The set of shortcomings that the Polish cryptanalysts exploited to such great effect included the following:

* The production of an early Enigma training manual containing an example of plaintext and its genuine ciphertext, together with the relevant message key. When Rejewski was given this in December 1932, it "made [his reconstruction of the Enigma machine] somewhat easier".[[83]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-Rejewski84P243-83)
* Repetition of the message key as described in [Rejewski's characteristics method](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#Rejewski's_characteristics_method), above. (This helped in Rejewski's [solving Enigma's wiring](https://en.wikipedia.org/wiki/Marian_Rejewski#Solving_Enigma's_wiring) in 1932, and was continued until May 1940.)
* Repeatedly using the same stereotypical expressions in messages, an early example of what Bletchley Park would later term [cribs](https://en.wikipedia.org/wiki/Crib_(cryptanalysis)). Rejewski wrote that "... we relied on the fact that the greater number of messages began with the letters *ANX*—German for "to", followed by *X* as a spacer".[[90]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-90)
* The use of easily guessed keys such as *AAA* or *BBB*, or sequences that reflected the layout of the Enigma keyboard, such as "three [typing] keys that stand next to each other [o]r diagonally [from each other]..."[[91]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-91) At Bletchley Park such occurrences were called *cillies*.[[92]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-David_Kahn_1991_p._113-92)[[93]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-93) Cillies in the operation of the four-rotor *Abwehr* Enigma included four-letter names and German obscenities. Sometimes, with multi-part messages, the operator would not enter a key for a subsequent part of a message, merely leaving the rotors as they were at the end of the previous part, to become the message key for the next part.[[94]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-94)
* Having only three different rotors for the three positions in the scrambler. (This continued until December 1938, when it was increased to five and then eight for naval traffic in 1940.)
* Using only six plugboard leads, leaving 14 letters *unsteckered*. (This continued until January 1939 when the number of leads was increased, leaving only a small number of letters unsteckered.)

Other useful shortcomings that were discovered by the British and later the American cryptanalysts included the following, many of which depended on frequent solving of a particular network:

* The practice of re-transmitting a message in an identical, or near-identical, form on different cipher networks. If a message was transmitted using both a low-level cipher that Bletchley Park broke by hand, and Enigma, the decrypt provided an excellent crib for Enigma decipherment.[[95]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-95)
* For machines where there was a choice of more rotors than there were slots for them, a rule on some networks stipulated that no rotor should be in the same slot in the scrambler as it had been for the immediately preceding configuration. This reduced the number of wheel orders that had to be tried.[[96]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-96)
* Not allowing a wheel order to be repeated on a monthly setting sheet. This meant that when the keys were being found on a regular basis, economies in excluding possible wheel orders could be made.[[97]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-Taunt_1993_108-97)
* The stipulation, for Air Force operators, that no letter should be connected on the plugboard to its neighbour in the alphabet. This reduced the problem of identifying the plugboard connections and was automated in some Bombes with a Consecutive Stecker Knock-Out (CSKO) device.[[98]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-98)
* The sloppy practice that John Herivel anticipated soon after his arrival at Bletchley Park in January 1940. He thought about the practical actions that an Enigma operator would have to make, and the short cuts he might employ. He thought that, after setting the alphabet rings to the prescribed setting, and closing the lid, the operator might not turn the rotors by more than a few places in selecting the first part of the indicator. Initially this did not seem to be the case, but after the changes of May 1940, what became known as the [Herivel tip](https://en.wikipedia.org/wiki/Herivel_tip" \o "Herivel tip) proved to be most useful.[[92]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-David_Kahn_1991_p._113-92)[[99]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-99)[[100]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-100)
* The practice of re-using some of the columns of wheel orders, ring settings or plugboard connections from previous months. The resulting analytical short-cut was christened at Bletchley Park *Parkerismus* after Reg Parker, who had, through his meticulous record-keeping, spotted this phenomenon.[[101]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-101)
* The re-use of a permutation in the German Air Force METEO code as the Enigma *stecker* permutation for the day.[[102]](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#cite_note-102)