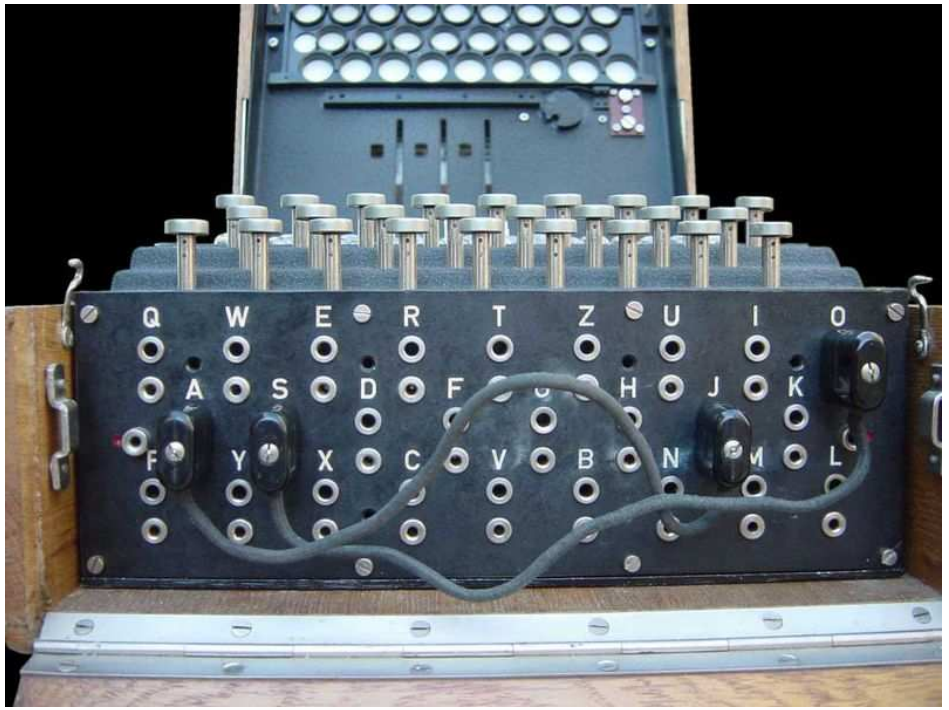
# Rotor machines and Enigma

Presented by
Michael Maurer

# German Enigma



# Overview

- Historical background
- Functionality
- Problems and Weaknesses
  - Reflector
  - Kerckhoff’s principle
- Breaking Enigma
  - Index of Coincidence
  - Bletchley Park

# Historcal background

- 1920s: need for mechanical encryption device
- Ideal solution: rotation of a substitution cipher
- Machines to **increase efficiency**
- 1917: American Edward Hebern: cipher machine with rotating disks
- 1918: German electric engineer **Albert Scherbius** patented rotor cipher machine, predecessor of Enigma
- 1923: first cipher machine Enigma A
- First on exhibitions for civil causes, later „**Wehrmacht**“ showed interest
- 1926: commercial Enigma purchased by „Wehrmacht“

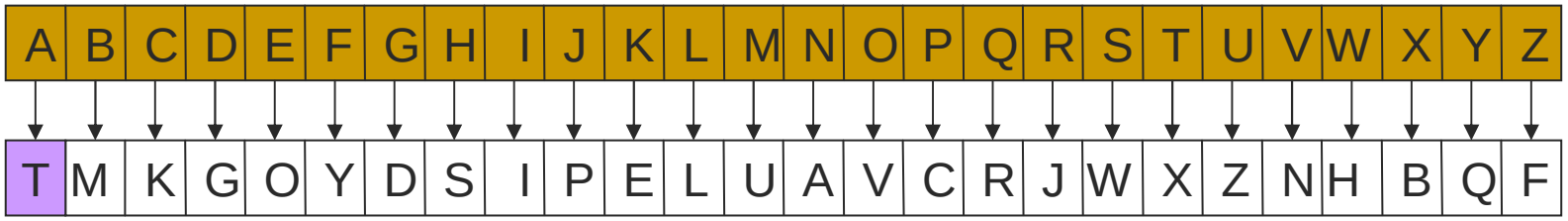
⇨ Enigma totally **vanished from civil market**

# Functionality

- Several rotors: all 26 letters of alphabet
- Rotors connected by wires ➡ encryption mechanically over electrical circuit
- After each encryption of single letter: one rotor rotated ➡ new encryption cipher obtained

After encryption of 1st letter, rotor rotated by one position

Rotor to produce the substitutions is given by



# Functionality Enigma

**Rotors:**

- 3 out of 5: Order important: 5*4*3 = 60
- Initial starting position: $26^3 = 17576$
- Stepping of rotors controlled by rings hitting notches
- ring positions: $26^2 = 676$

**Reflector:** en- and decryption

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X | R | E | G | C | Y | D | S | P | Q | L | K | U | Z | V | I | J | B | H | W | M | O | T | A | F | N |

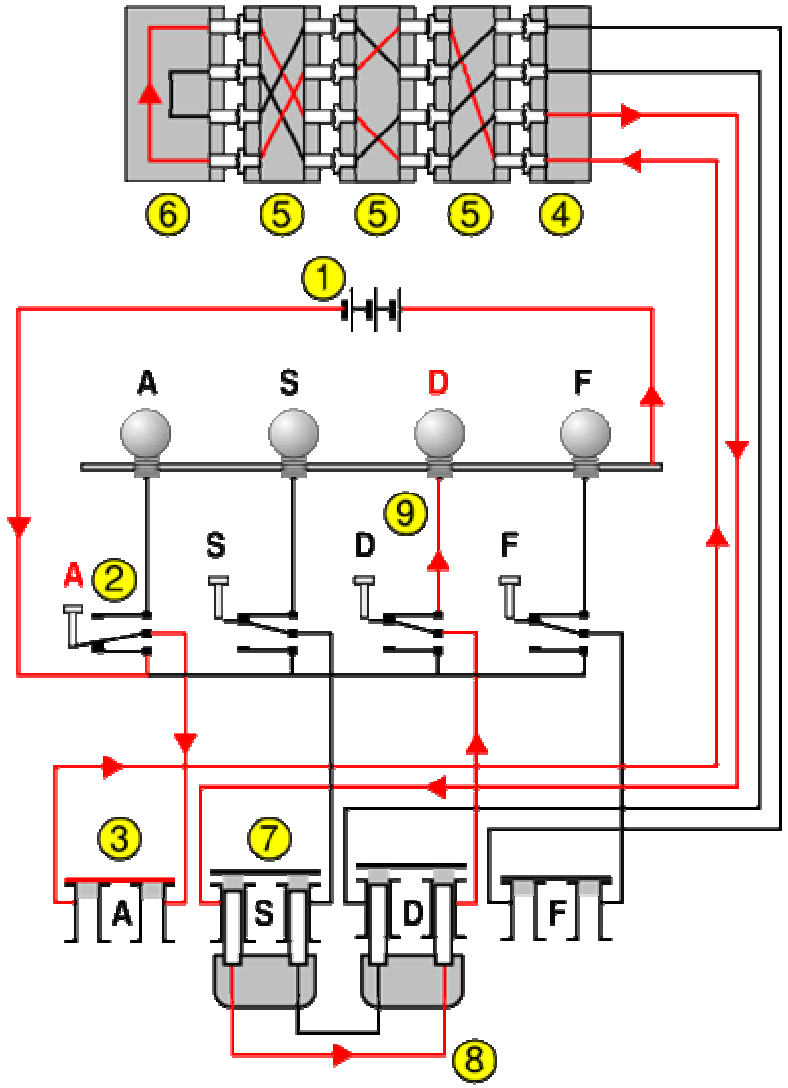
**Plug board:** swap letters twice: $10^{14}$ possible keys

➡ **total number of keys ≈ $2^{75}$**

# Functionality Enigma

**Assembly of Enigma:**

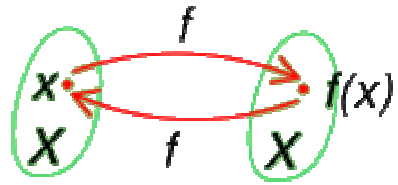
- Battery (1)
- Keyboard(2)
- Plugboard(3, 7, 8)
- Wired rotors (4, 5, 6)
- Lamps (9)



# Problems and Weaknesses

**Reflector weakens Enigma:**

- Function: no difference between en- and decryption
- **Problem1:** encryption becomes **involutary**,
  means: If K⟶T, T⟶K




- **Problem2:** none letter is encrypted by itself, because electricity can‘t go same way back

➡ Heavy Reduction of encryption alphabet

# Problems and Weaknesses

**Kerckhoff‘s principle:**

*The security of a system should not depend on the privacy of the algorithm. It should only be based on the secrecy of the key.*

**Contradiction to Kerckhoff:**

- Security of Enigma depended on wiring of rotors
- Wiring was part of algorithm, not part of key
- Wiring never changed from 1920s until 1945

# Breaking Enigma

**Index of Coincidence:**

$$IC(x) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}$$

$x_1,\ldots,x_n$ string of letters

$f_0,\ldots,f_{25}$ frequency of the letters in that string

- Random string: IC(x) ≈ 0.038
  natural language: IC(x) ≈ 0.065
- Large single ciphertext
- Text decrypted and then IC computed
- **Wanted:** New obtained text similar to correct statistics of natural language

# Breaking Enigma

**How can IC be used for attack on Enigma?**

1. **Find the rotor order**
   - Trying all rotor orders and positions searching highest IC
   - Operations : $60*26^3 \approx 2^{20}$

2. **Approximation to rotor start positions**
   - **We have:** rotor order from step 1
   - Trying all rotor positions and ring positions for 1st ring only, again searching highest IC
   - Operations: $26^4 \approx 2^{19}$

# Breaking Enigma

3. **Find ring and rotor start positions**
   - **We have:** 1st ring and 1st rotor start positions, approximations for other rings and starting positions from 1 and 2
   - firstly: search positions for the 2nd ring and rotor, then same procedure for last remaining rotor
   - Operations: $26^2 \approx 2^9$

4. **Find the plug settings**
   - **We have:** rotor order, position and ring positions
   - IC as test statistic again
   - test statistic derived of the trigram information of the underlying language

# Breaking Enigma

**Enigma broken at Bletchley Park (BP)**

- Polish mathematician Marian Rejewski guessed correct wiring of rotors with first Enigma(1932)
- With help of „Zyklometer“ and „Bomba“ (very similar to Enigma) Rejewski found initial rotor positions
- British Alan Turing invented „Turing-Bomba“ at BP
  - Exploits involutory of Enigma
  - Build as several consecutively applied Enigmas
  - Key found by Exhaustion ( brute-force )

⇨ January 1940 Allies could break all German radio massages