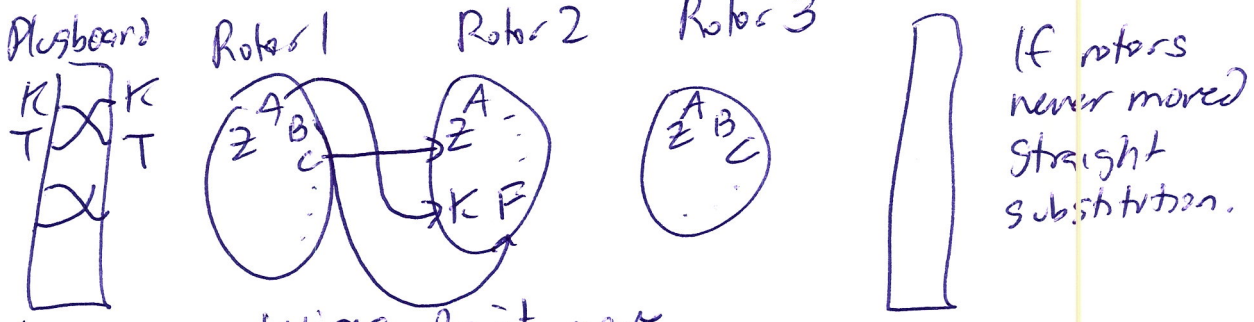
ENIGMA

Code Book - Simon Singh
Cht 3 - Details of Enigma
Cht 4 - How Enigma was Broken

ADFGVX - Germans used in WWI

→ Machine (Must faster than humans, slower than a modern day computer)

Arthur Scherbius created Enigma. ~ 1919
(initially private used)



rotors are like wheels on an odometer!

After encrypting a single letter, ROTOR 3 rotates 1 position. If it loops back to A, Rotor 2 rotates 1 pos. If Rotor 2 gets back to A, Rotor 1 rotates 1 position

Rotors have $26 \times 26 \times 26 = 17,536$ possible positions.

Reflector was added so no letter encrypts as itself. Rotors ordered in 6 ways
Total Config = $6 \times 26^3 = 102,$...

9/25/19 ②

After WWI, French, Polish has a peace time pact to share intelligence info.

French secret agent → obtained Enigma blueprint.

Hans Thilo-Schmidt (worked w/Enigma).

french → w/blueprints thought it was way too hard to break

french → gave info Polish

1929-~~B~~ 1932

Marian Rejewski mathematician

Figure 39 An army Enigma machine ready for use.

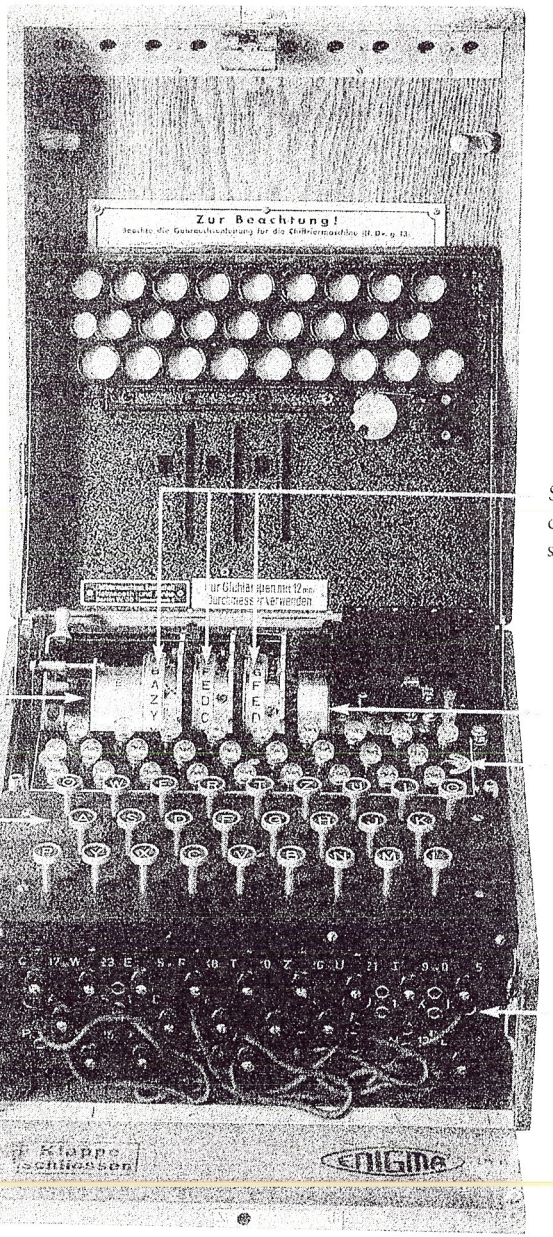


Figure 40 An Enigma machine with the inner lid opened, revealing the three scramblers.

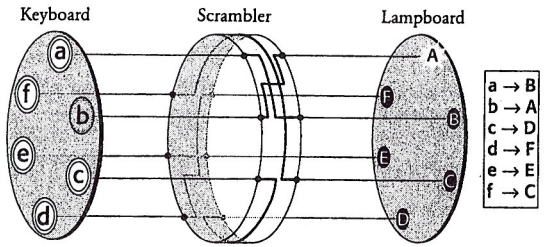


Figure 33 A simplified version of the Enigma machine with an alphabet of just six letters. The most important element of the machine is the scrambler. By typing in **b** on the keyboard, a current passes into the scrambler, follows the path of the internal wiring, and then emerges so as illuminate the **A** lamp. In short, **b** is encrypted as **A**. The box to the right indicates how each of the six letters is encrypted.

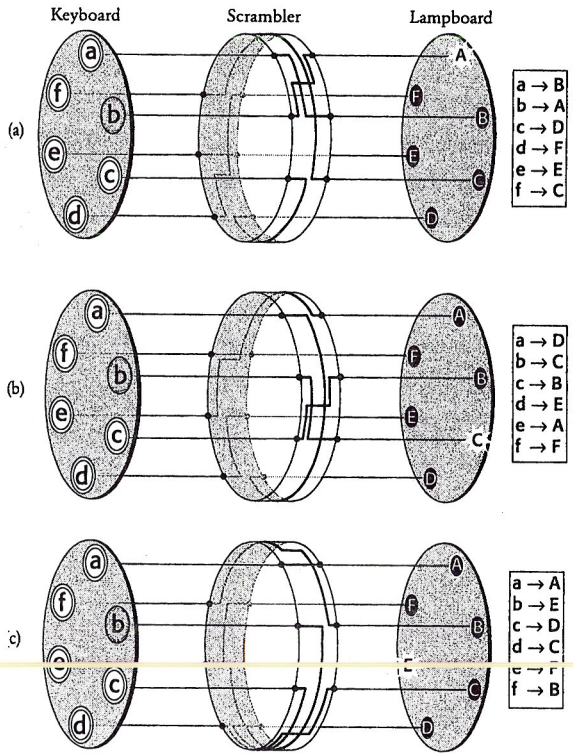


Figure 34 Every time a letter is typed into the keyboard and encrypted, the scrambler rotates by one place, thus changing how each letter is potentially encrypted. In (a) the scrambler encrypts **b** as **A**, but in (b) the new scrambler orientation encrypts **b** as **C**. In (c), after rotating one more place, the scrambler encrypts **b** as **E**. After encrypting four more letters, and rotating four more places, the scrambler returns to its original orientation.

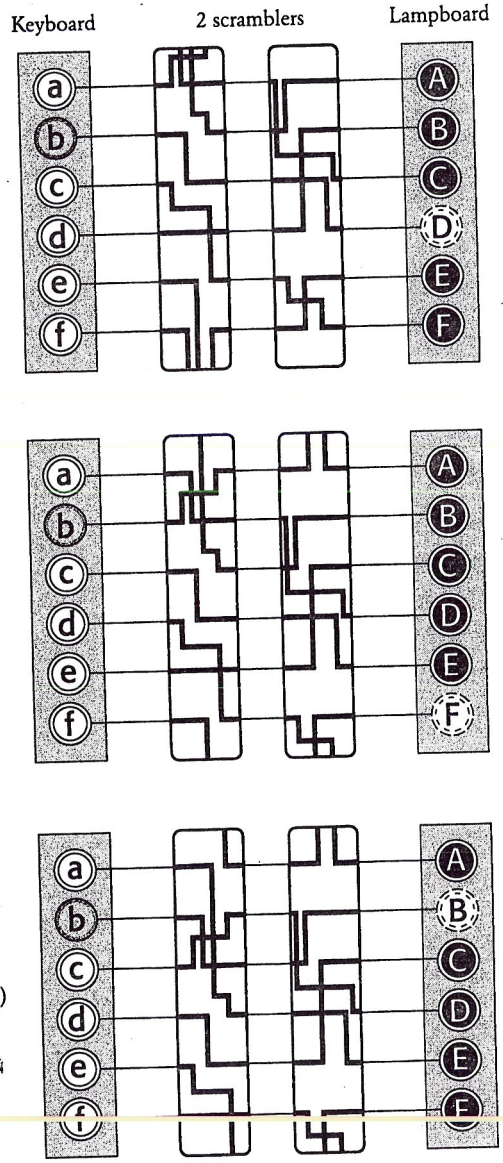


Figure 35 On adding a second scrambler, the pattern of encryption does not repeat until 36 letters have been enciphered, at which point both scramblers have returned to their original positions. To simplify the diagram, the scramblers are represented in just two dimensions; instead of rotating one place, the wirings move down one place. If a wire appears to leave the top or bottom of a scrambler, its path can be followed by continuing from the corresponding wire at the bottom or top of the same scrambler. In (a), **b** is encrypted as **D**. After encryption, the first scrambler rotates by one place, also nudging the second scrambler around one place–this happens only once during each complete revolution of the first wheel. This new setting is shown in (b), in which **b** is encrypted as **F**. After encryption, the first scrambler rotates by one place, but this time the second scrambler remains fixed. This new setting is shown in (c), in which **b** is encrypted as **B**.

that six pairs of letters could be swapped, leaving fourteen letters unplugged and unswapped. The letters swapped by the plugboard are part

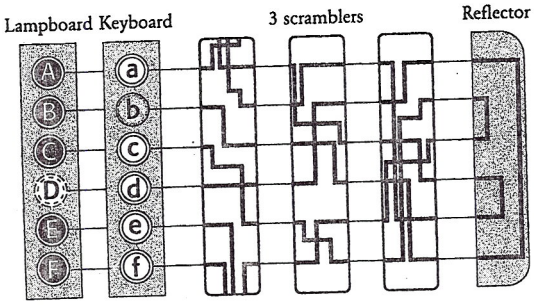


Figure 36 Scherbius's design of the Enigma included a third scrambler and a reflector that sends the current back through the scramblers. In this particular setting, typing in b eventually illuminates D on the lampboard, shown here adjacent to the keyboard.

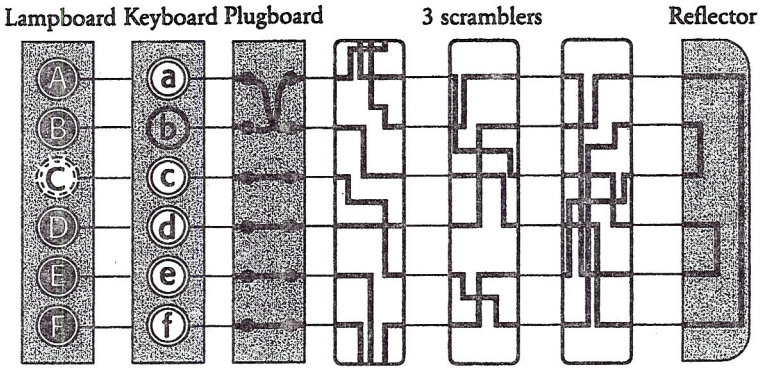


Figure 37 The plugboard sits between the keyboard and the first scrambler. By inserting cables it is possible to swap pairs of letters, so that, in this case, b is swapped with a. Now, b is encrypted by following the path previously associated with the encryption of a. In the real 26-letter Enigma, the user would have six cables for swapping six pairs of letters.