

# Secret Key Cryptography (Spring 2006)

Instructor: Adi Shamir

Teaching assistant: Eran Tromer

## Appendix to Lecture 2:

### Rejewski's method for recovering the Enigma message password

The example in Garlinksi's book (partially shown in class) is partial and inaccurate. The following works out the missing details. For another account (containing all the notation but also missing details of the analysis), see Rejewski's paper on the course webpage.

#### Preparation

By observing how the 1st ciphertext letter is mapped to the 4th ciphertext letter in the day's transmissions, we obtain the permutation  $AD$  and observe that it has the following cycle structure:

$$AD = (\mathbf{A})(\mathbf{S})(\mathbf{BC})(\mathbf{RW}) \dots$$

Similarly, looking at the 2nd and 5th ciphertext letters we find the permutation  $BE$ :

$$BE = (\mathbf{D})(\mathbf{K})(\mathbf{AXT})(\mathbf{CGY})(\mathbf{BLFQVEOUM})(\mathbf{HJPSWIZRN})$$

And looking at the 3rd and 6th ciphertext letters we can find the permutation  $CF$ :

$$CF = (\mathbf{ABVIKTJGFCQNY})(\mathbf{DUZREHLXWPSMO})$$

Looking at the captured ciphertext prefixes, we note that the prefix  $\mathbf{SYXSCW}$  appears several times in adjacent captured transmissions, implying a lazy Enigma operator that used the same message password. We guess (based on past experience) that this message password is the "cilly" password  $\mathbf{AAA}$ . Hence, by definition of  $A, B, C, D, E, F$ :

$$A(\mathbf{A}) = \mathbf{S}, B(\mathbf{A}) = \mathbf{Y}, C(\mathbf{A}) = \mathbf{X}, D(\mathbf{A}) = \mathbf{S}, E(\mathbf{A}) = \mathbf{C}, F(\mathbf{A}) = \mathbf{W}$$

#### Analyzing $AD$

Since the only cycles of size 1 in  $AD$  are  $(\mathbf{A})$  and  $(\mathbf{S})$ , it must hold that both  $A$  and  $D$  contain the cycle  $(\mathbf{AS})$ :

$$A = (\mathbf{AS}) \dots, \quad D = (\mathbf{AS}) \dots$$

This is consistent with the cilly ( $A(\mathbf{A}) = \mathbf{S}$  and  $D(\mathbf{A}) = \mathbf{S}$ ), and thus lends some credence to our guess of the cilly. But we don't learn anything else yet.

#### Analyzing $BE$

We know  $B(\mathbf{A}) = \mathbf{Y}$  and  $BE(\mathbf{A}) = \mathbf{X}$ , hence  $E(\mathbf{Y}) = E(B(\mathbf{A})) = BE(\mathbf{A}) = \mathbf{X}$ .<sup>1</sup> From this and  $BE(\mathbf{G}) = \mathbf{Y}$  we deduce  $B(\mathbf{X}) = B(E(\mathbf{Y})) = EB(\mathbf{Y}) = E^{-1}B^{-1}(\mathbf{Y}) = (BE)^{-1}(\mathbf{Y}) = \mathbf{G}$ . From this and  $BE(\mathbf{X}) = \mathbf{T}$  we deduce  $E(\mathbf{G}) = E(B(\mathbf{X})) = BE(\mathbf{X}) = \mathbf{T}$ . From the latter and  $BE(\mathbf{C}) = \mathbf{G}$  we deduce  $B(\mathbf{T}) = \mathbf{C}$ , and finally using  $BE(\mathbf{T}) = \mathbf{A}$  we deduce  $E(\mathbf{C}) = \mathbf{A}$ . Overall, we have deduced the following cycle of mappings:

$$\rightsquigarrow \mathbf{A} \xrightarrow{B} \mathbf{Y} \xrightarrow{E} \mathbf{X} \xrightarrow{B} \mathbf{G} \xrightarrow{E} \mathbf{T} \xrightarrow{B} \mathbf{C} \xrightarrow{E} \rightsquigarrow$$

Hence, we've fully derived the values of  $B$  and  $E$  on all letters involved in the 3-cycles of  $BE$ . If you've solved Exercise 1 by direct argument, you probably see that this is not a coincidence — what we've done amounts to the following.

---

<sup>1</sup>Our notation is  $PQ(\alpha) = Q(P(\alpha))$ .

