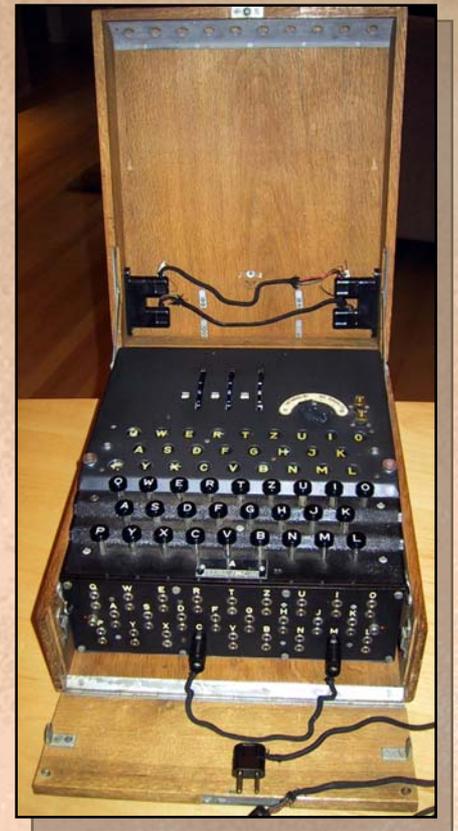


The Enigma Machine



History of Computing

December 6, 2006

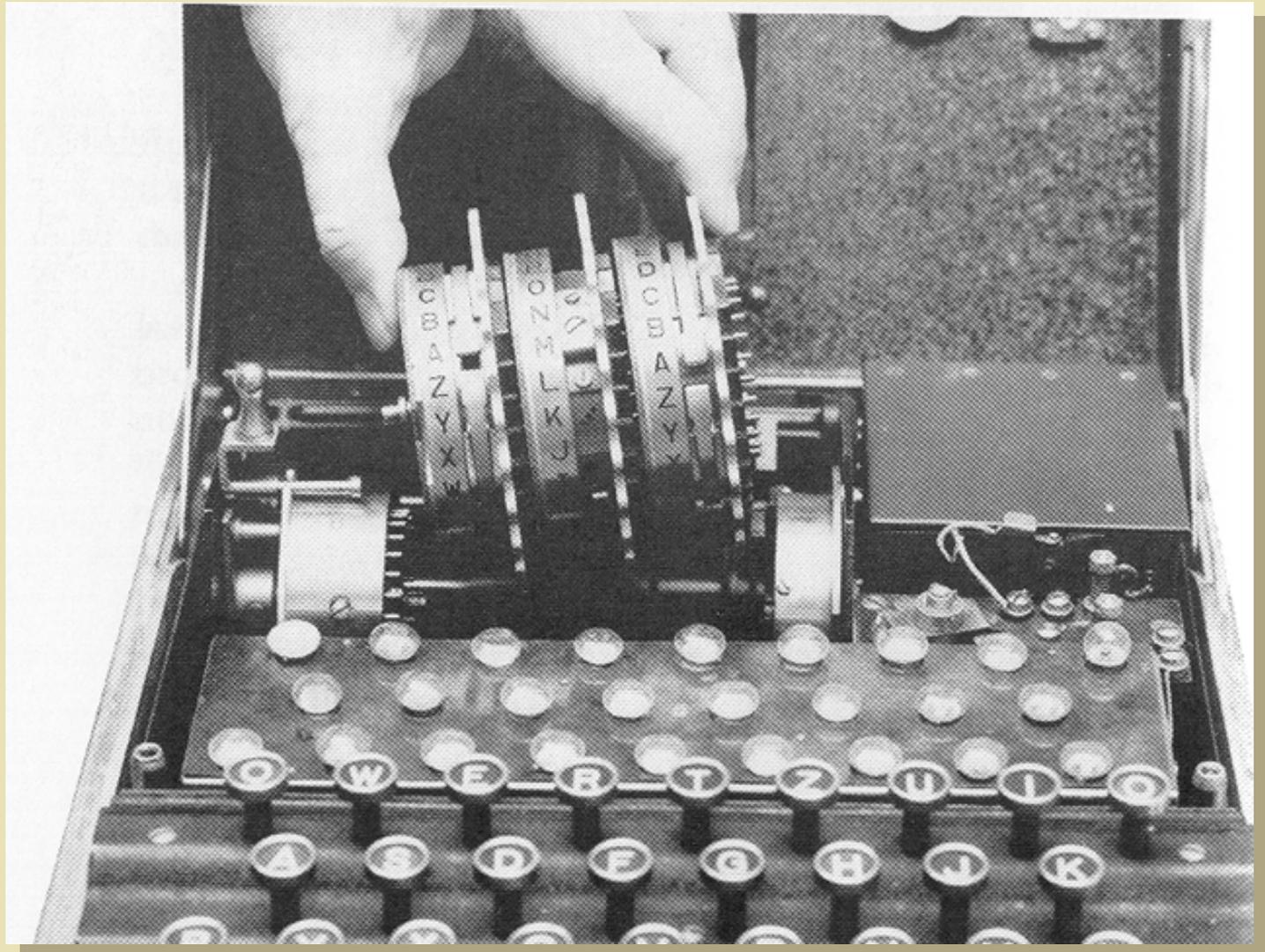
Mike Koss



Invention of Enigma

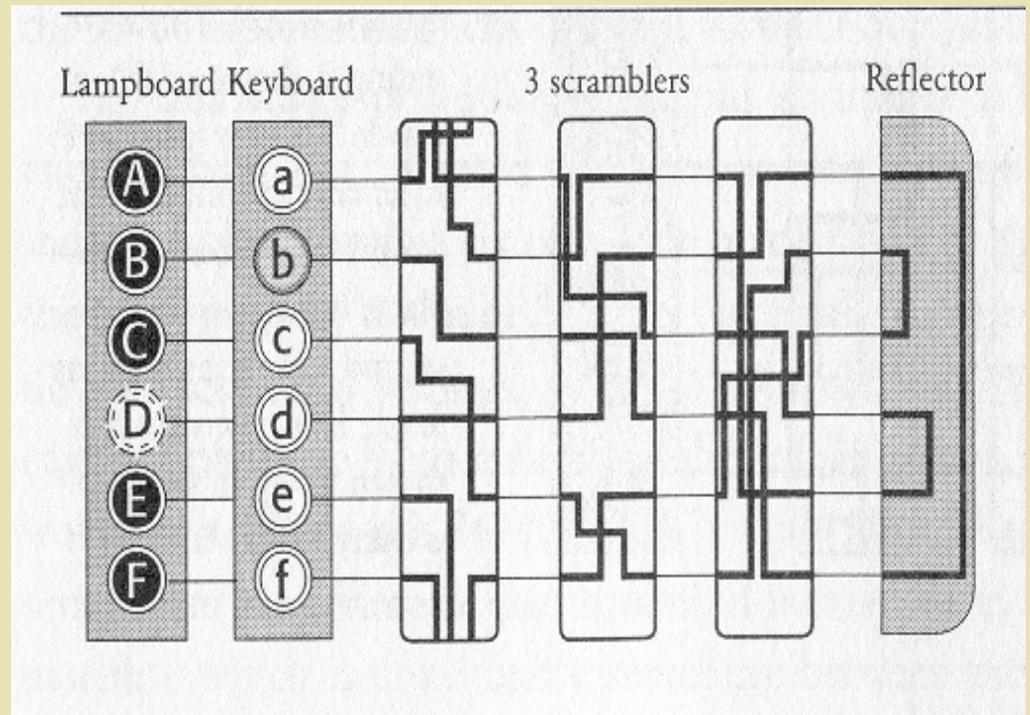
- ◆ Invented by Arthur Scherbius, 1918
- ◆ Adopted by German Navy, 1926
- ◆ Modified military version, 1930
- ◆ Two Additional rotors added, 1938

How Enigma Works



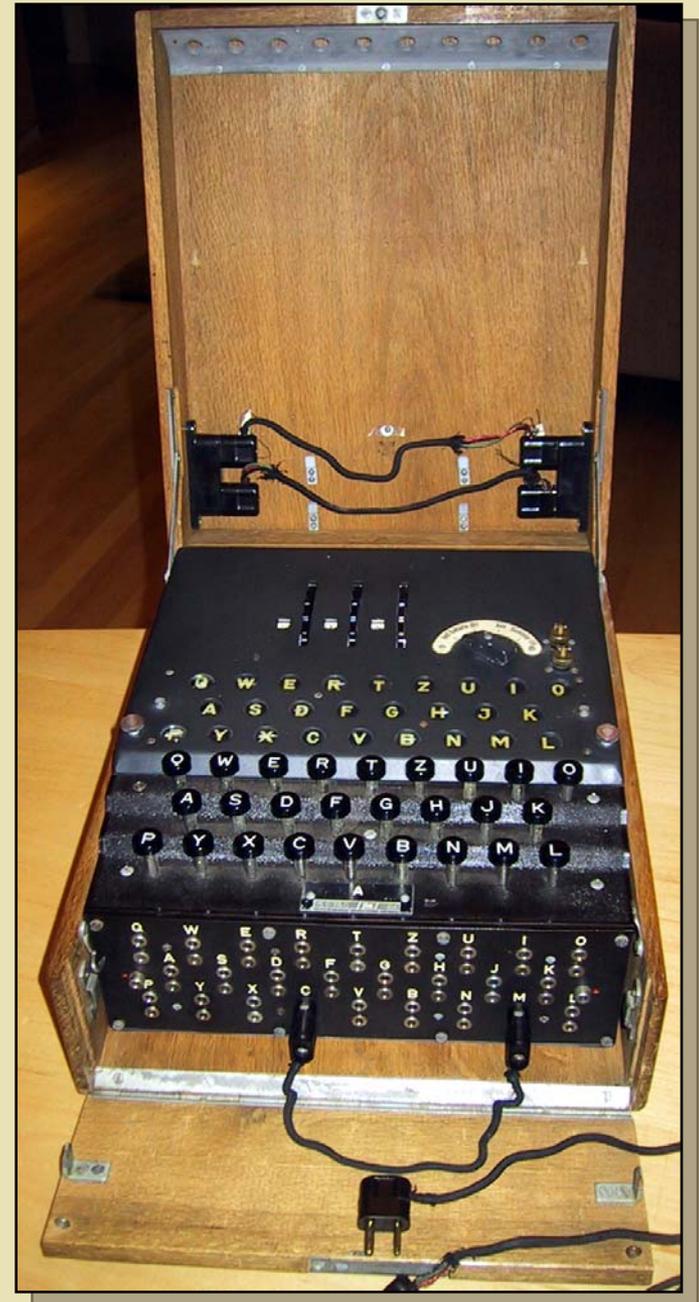
Scrambling Letters

- ◆ Each letter on the keyboard is connected to a lamp letter that depends on the wiring and position of the rotors in the machine.
- ◆ Right rotor turns before each letter.



How to Use an Enigma

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



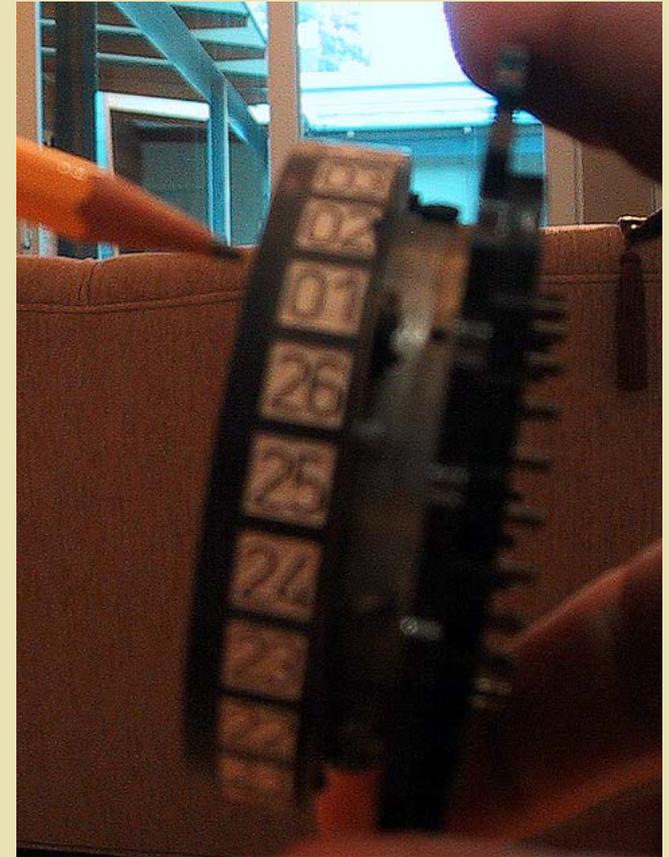
Setup: Select (3) Rotors

- ◆ We'll use I-II-III

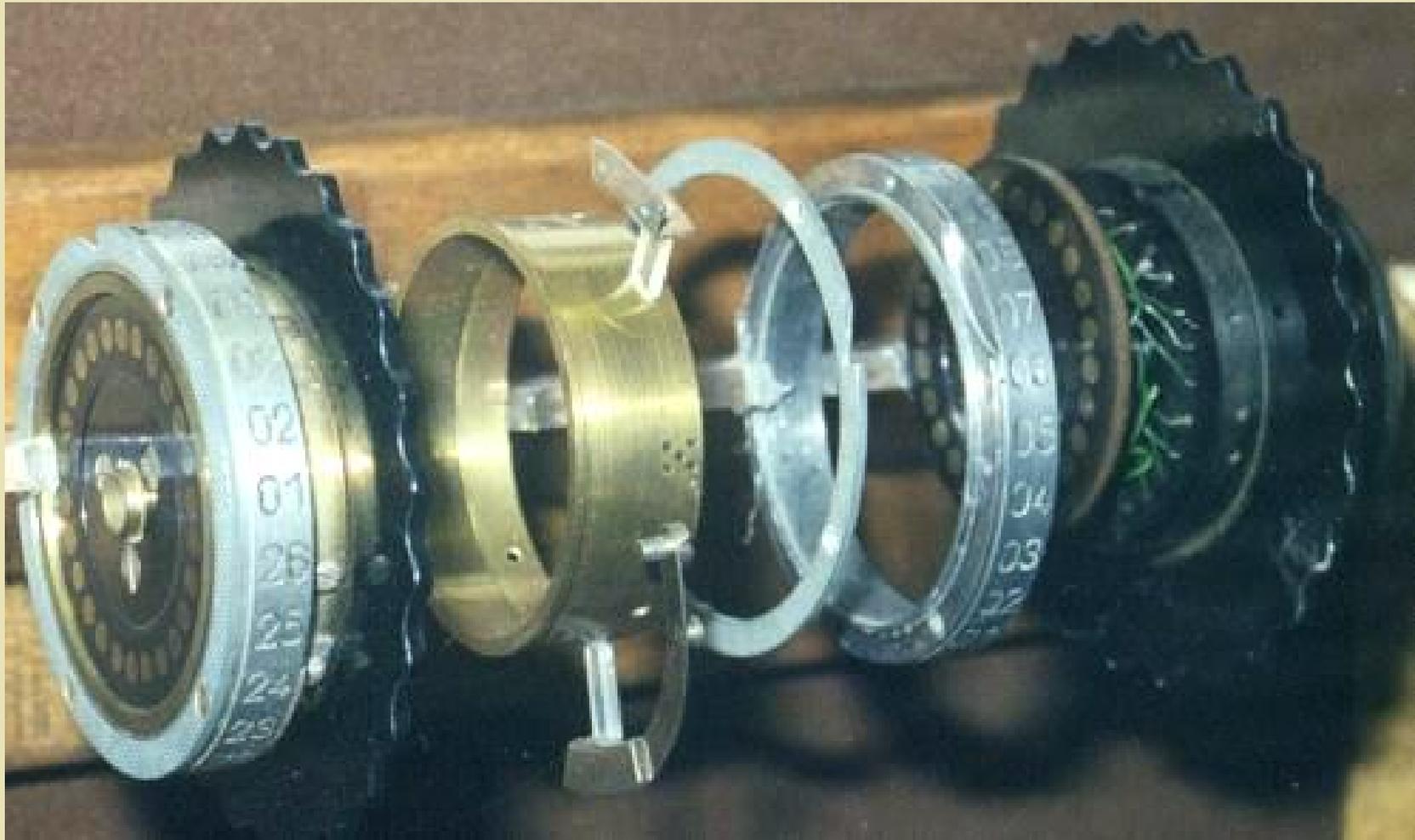


Setup: Rotor Ring Settings

- ◆ We'll use A-A-A (or 1-1-1).

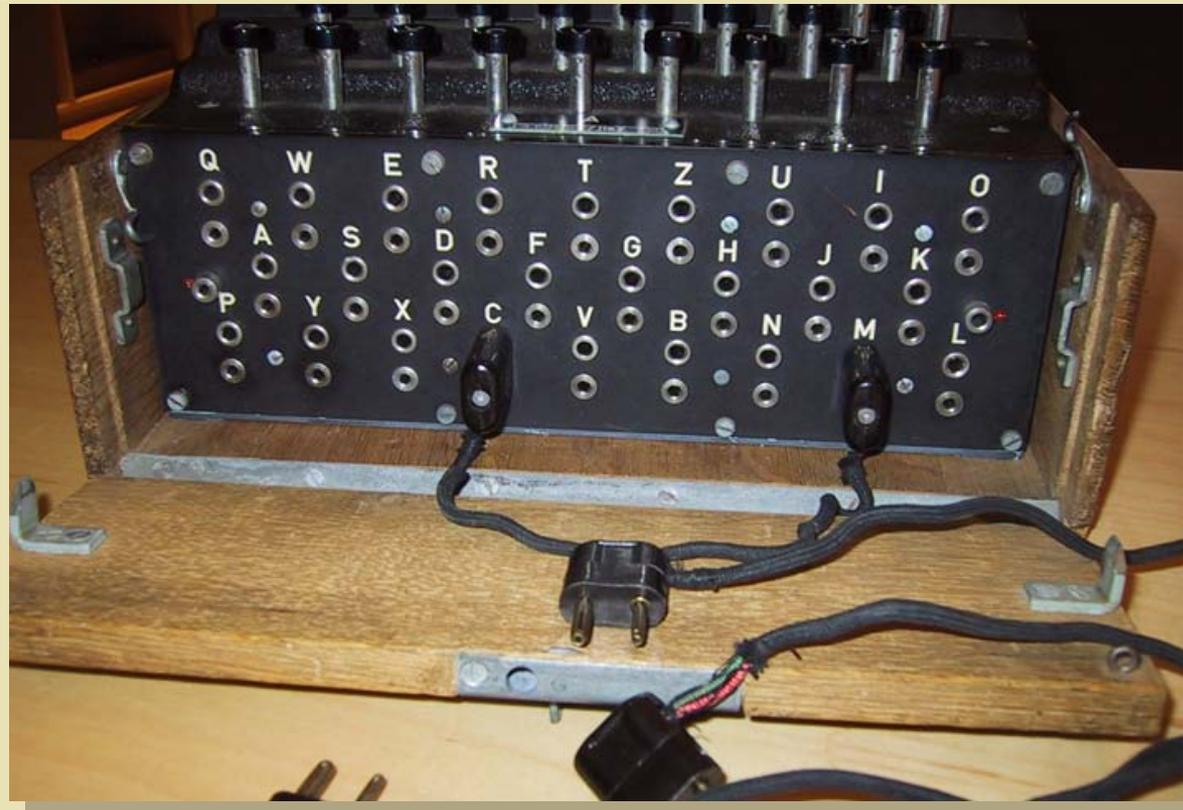


Rotor Construction



Setup: Plugboard Settings

- ◆ We won't use any for our example (6 to 10 plugs were typical).



Setup: Initial Rotor Position

- ◆ We'll use "M-I-T" (or 13-9-20).





Encoding: Pick a “Message Key”

- ◆ Select a 3-letter key (or *indicator*) “at random” (left to the operator) for *this message only*.
- ◆ Say, I choose “M-C-K” (or 13-3-11 if wheels are printed with numbers rather than letters).



Encoding: Transmit the Indicator

- ◆ Germans would transmit the indicator by encoding it using the initial (daily) rotor position...and they sent it TWICE to make sure it was received properly.
- ◆ E.g., I would begin my message with “MCK MCK”.
- ◆ Encoded with the daily setting, this becomes: “NWD SHE”.



Encoding: Reset Rotors

- ◆ Now set our rotors to our chosen message key “M-C-K” (13-3-11).
- ◆ Type body of message:
“**ENIGMA REVEALED**” encodes to
“**QMJIDO MZWZJFJR**”.
- ◆ Complete message is then:
NWDSHE QMJIDO MZWZJFJR



Decoding: Initial Setting

- ◆ Setup is the SAME for encoding and decoding. Set rotors to “M-I-T” (13-9-20).



Decoding: Decode Indicator

- ◆ Type in message indicator: “NWDSHE”.
- ◆ Confirm it decodes to “MCK MCK” (a valid message key).



Decoding: Message

- ◆ Set rotors to “M-C-K” (13-3-11)
- ◆ Type remainder of message:
“**QMJIDO MZWZJFJR**” becomes
“**ENIGMA REVEALED**”!



A Paper Enigma Machine

- ◆ Each rotor is modeled as a strip of paper; the electrical contacts are replaced by matching letters on left and right side of the strip.
- ◆ Keyboard and Lamps are replaced by a vertical list of letters on the right.
- ◆ Reflecting rotor is replaced by a matching group of letters on the left.
- ◆ Plugboard and rotor “ring settings” are not modeled.

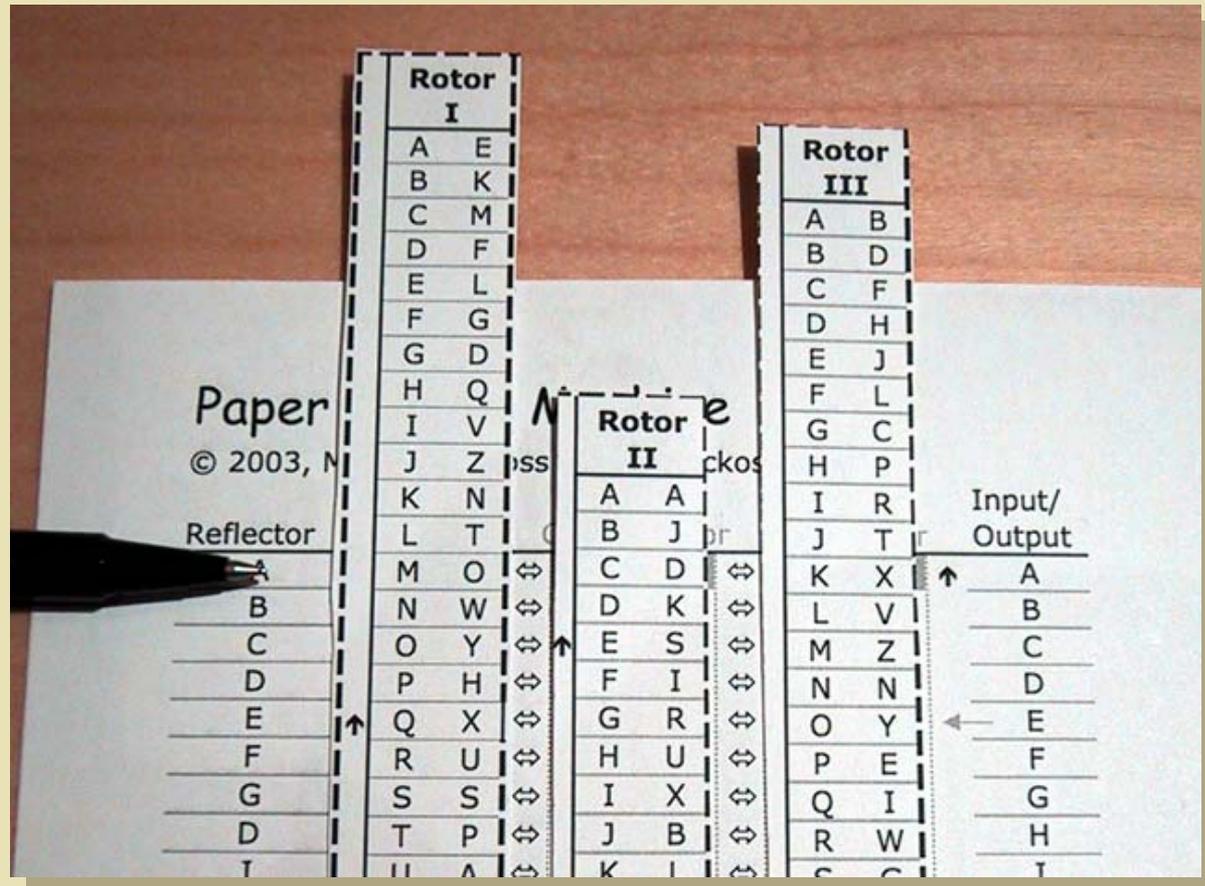
Sample Encode

- ◆ Rotor order: I, II, III
- ◆ Rotor setting: M, C, K
- ◆ Encode the letter “E”



Initial Setting

- ◆ Rotors I, II, and III
- ◆ “Window settings” of “M-C-K”



Encode a letter

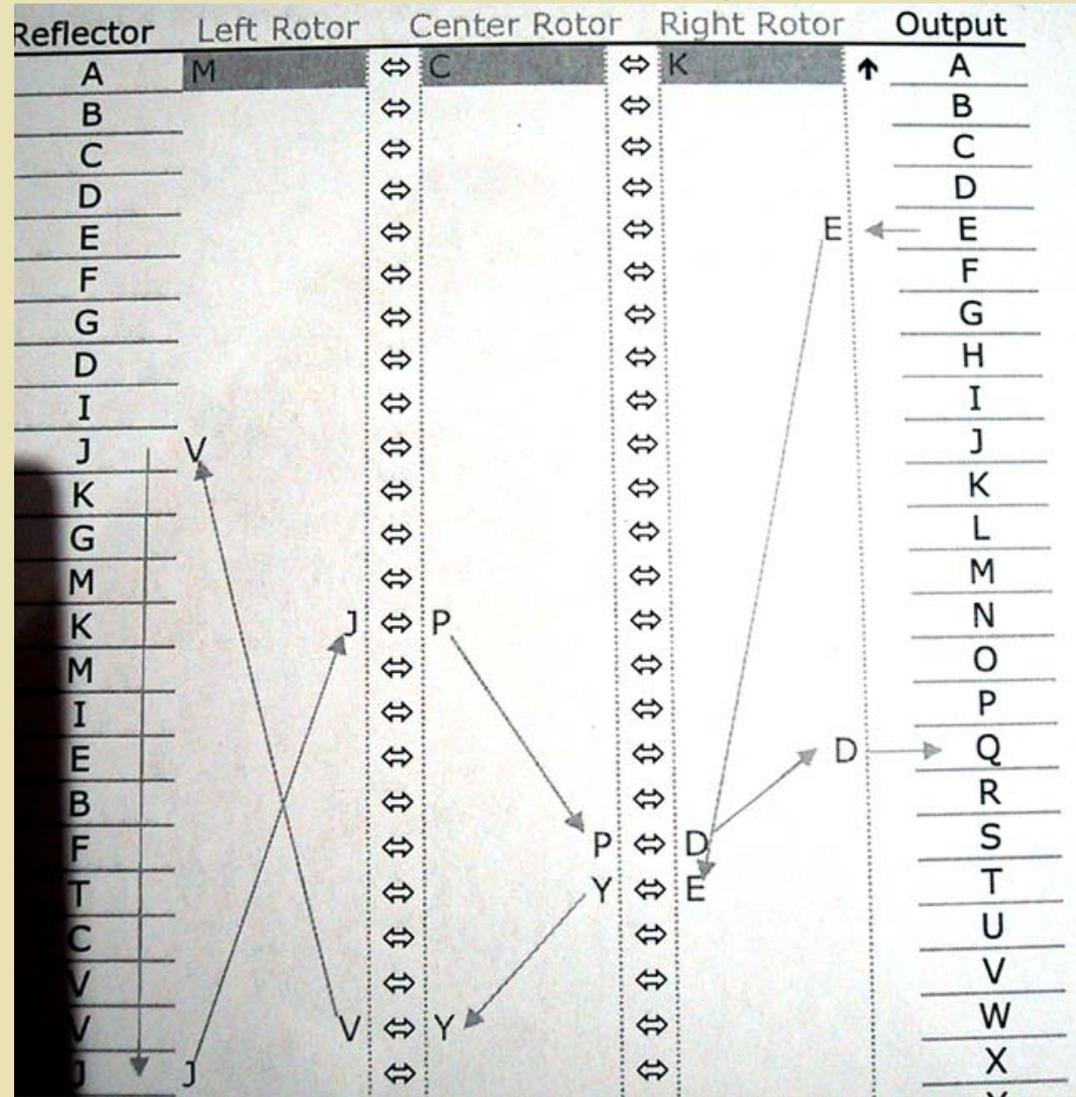
- ◆ (First!) Advance the right-most rotor (III) by moving it up one row.



Reflector	K	N	A	A	J	T	Input/ Output
A	L	T	B	J	K	X	A
B	M	O	C	D	L	V	B
C	N	W	D	K	M	Z	C
	O	V	E	S	N	N	

“Manual” Electricity

- ◆ Start at “E” on the right column.
- ◆ Trace through each rotor, matching like letters.





Rollover

- ◆ When the “notch” arrow reaches the window, move the wheel to it’s left up one row before encoding.
- ◆ When the center wheel arrow reaches the window, remember to move BOTH center and left wheels!



Breaking Enigma

- ◆ Poles intercept commercial Enigma in the mail, 1928
- ◆ Recruit math students at Poznan University, 1929
- ◆ Poles (Rozycki, Zygaliski, Rejewski) break the 3-rotor machine, 1932-1939
- ◆ Overwhelmed by 2 new rotors in 1938
- ◆ Poles hand over methods and machine copy to British and French in 1939
- ◆ Government Code & Cipher “School” created at Bletchley Park, 1939



Vulnerabilities

- ◆ Encryption of doubled indicators reveals information about rotor positions.
- ◆ Operators choose poor message keys (e.g., “BER”, “LIN”, “HIT”, “LER”, “JJJ”, “QWE”).
- ◆ Letter never encrypts to itself (allows known plaintext attack).

US Army, M-209 (Hagelin)



Swiss,
NEMA
(New
Machine)



Hagelin CD-57



Hagelin CX-52 RT (Random Tape)



Reihenschieber

