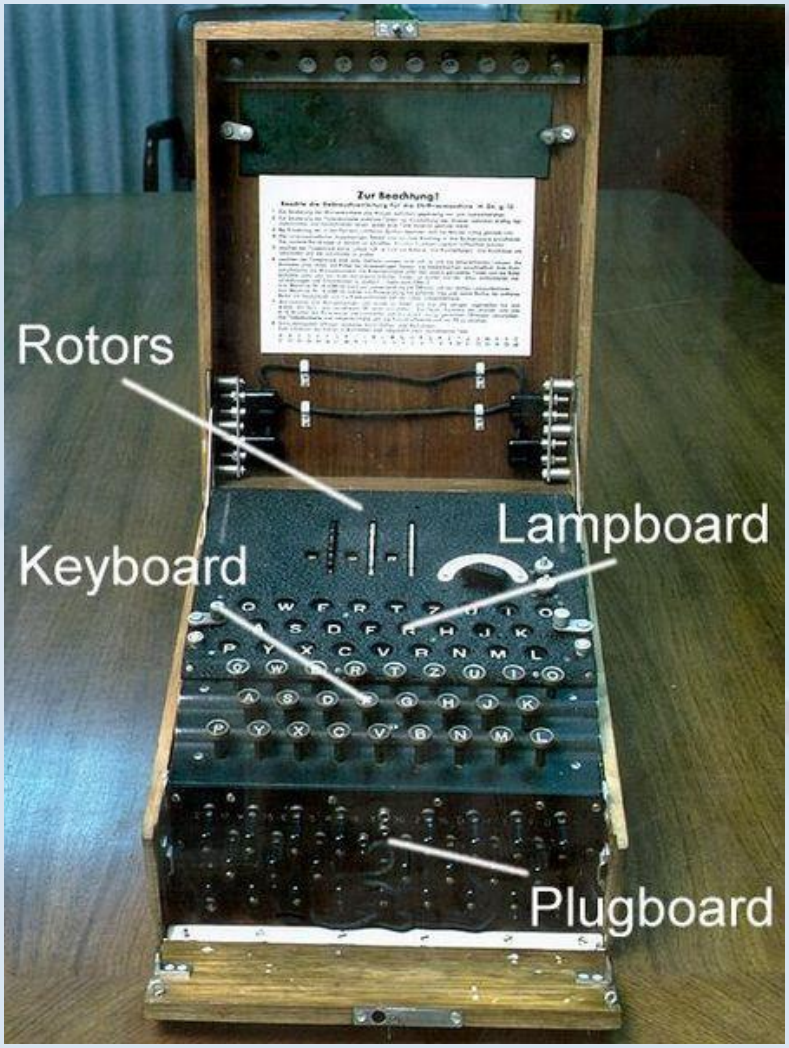
Solving the Enigma

How the Western Allies Cracked the German Secret Codes During WW II

Vital to Allied Effort

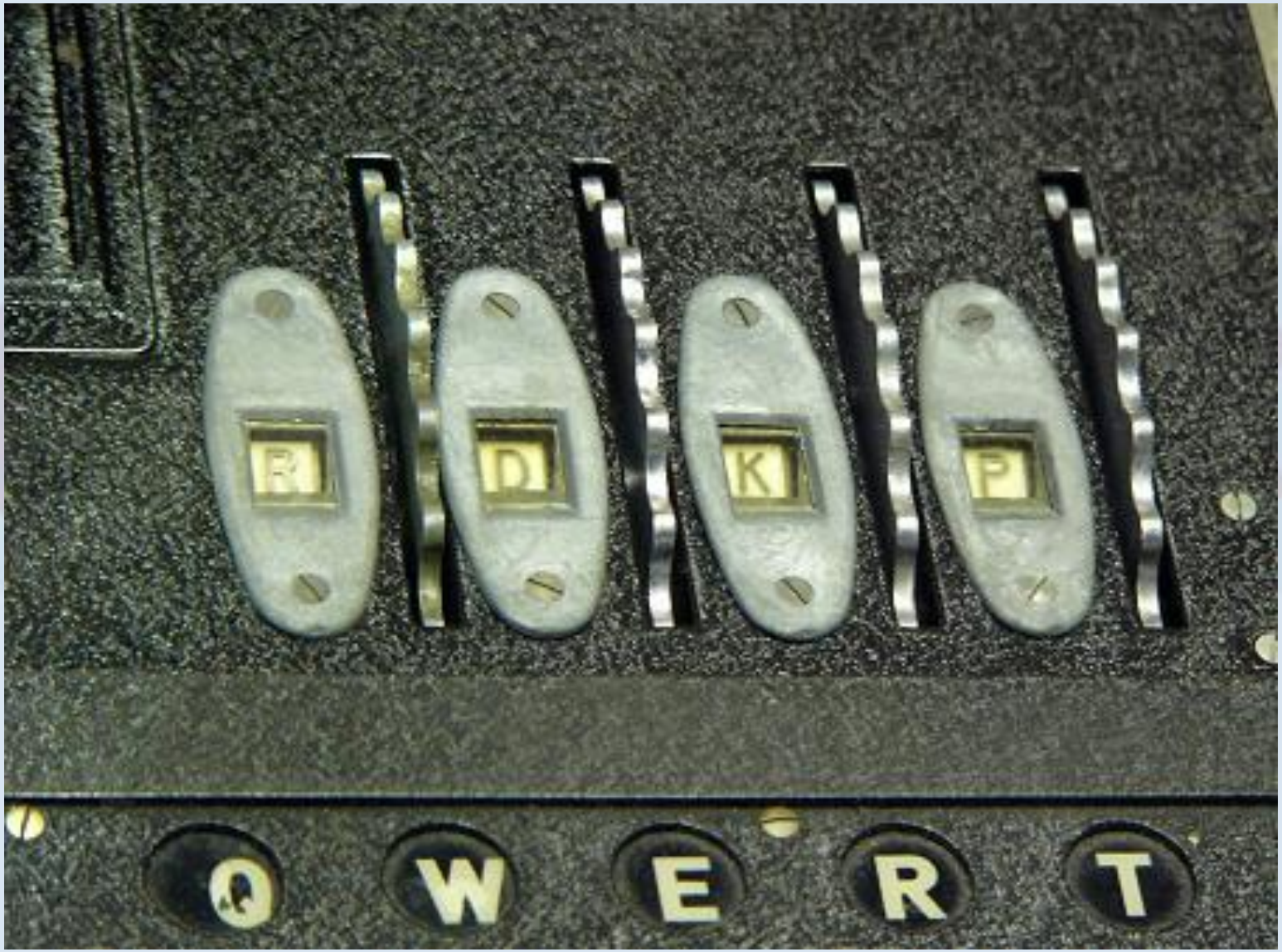
- Winston Churchill called the cracking of the German Enigma codes “the secret weapon that won the war.”
- The intelligence discovered by reading the German’s Enigma traffic—codenamed “Ultra” by the British—was decisive throughout the war. Ultra led to victories in the U-Boat struggle and the battles against Rommel in North Africa.

Description of the Enigma Machine

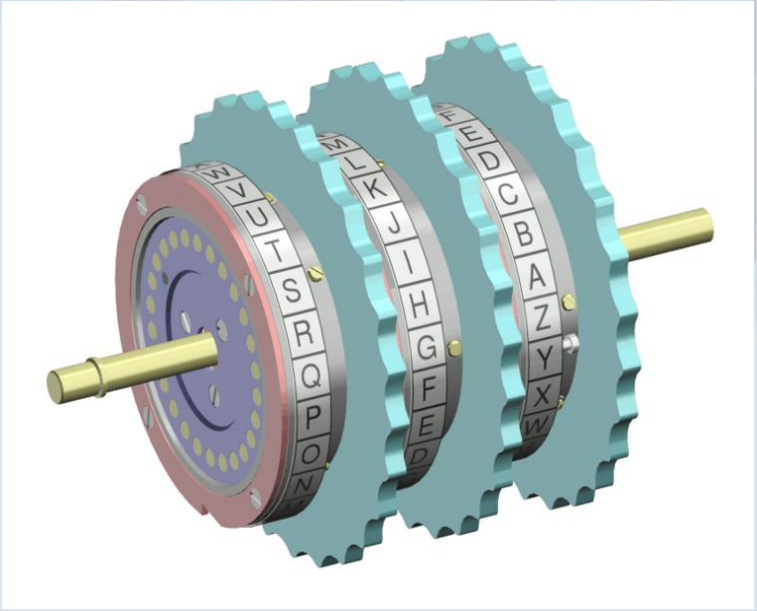


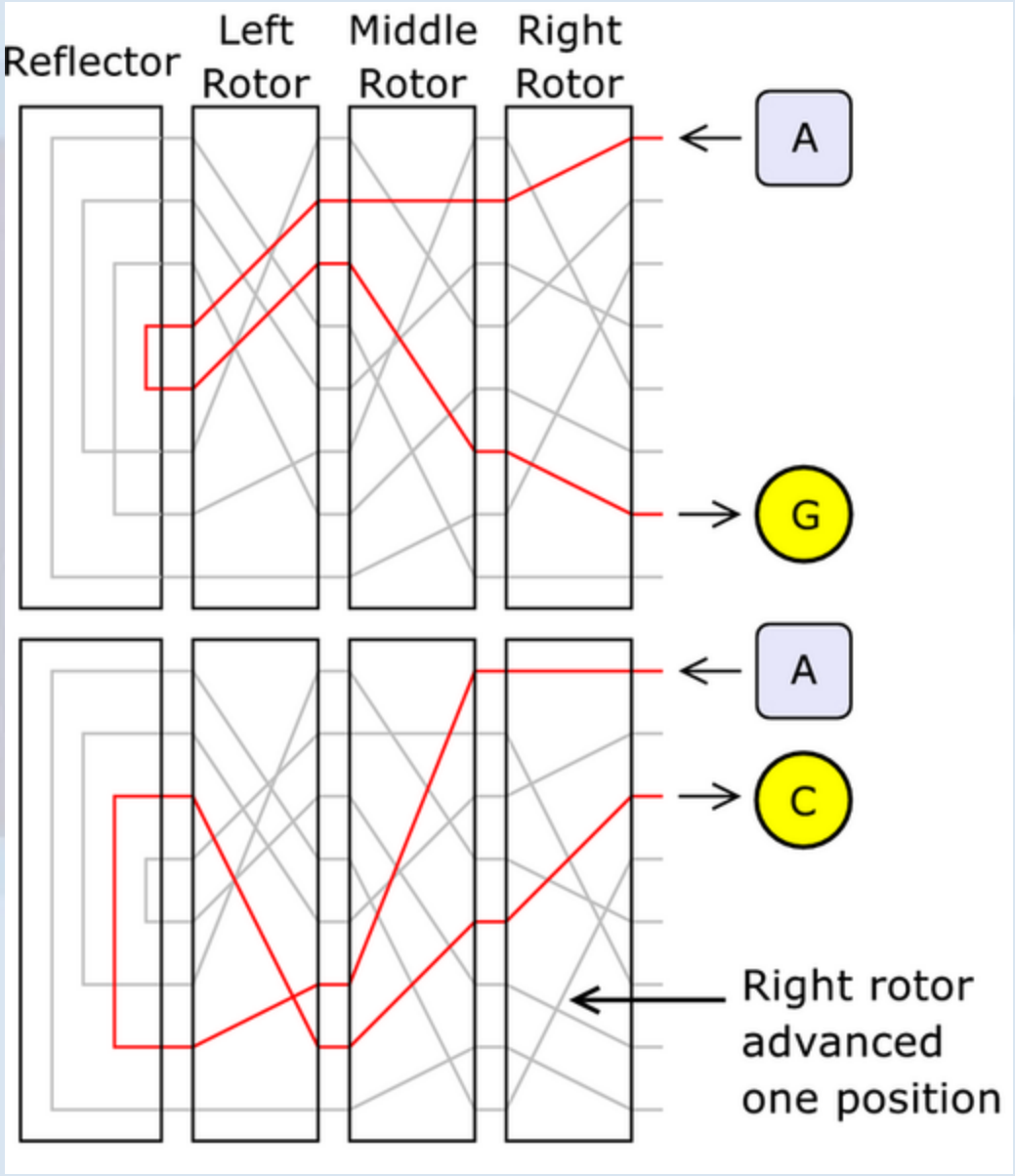
- The Enigma used 3 rotors to scramble the plaintext. The Enigma operator typed a letter on the keyboard and wrote down the letter that was lit on the lamp board.

Close-up of Rotor Window



Enigma Rotors





Enigma Flaws

- The Enigma machine had only one design weakness. A letter would never be encrypted as itself. E.g. ‘A’ would never be transposed to ‘A’.

- The German encryption procedures was the real weakness.

  Gordon Welchman: “The machine as it was would have been impregnable if it had been used properly.”

  Welchman pointed out twelve serious errors in procedure that, if corrected, would “have stopped us cold”.

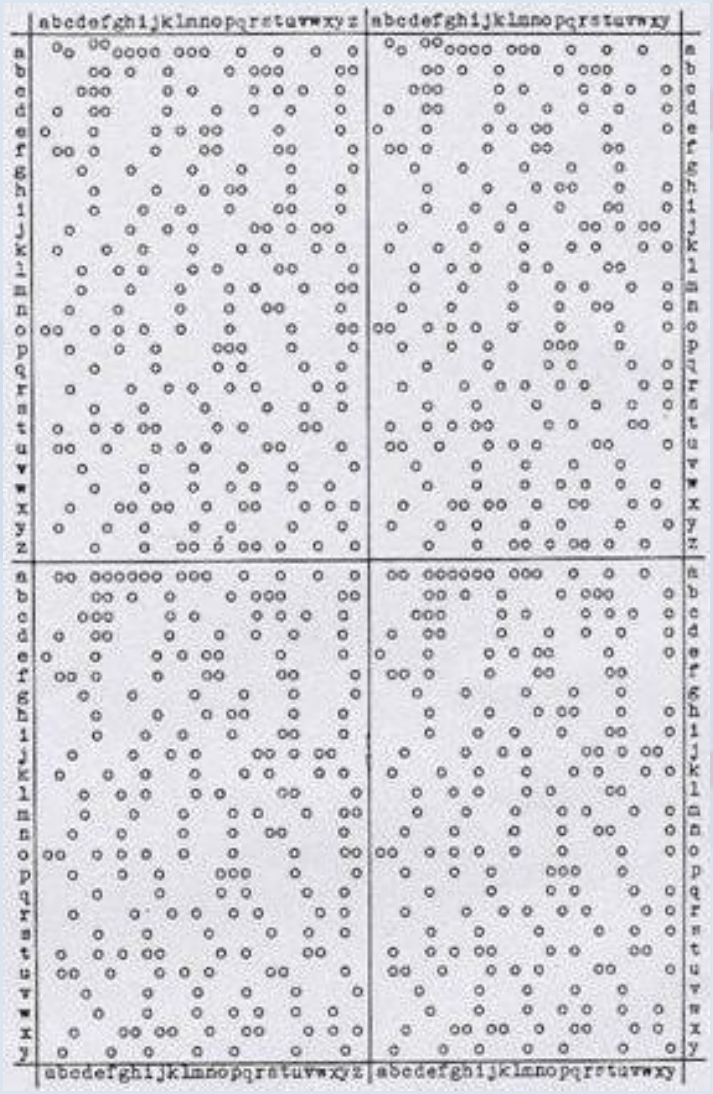
General Procedure, 1931-1940

- Clerk used codebook to retrieve settings for current month/week/day.
- First setting determined rotor order and ring settings:
  III,I, II; XAG (trigram)
- Second trigram determined the initial position of the rotors. E.g. FJI
- Clerk would choose a third trigram randomly, type it in **twice** and write down the results.
  Clerk chooses: QOP
  Output: UMHWGB
  These six letters were sent at the beginning of the message.
- Clerk would then change the rotors to match his random trigram (QOP in the example) and encrypt the rest of the message.

Exploiting the Flaw

- The stupidity of this is stunning. Every message had three pairs of letters that were the same!
- In 1933 the Polish Cipher Bureau, led by mathematician Marian Rejewski, began to break Enigma messages.
- Rejewski looked for messages with repeated pairs of letters, called “indicators”.
  Example: “RXW RAP”
- Built a catalog of rotor settings that could create different indicators.
- Each indicator reduced the number of possible rotor settings by roughly 40%.

Perforated Sheets



- By 1938 the size of the indicator catalog was becoming sizable. Henryk Zygalski designed perforated sheets that helped sort through the known indicators. When a message with an indicator was found, a sheet was stacked on top of other sheets on a glass table with a light underneath. Anywhere that light shown through was a possible solution.

Polish Bombe

- The PCB designed machines, called “Bombe” by the British, to take the possible solutions and run through them mechanically.
- In 1938, using the sheets and the bombe, the Poles were reading 70% of Enigma traffic.

British version of the bombe

Poles Reveal All to Allies

- Later in 1938 the Germans added two more rotors to the original set of three. Three were still used in the Enigma but the permutations of the rotors increased from 6 to 60. The PCB didn't have the resources to deal with the added complexity.
- The Poles invited Britain and France to a meeting in Warsaw in July '39. Neither ally had had a single success in cracking Enigma. PCB provided them with replica Enigma machines and instructions on how to create the sheets.
- Britain read its first Enigma message in January, 1940.

The Germans Wise Up…Sort Of

- In May, 1940, Germany changed its encoding procedures to eliminate the repeating of the random trigram.
- Britain's codebreakers, located in Bletchley Park (BP) were no longer able to read messages but this time they knew it could be accomplished!
- Germans didn't eliminate other practices.

Cribs

- Alan Turing and Gordon Welchman improved the bombe to work faster but it needed plaintext to compare to ciphertext.
- Turing came up with the idea of “cribs”, plaintext that was thought to be contained in a ciphertext. An example is a weather report. Past decrypts provided the cribs.
- The flaw in the Enigma machine (letters are never transposed to themselves) helped codebreakers look for cribs.

Narrowing Down the Possibilities

- Even Turing's bombe would take too long if it had to run through all permutations. Something else was needed to rule out as many as possible.
- Many clever little tricks.
- "Herivel Tip": Cryptologist John Herivel realized that lazy clerks would choose a random trigram that was very close to the ring settings.

Conclusion

- By end of the war BP could read almost all Enigma messages within a few hours.
- Around 500K total messages read.
- Germany never realized its secrets were compromised, possibly because of “aggressive” mentality.
- Side topics: French Enigma spy; U-Boat captures; giving Ultra intelligence to Russia without revealing the source.
- Wikipedia has a lot of information.