**Good operating procedures, properly enforced, would have made the plugboard Enigma machine unbreakable. However, most of the German military forces, secret services and civilian agencies that used Enigma employed poor operating procedures, and it was these poor procedures that allowed the Enigma machines to be reverse-engineered and the ciphers to be read.**

The Enigma rotor cipher machine was potentially an excellent system. It generated a polyalphabetic substitution cipher -- a substitution cipher is a method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution.

**A major weakness of the system, however, was that no letter could be enciphered to itself. This meant that some possible solutions could quickly be eliminated because of the same letter appearing in the same place in both the ciphertext and the putative piece of plaintext.**

**Marian Rejewski spotted the Germans' major procedural weaknesses of specifying a single indicator setting for all messages on a network for a day, and repeating the operator's chosen message key in the enciphered 6-letter indicator. Those procedural mistakes allowed Rejewski to decipher the message keys without knowing any of the machine's wirings.**

Even though Rejewski did not know the rotor wirings or the plugboard permutation, the German mistake allowed him to reduce the number of possible substitution ciphers to a small number.

**Rejewski also exploited cipher clerk laziness. Scores of messages would be enciphered by several cipher clerks, but some of those messages would have the same encrypted indicator. That meant that both clerks happened to choose the same three letter starting position. Such a collision should be rare with randomly selected starting positions, but lazy cipher clerks often chose starting positions such as "AAA", "BBB", or "CCC". Those security mistakes allowed Rejewski to solve each of the six permutations used to encipher the indicator.**

That solution was an extraordinary feat. Rejewski did it without knowing the plugboard permutation or the rotor wirings. Even after solving for the six permutations, Rejewski did not know how the plugboard was set or the positions of the rotors. Knowing the six permutations also did not allow Rejewski to read any messages.

**Rejewski, in 1934 or 1935, devised a machine to facilitate making the catalog and called it a cyclometer. This "comprised two sets of rotors... connected by wires through which electric current could run. Rotor N in the second set was three letters out of phase with respect to rotor N in the first set, whereas rotors L and M in the second set were always set the same way as rotors L and M in the first set".[56] Preparation of this catalog, using the cyclometer, was, said Rejewski, "laborious and took over a year, but when it was ready, obtaining daily keys was a question of [some fifteen] minutes".[57]**

However, on 1 November 1937, the Germans changed the Enigma reflector, necessitating the production of a new catalog—"a task which [says Rejewski] consumed, on account of our greater experience, probably somewhat less than a year's time".[57]

This characteristics method stopped working for German naval Enigma messages on 1 May 1937, when the indicator procedure was changed to one involving special codebooks (see German Navy 3-rotor Enigma below).[58] Worse still, on 15 September 1938 it stopped working for German army and air force messages because operators were then required to choose their own Grundstellung (initial rotor setting) for each message. Although German army message keys would still be double enciphered, the days keys would not be double enciphered at the same initial setting, so the characteristic could no longer be found or exploited.

**On 15 December 1938, the German Army increased the complexity of Enigma enciphering by introducing two additional rotors (IV and V). This increased the number of possible wheel orders from 6 to 60.**