



# Enigma és kódfejtés

Tihanyi Bence



# Az Enigma Története

- Az **Enigma** üzenetek titkosítására használt, forgótárcsás, elektromechanikus berendezés.
- Görög eredetű szó, jelentése: rejtély, rejtvény.
- **Arthur Scherbius** német mérnök fejlesztette ki az első világháború végén.
- 1920-tól kereskedelmi forgalomban
- Először **Marian Rejewski** legynel matematikus által vezetett csoport törte fel 1932-ben

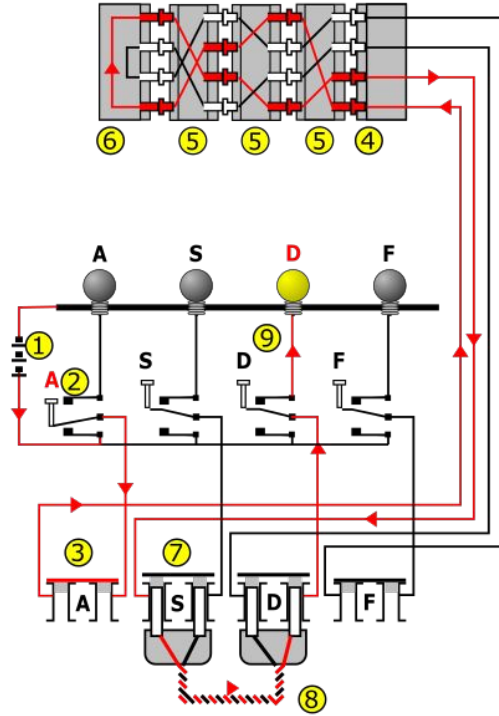


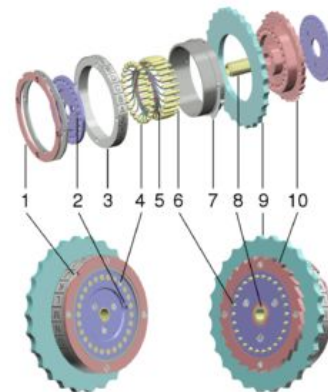
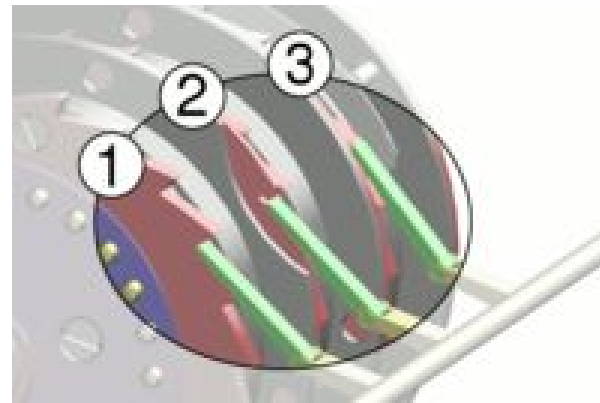
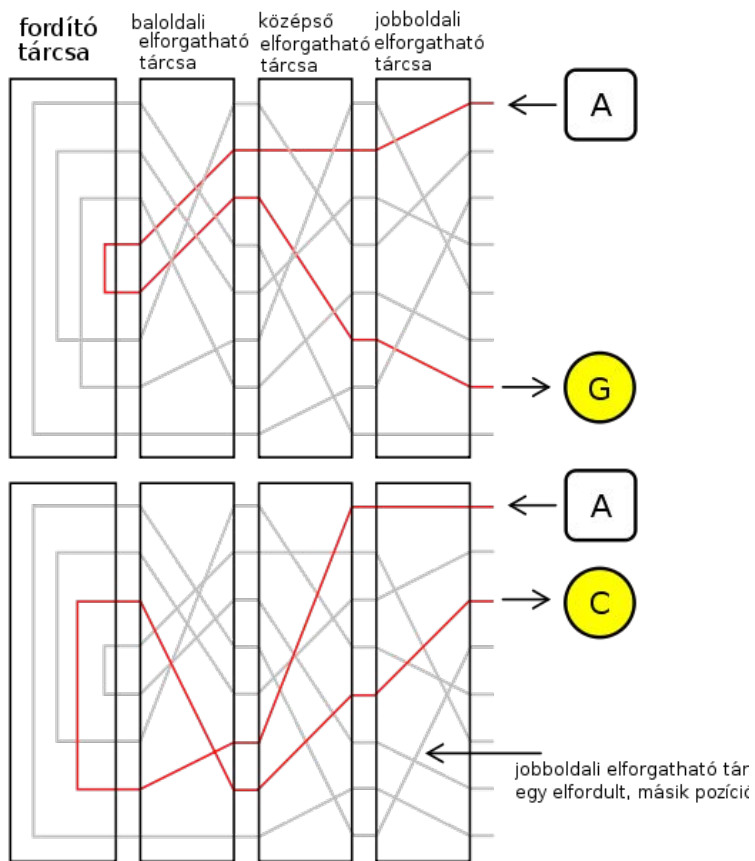
# Az Enigma Története

- A második világháború során a németek használták több különböző verzióját
- **1940-től Alan Turing vezetésével** Bletchley Parkban állomásozó szövetséges csoport törte fel újra
- Becslések szerint Turing munkája Európában mintegy 2 évvel rövidítette le a háborút

# Felépítése









$$\frac{1}{n!} \prod_{i=1}^n \frac{(26 - 2i + 2)(26 - 2i + 1)}{2} = \frac{26!}{2^n \cdot n! \cdot (26 - 2n)!}$$

Az első években hat, később öt-nyolc átkötést használtak, de 1939-től mindig tízet. Ezzel: 150 738 274 937 250 lehetőség adódik. A kettes számrendszerhez alkalmazkodva: közelítőleg  **$2^{47}$  lehetőség**.

---

# Feltörése



# Feltörése

- A lehetséges kulcsok számának csökkentésén alapult
- 27 betűs szövegben a nem ütközések számának várható

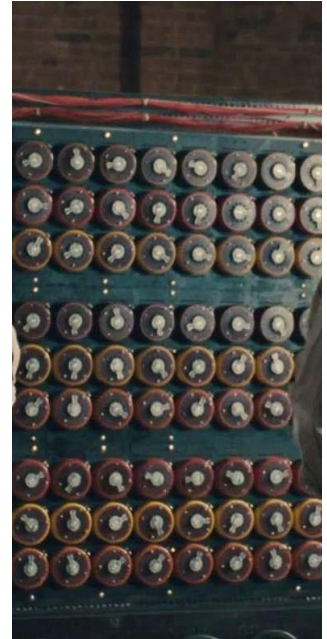
értéke 26 elemű abc, és 27 betűs szöveg, és 24 betűs

szó esetén:  $27 * (1 - \frac{1}{26})^{24}$

```
BHNCXSEQKOBIIODWFBTZGCEYHQJEWYOYNBDXHQBALHTSSDPWGW
1 OBERKOMMANDODERWEHRMACHT
2 OBERKOMMANDODERWEHRMACHT
3 OBERKOMMANDODERWEHRMACHT
4 OBERKOMMANDODERWEHRMACHT
5 OBERKOMMANDODERWEHRMACHT
6 OBERKOMMANDODERWEHRMACHT
7 OBERKOMMANDODERWEHRMACHT
8 OBERKOMMANDODERWEHRMACHT
9 OBERKOMMANDODERWEHRMACHT
10 OBERKOMMANDODERWEHRMACHT
11 OBERKOMMANDODERWEHRMACHT
12 OBERKOMMANDODERWEHRMACHT
13 OBERKOMMANDODERWEHRMACHT
14 OBERKOMMANDODERWEHRMACHT
15 OBERKOMMANDODERWEHRMACHT
16 OBERKOMMANDODERWEHRMACHT
17 OBERKOMMANDODERWEHRMACHT
18 OBERKOMMANDODERWEHRMACHT
19 OBERKOMMANDODERWEHRMACHT
20 OBERKOMMANDODERWEHRMACHT
21 OBERKOMMANDODERWEHRMACHT
22 OBERKOMMANDODERWEHRMACHT
23 OBERKOMMANDODERWEHRMACHT
24 OBERKOMMANDODERWEHRMACHT
25 OBERKOMMANDODERWEHRMACHT
26 OBERKOMMANDODERWEHRMACHT
27 OBERKOMMANDODERWEHRMACHT
BHNCXSEQKOBIIODWFBTZGCEYHQJEWYOYNBDXHQBALHTSSDPWGW
```

# Feltörése

- A Turing bomba segítségével percenként  $26 \cdot 120$  lehetőséget tudtak kipróbálni.
- A háború végére csak Nagy-Britanniában ~210 Turing-bombát üzemeltettek
- Percek alatt tudták feltörni a kódokat.



Turing-bomba



# Források

- [https://en.wikipedia.org/wiki/Enigma\\_machine](https://en.wikipedia.org/wiki/Enigma_machine)
- [https://en.wikipedia.org/wiki/Alan\\_Turing](https://en.wikipedia.org/wiki/Alan_Turing)
- <https://en.wikipedia.org/wiki/Cryptography>
- [https://en.wikipedia.org/wiki/Cryptanalysis\\_of\\_the\\_Enigma](https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma)
- [https://people.physik.hu-berlin.de/~palloks/js/enigma/enigma-m4\\_v16\\_en.html](https://people.physik.hu-berlin.de/~palloks/js/enigma/enigma-m4_v16_en.html)