Cracking the enigma

Recall that deciphering a message encrypted by the enigma required:

- Knowledge of the plugboard configuration
- Drum setup (rotors, initial positions, notches)
- Reflector plate knowledge.

However, if we accept that permutation ciphers are insecure (something we will soon justify) then recalling that the action of the enigma is:

$$P^{-1} R_1^{-1} R_2^{-1} R_3^{-1} R R_3 R_2 R_1 P$$

we observe:

If we can figure out the rotor configuration, what's leftover is simply a permutation cipher. (Not exactly, but the point is that what remains is a few unknown constant permutations) KEY.

So we focus on cracking the initial rotor configuration.

Early war and Polish codebreaking: (Rejewski)

The enigma machine was used as follows:
Cipher clerks, on a monthly basis, would be given a table of daily keys (not really daily, but changed at various intervals). These were instructions on how to set up the enigma, depending on the time.