4 Cryptanalysis of the Enigma Without Plugboard

The Commercial Enigma

The types C and D of Enigma had a reflecting rotor but no plugboard. They were sold on the free market and could be comprehensively analyzed by everyone.

In the Spanish civil war all parties used the Enigma D. All big powers broke it.

The substitution of the commercial Enigma simplifies to

$$c_i = \sigma_z^{-1} \pi \sigma_z(a_i)$$

where σ_z is the substitution by the three rotors in state $z = (z_1, z_2, z_3)$. The reflecting rotor was fixed during encryption but could be inserted in any of 26 positions.

Searching for Isomorphs

In a section of the text where only rotor 1 moves, the two inner rotors together with the reflecting rotor yield a constant involution $\tilde{\pi}$. If the plaintext for this section (say of length m) is known, then we have equations

$$\begin{array}{rcl} c_1 & = & \left[\rho_1^{(z_1)}\right]^{-1} \tilde{\pi} \rho_1^{(z_1)}(a_1) \\ c_2 & = & \left[\rho_1^{(z_1+1)}\right]^{-1} \tilde{\pi} \rho_1^{(z_1+1)}(a_2) \\ & \ldots & \\ c_m & = & \left[\rho_1^{(z_1+m-1)}\right]^{-1} \tilde{\pi} \rho_1^{(z_1+m-1)}(a_m) \end{array}$$

Hence for $i = 1, \ldots, m$ the intermediate text

$$c_i' = \rho_1^{(z_1+i-1)}(c_i) = \tilde{\pi} \rho_1^{(z_1+i-1)}(a_i)$$

is the monoalphabetic image $c_i' = \tilde{\pi}(a_i')$ of the intermediate text

$$a_i' = \rho_1^{(z_1+i-1)}(a_i)$$

under the involution $\tilde{\pi}$.

Therefore pattern search identifies the fast rotor and its state by testing all rotors and all initial states. For determining a_i' from a_i we have to test all three rotors with all 26 start positions, and determine c_i' from c_i with the same rotor in the same position. This exhaustion comprises $3 \times 26 = 78$ different constellations, each of which has to be tested for a matching pattern. Probably there are several false solutions in addition to the correct one.

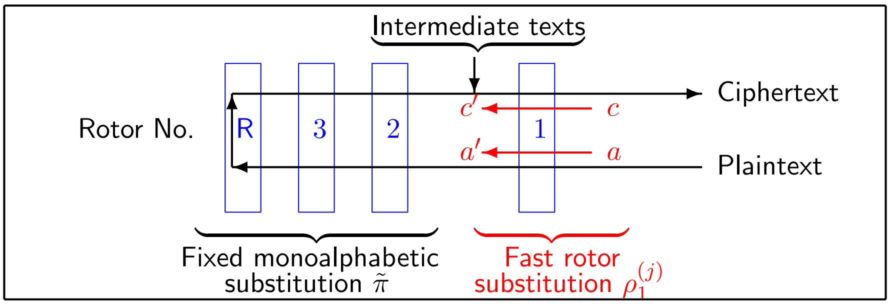
Intermediate texts
Rotor No.
R
3
2
1
Ciphertext
Plaintext
c'
c
a'
a
Fixed monoalphabetic substitution $\tilde{\pi}$
Fast rotor substitution $\rho_1^{(j)}$

Figure 2: *Searching for isomorphs*

The next sieving step uses the fact that $\tilde{\pi}$ is a fixed involution. If for a possible solution we find a coincidence $c'_i = a'_j$ with $j \neq i$, then we test for

$$a'_i \mapsto c'_i = a'_j \mapsto c'_j \overset{?}{=} a'_i$$

If no, we discard the solution. If yes, we even identified a 2-cycle of $\tilde{\pi}$, reducing the number of $26^2 = 676$ possible states of the two inner rotors. A useful tool for this is a precomputed table of length 676 for each of the 6 different combinations of these two rotors that contains the cycle decomposition of $\tilde{\pi}$ for all states, making a total of $6 \times 676 = 4056$ involutions.

Precomputing the lookup table is easy: Let the cycles of π be $(a_1, b_1), \ldots, (a_{13}, b_{13})$. Let $\xi = \rho_3^{(z_3)} \circ \rho_2^{(z_2)}$ be the combined substitution by rotors 2 and 3. Then the cycle decomposition of $\tilde{\pi} = \xi^{-1} \circ \pi \circ \xi$ is

$$\tilde{\pi} = (\xi^{-1}a_1, \xi^{-1}b_1), \ldots, (\xi^{-1}a_{13}, \xi^{-1}b_{13})$$

We only need to apply the fixed substitution ξ^{-1} to the string $a_1b_1 \ldots a_{13}b_{13}$.

The location of known plaintext, if not known a priori, may be narrowed down by negative pattern search.

Conclusion

The introduction of the reflecting rotor aimed at a significant gain for the security of Enigma by doubling the number of rotor passages. This turned out to be an illusory complication. The attack by isomorphs reduces the cryptanalysis to the exhaustion of position and state of three rotors only, and even this is reduced in a substantial manner.

To prevent this attack the Wehrmacht (= army) introduced the plugboard when adopting the Enigma.