, 8, 4, 4, 1, 1	(BIXTZNKJ) (EPVHOQFW) (CYDR) (GMLS) (A) (U)
...	...	...

(iv) *Using the characteristic of the day (*i.e. *the lengths of the cycles, but not the permutations themselves, since they might be subjected to changes through the plugboard), find the starting position of the rotors from this table.*
Warning: *The rotors move* before *a letter is encrypted.*

(v) *Assuming that only a few plugboard connections are made (meaning that most of the letters are not swapped by the plugboard), using the permutations you just computed and the permutations from the table, determine the plugboard configuration.*

(vi) *We also have intercepted the following double enciphered key on the same day:* `VQQ CQT`. *Decrypt and find the corresponding message key.*