Enigma - Machine   Enigma M3

Enigma Simulator V7.0

101computing.net/enigma-machine-emulator

github.com/NationalSecurityAgency/enigma-simulator

piotte13.github.io/enigma-cipher

Daniel Palloks Universal Enigma   cribs

References / Bibliography / Further Reading / External Links

1931 Poland — Henryk Zygalski, Jerzy Rózycki, Marian Rejewski

1. "Reciprocal": If c → R then r → C (same wheel position)
2. "Non-crashing": A cannot encipher as A
3. Turnover notches on the alphabet rings.
4. Plugboard (6 wires in 1931)

Our clues

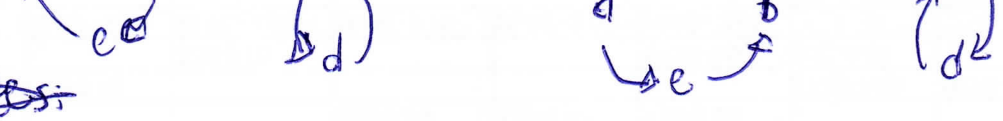
- An imperfect model: a commercial machine
- Constraint: Same machines are used to Encrypt/Decrypt
- The data: The intercepted radio traffic

Tools: Pattern searching, data mining and mathematics of group Theory

The Traffic Data — First 6 letters | Gordon Welchman

Repeats & In depth (CI)

21.39



~~As cycles:~~

As cycles: (abe) (cd)   (aeb) (cd)

As a matrix $N = \begin{pmatrix} a & b & c & d & e \\ b & e & d & c & a \end{pmatrix}$