# Enigma Machine

## CRIPTOGRAFIA

João Fernandes, nº49834
Tiago Costa, nº49942

# The Machine

- The Enigma machine is a series of electro-mechanical rotor cipher machines.
- Used to encrypt and decrypt war codes.
- It's fame stems from the use by the German military.

# Historical Backgraund

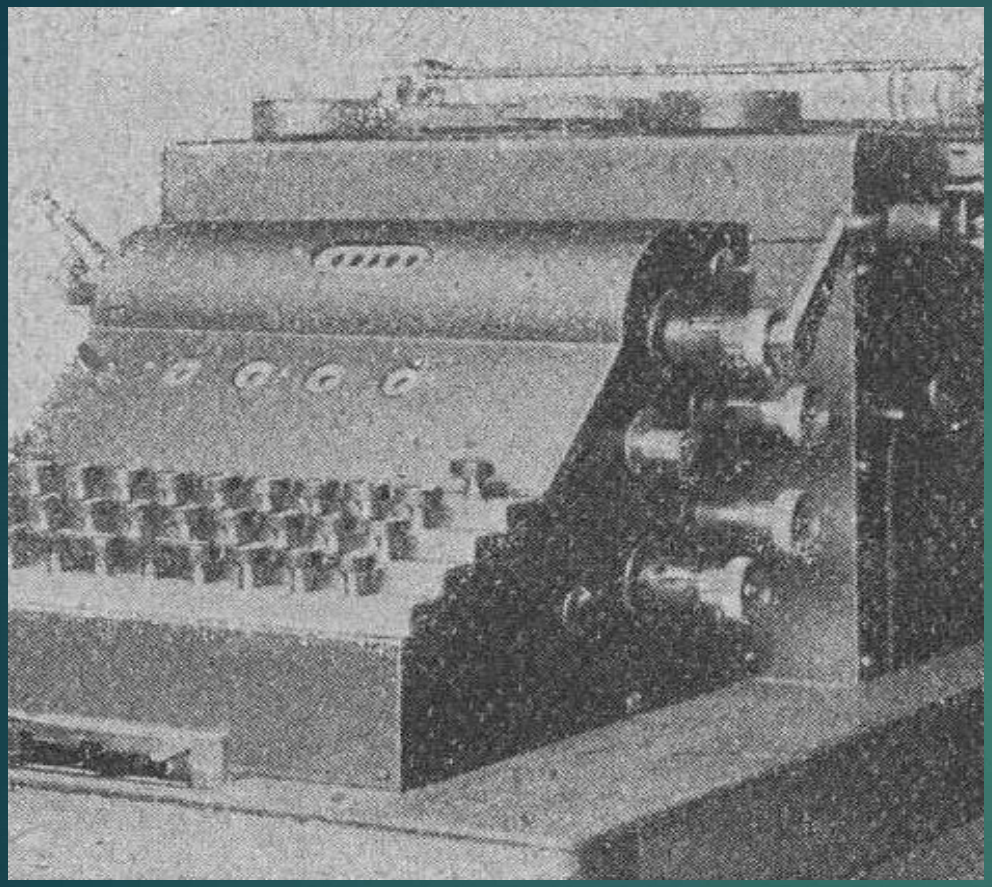
- The Enigma was patented by Arthur Scherbius in 1918.
- The first model (Enigma A) had as dimensions 65x45x35 and weighed 50 Kg.

Born: 30 October 1878, Frankfurt

Died: 13 May 1929 (aged 50), Berlin

Nationality: German

Education: Technical University Munich &
University of Hanover PhD in Engineering



Enigma A


Enigma D

# 2th World War

- During the 2th World War, the Enigma Machine was used by the Germans in:
  - Radio communications;
  - Telegraphic communications;
  - Meteorological bulletins.

- The Machine was considered unbreakable!

# The Mechanics

- http://enigmaco.de/enigma/enigma.html

# The Math Behind

- Rotor (3 of 5)
- Rotors Starting Positions
- Plugboard (20 pairs)

# The Math Behind

- mod(26)
- Symmetrical
  - Transposition;
  - Replacement.
- Key

# Crack the Code

- The code was cracked in 1933 by three polish mathematicians.

Jerzy Różycki:

Born: 24 July 1909
Olszana, Russian Empire(now Vilshana, Ukraine)

Died: 9 January 1942 (aged 32) Mediterranean Sea

Marian Rejewski:

Born: 16 August 1905
Bromberg, German Empire (now Bydgoszcz, Poland)

Died: 13 February 1980 (aged 74)
Warsaw, People's Republic of Poland

Henryk Zygalski:

Born: 15 July 1908 Posen, German Empire

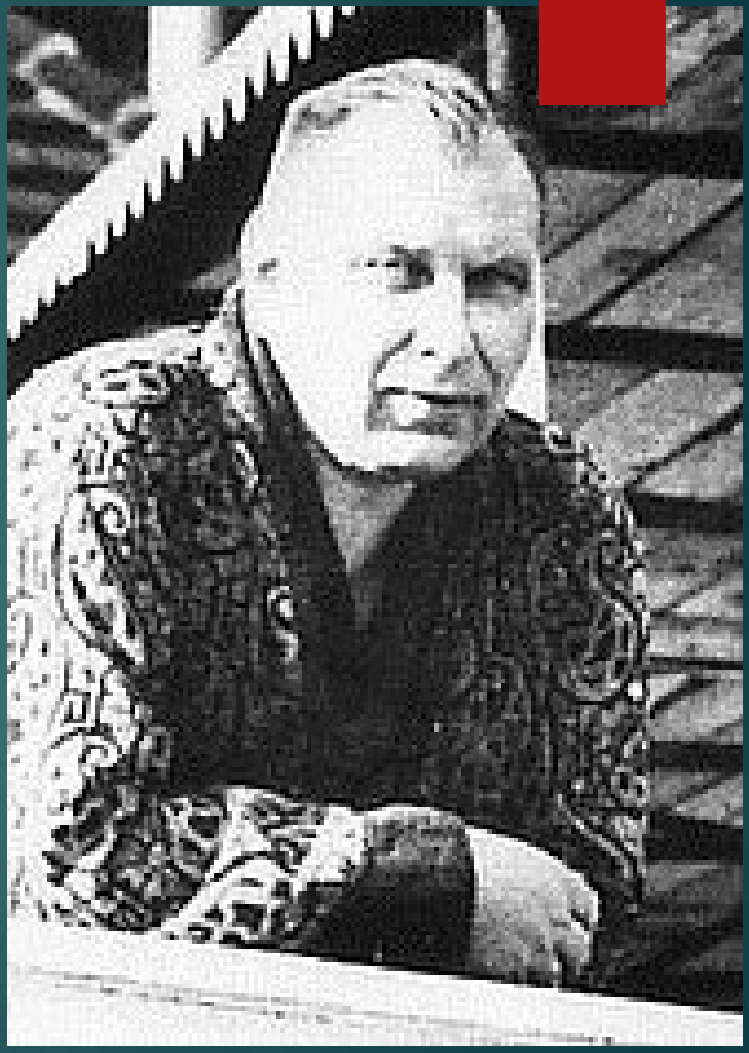
Died: 30 August 1978 (aged 70) Liss, England

# The Spy

- The French spy Hans-Thilo Schmidt obtained access to German cipher materials that included the daily keys used in September and October 1932.

Born: 18 May 1893

Died: 19 September 1943 (aged 50)
Berlin, Germany



# The Fake Enigma

- The French passed the material to the Poles, and Rejewski used some of that material and the message traffic in September and October to solve for the unknown rotor wiring.
- Consequently, the Polish mathematicians were able to build their own Enigma machines, which were called Enigma doubles.

# Counter Attack

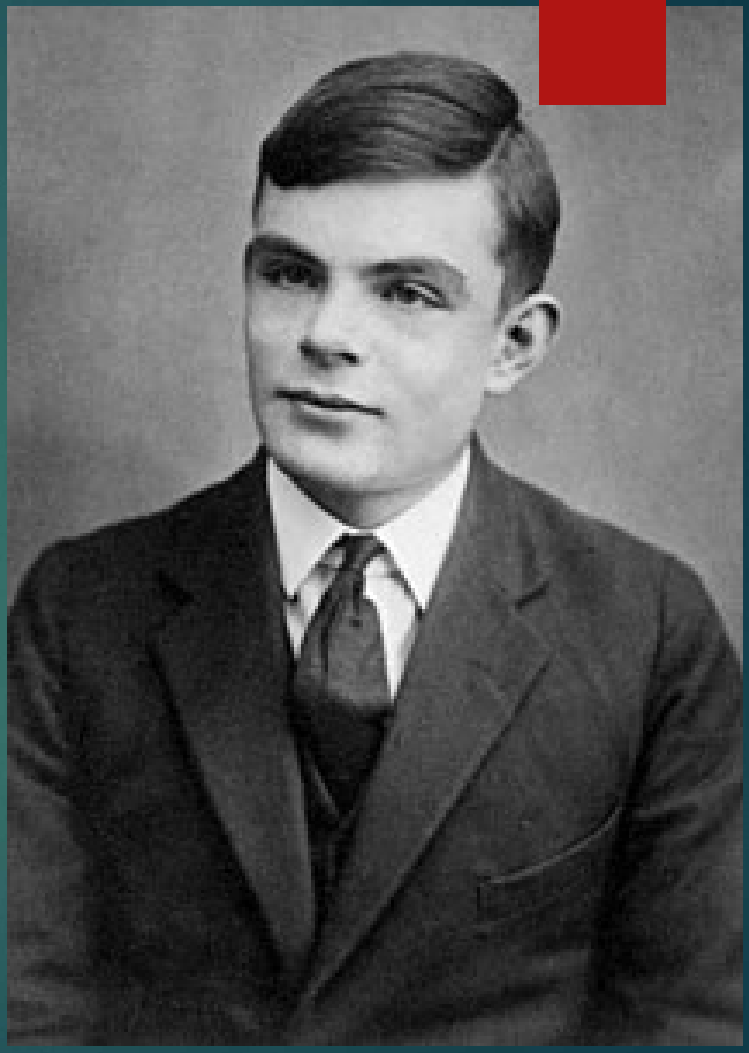
- Between 1933 and 1938, the Poles were able to follow the progress that the Germans were making to the machine.
- This was possible thanks to a machine called the Bomba.

# Alan Turing

Born: 23 June 1912, Maida Vale, London, England

Died: 7 June 1954 (aged 41), Wilmslow, Cheshire, England

Cause of death: Suicide



# Alan Turing Bombe