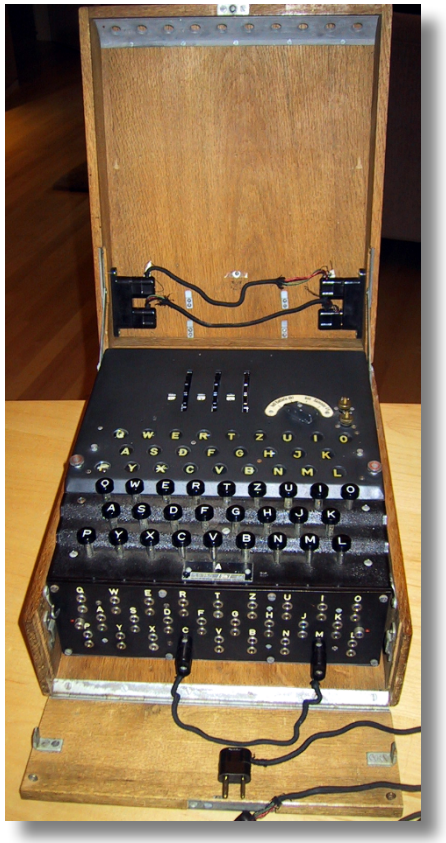


The Enigma Machine

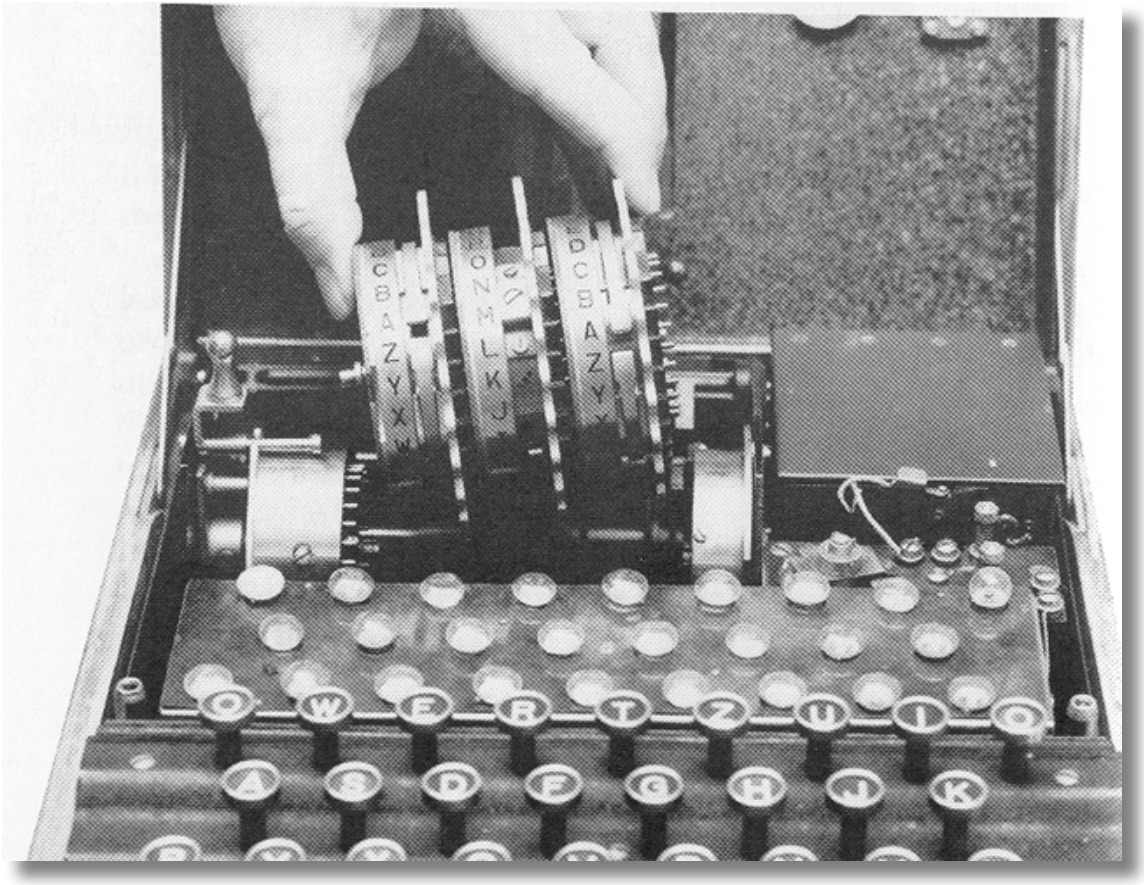
Yan Huang

History

- Invented by Arthur Scherbius, 1918
- Adopted by German Navy, 1926
- Modified military version, 1930
- Two Additional rotors added, 1938

Video from Numberphile

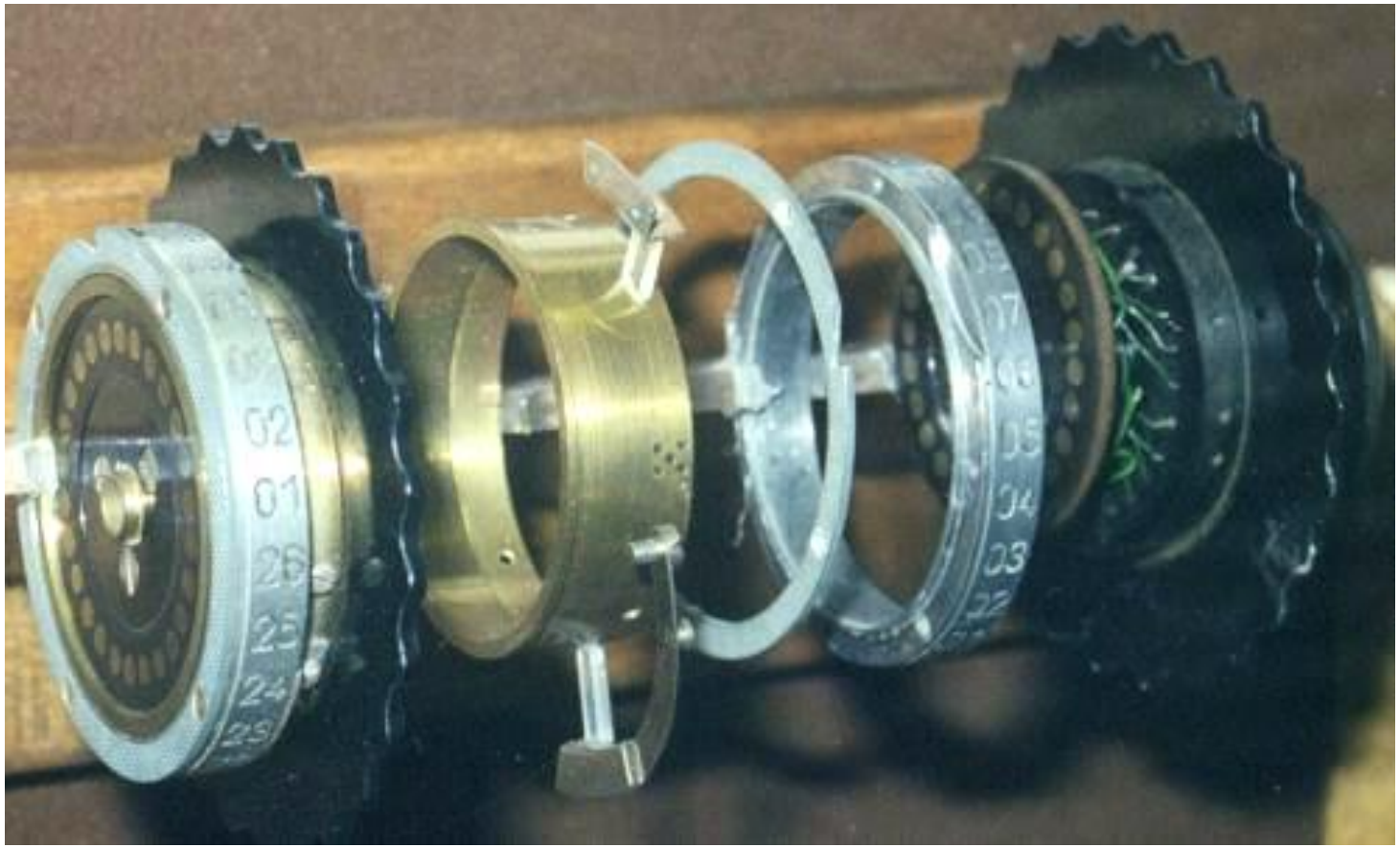
https://www.youtube.com/watch?v=G2_Q9FoD-oQ

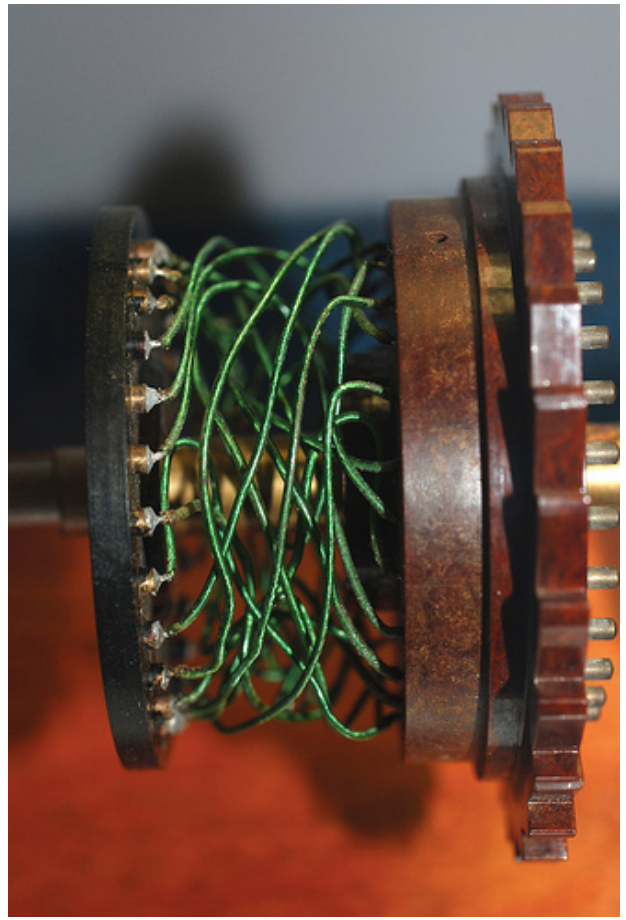


Using an Enigma

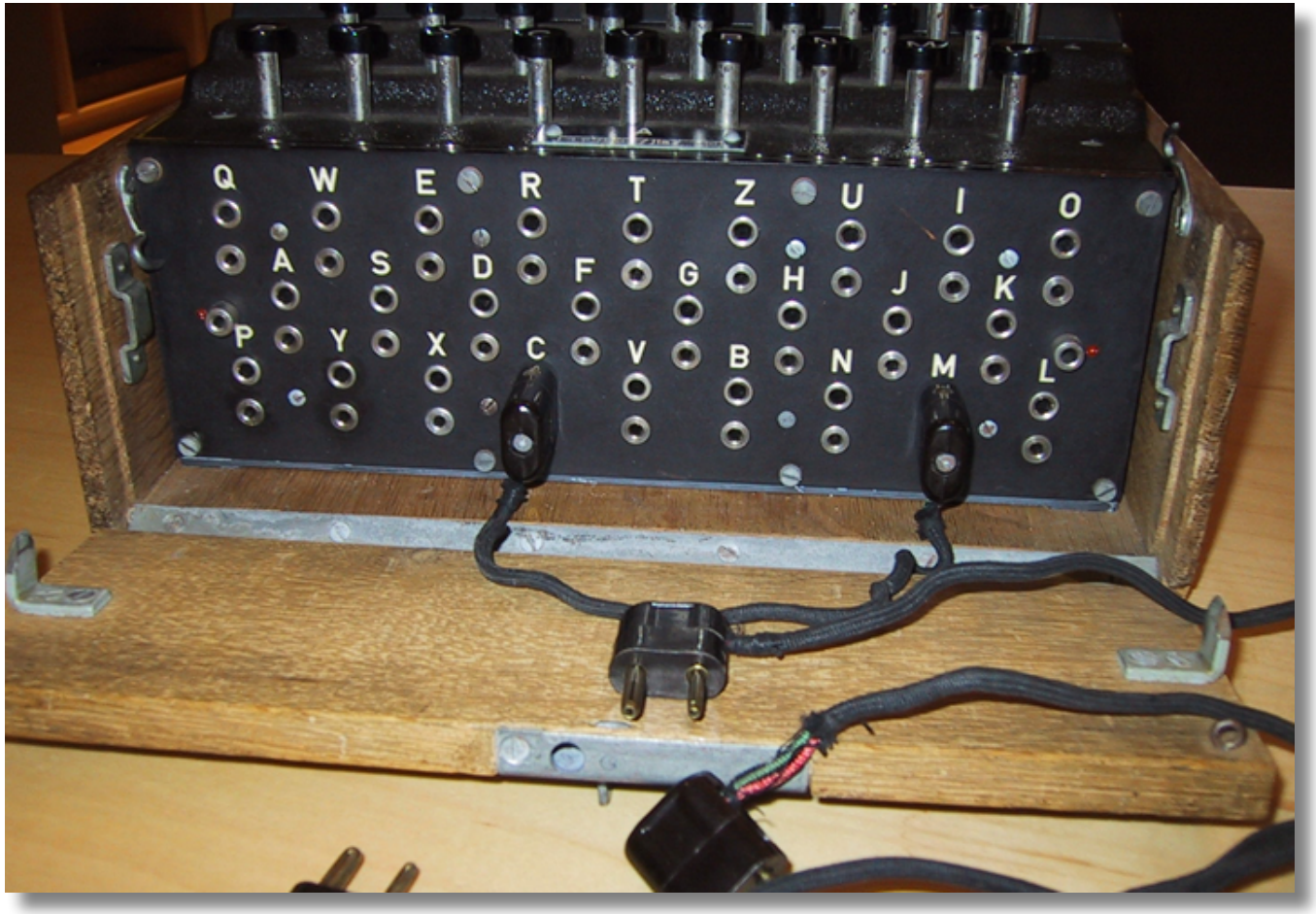
- Daily Setup
  - Secret settings distributed in code books.
- Encoding/Decoding a Message

Rotors





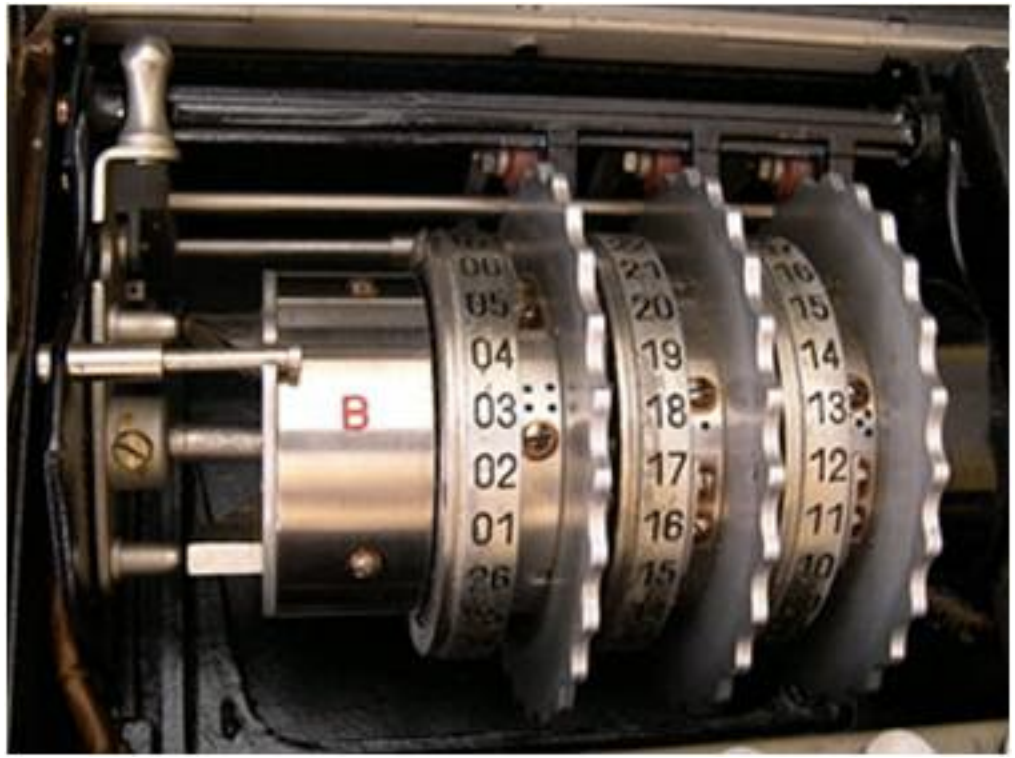
Plugboard

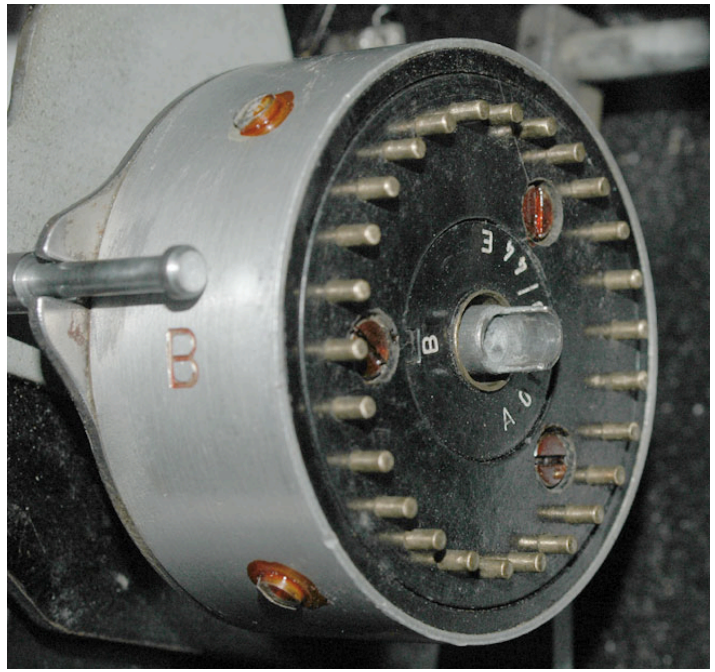


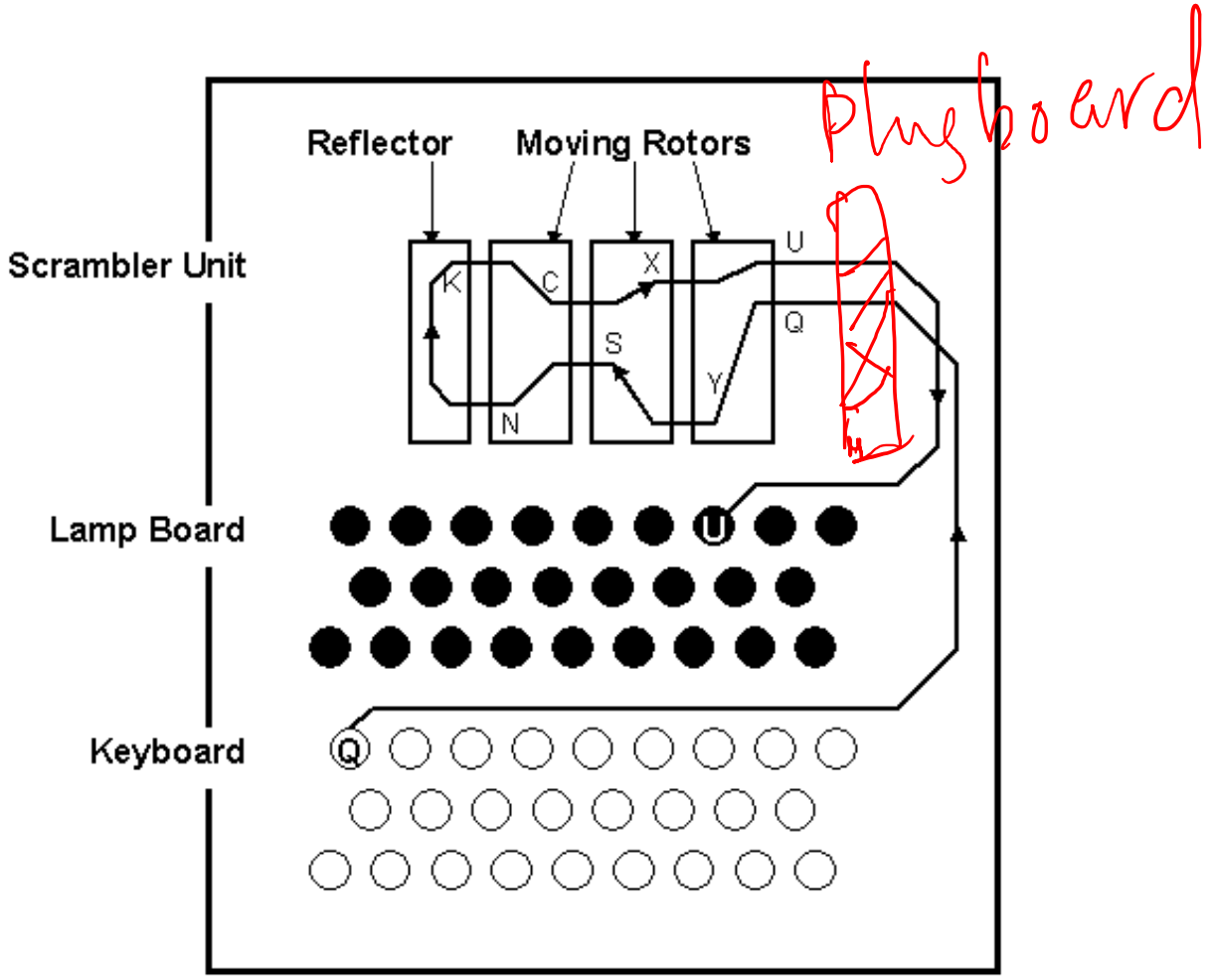
Every plug-line connects two letters.

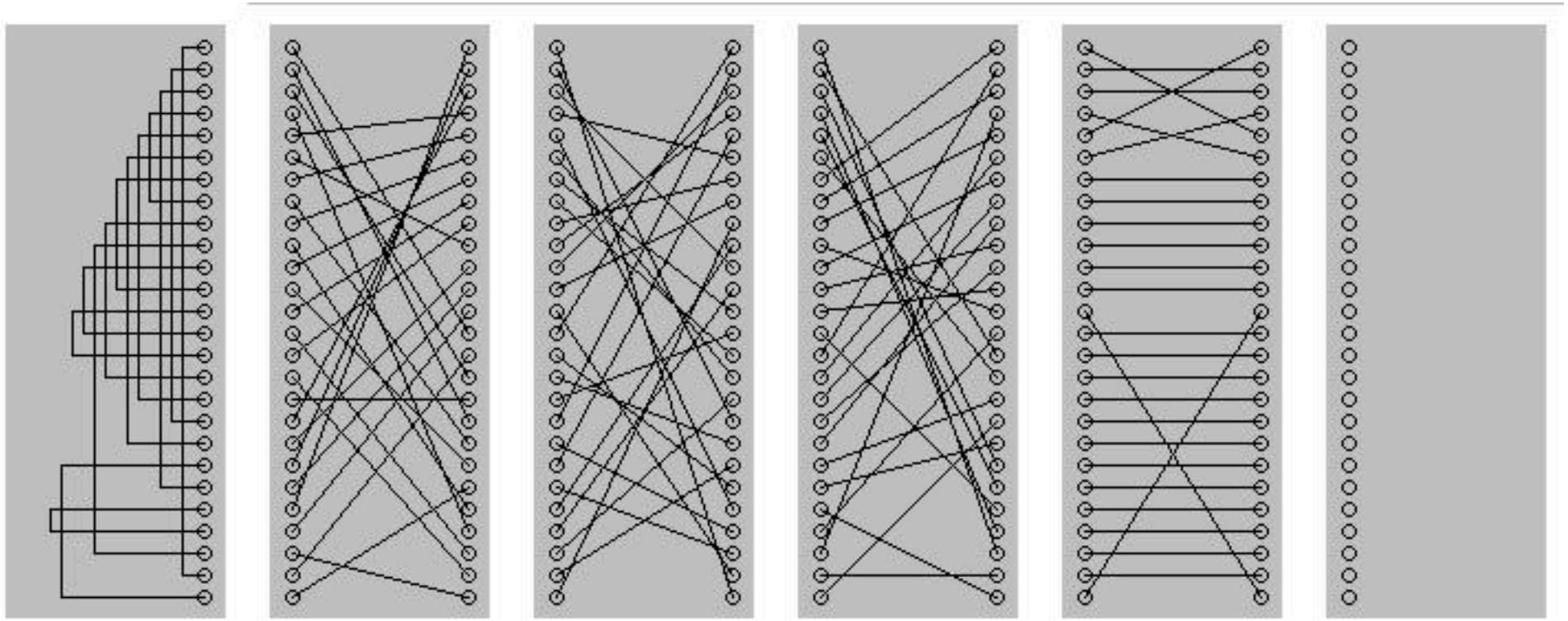
Initial Rotor Position

Reflector






Plugboard
Reflector
Moving Rotors
Scrambler Unit
K
C
X
U
Q
S
Y
N
Lamp Board
U
Keyboard
Q

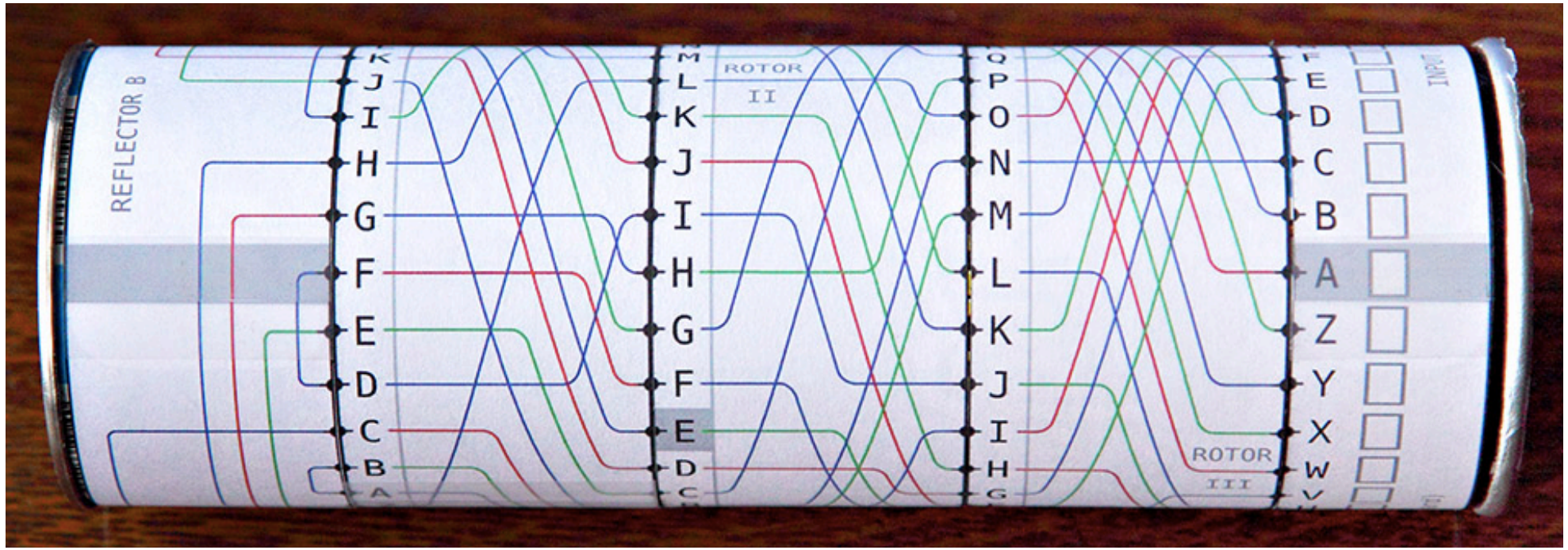


Reflector Wheel 1 Wheel 2 Wheel 3 Plugboard Keyboard & Lightboard

Implementing A Enigma Machine

- Paper Enigma

  http://wiki.franklinheath.co.uk/index.php/Enigma/Paper_Enigma



Notation for Permutations

- Consider permutations over $\{1, 2, 3, 4, 5\}$

  (1 2):

  $$1 \to 2, \quad 2 \to 1, \quad 3 \to 3, \quad 4 \to 4, \quad 5 \to 5$$

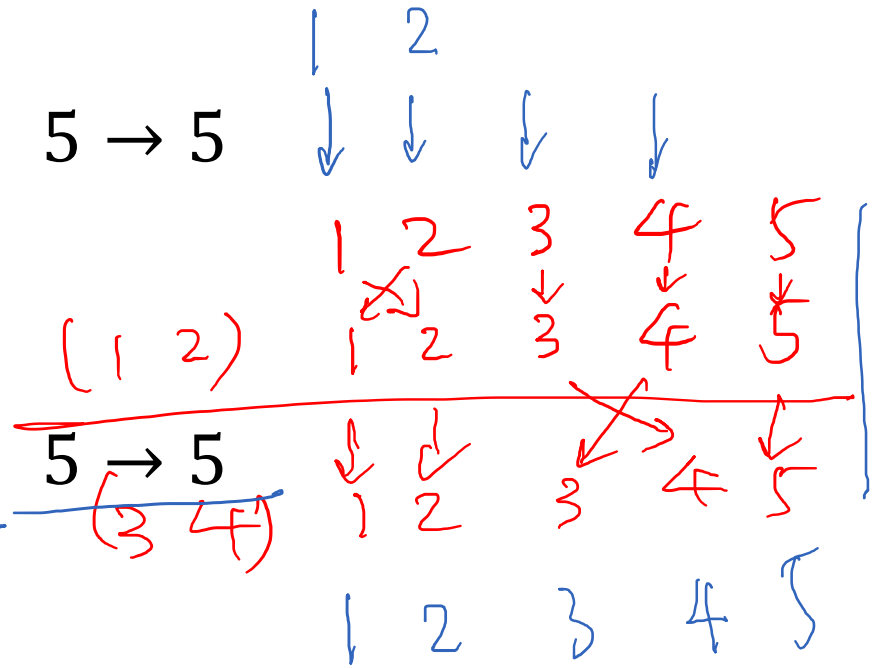
  (2 3 4):

  $$1 \to 1, \quad 2 \to 3, \quad 3 \to 4, \quad 4 \to 2, \quad 5 \to 5$$

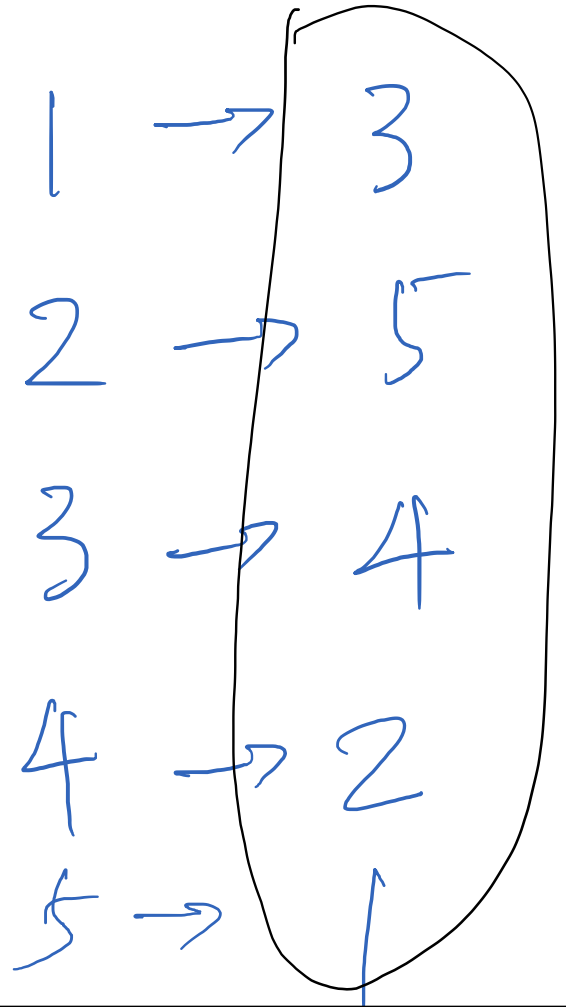
- Compose permutations

  (1 2) (3 4):

  $$1 \to 2, \quad 2 \to 1, \quad 3 \to 4, \quad 4 \to 3, \quad 5 \to 5$$



$(1\ 3\ 4)(2\ 5\ 1)$:



$(1\ 3)(4\ 3)(5\ 2)$:

$1 \to 4$

$2 \to 5$

$3 \to 1$

$4 \to 3$

$5 \to 2$