



The Enigma Machine

History of Computing

December 6, 2006

Mike Koss

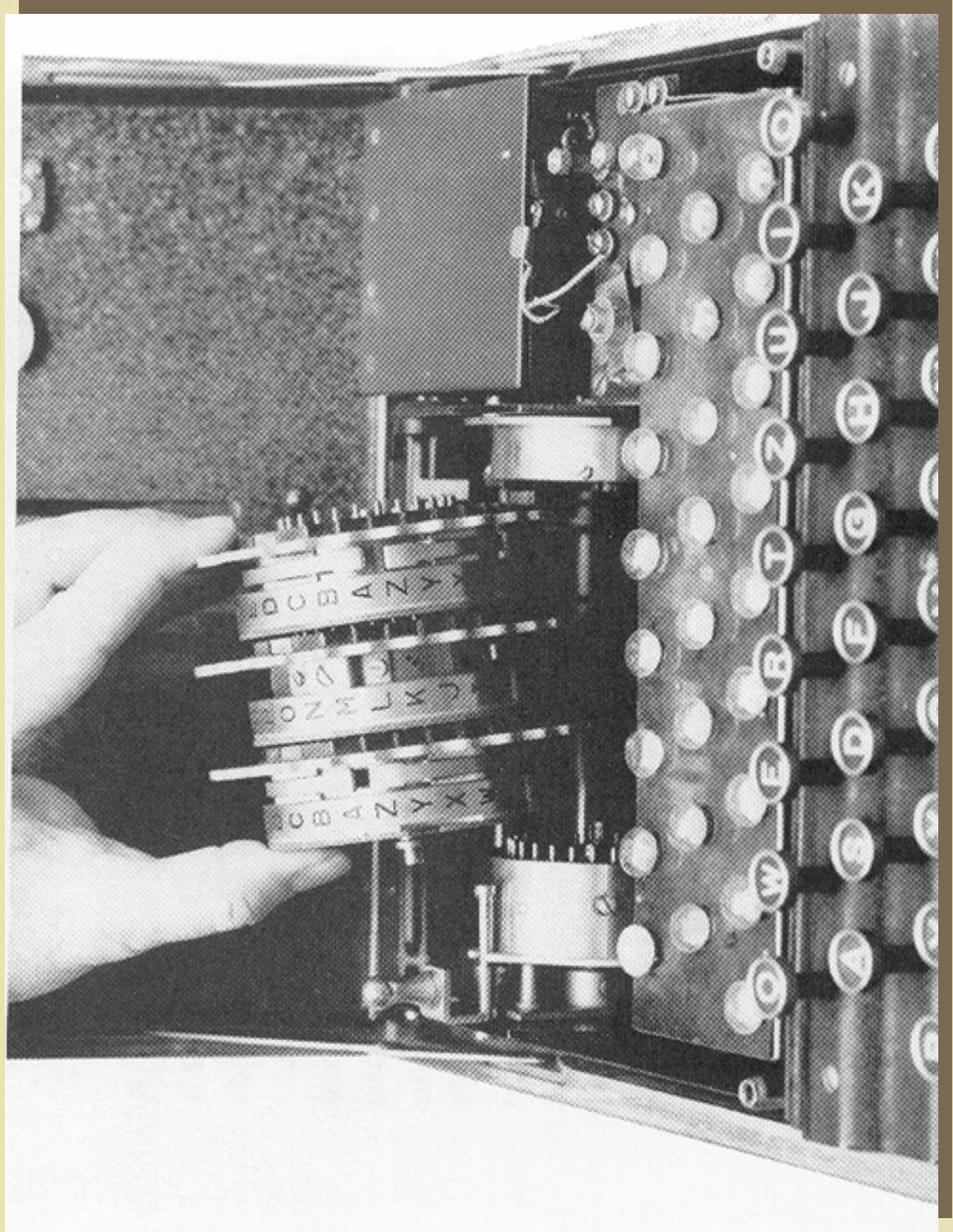


Invention of Enigma

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

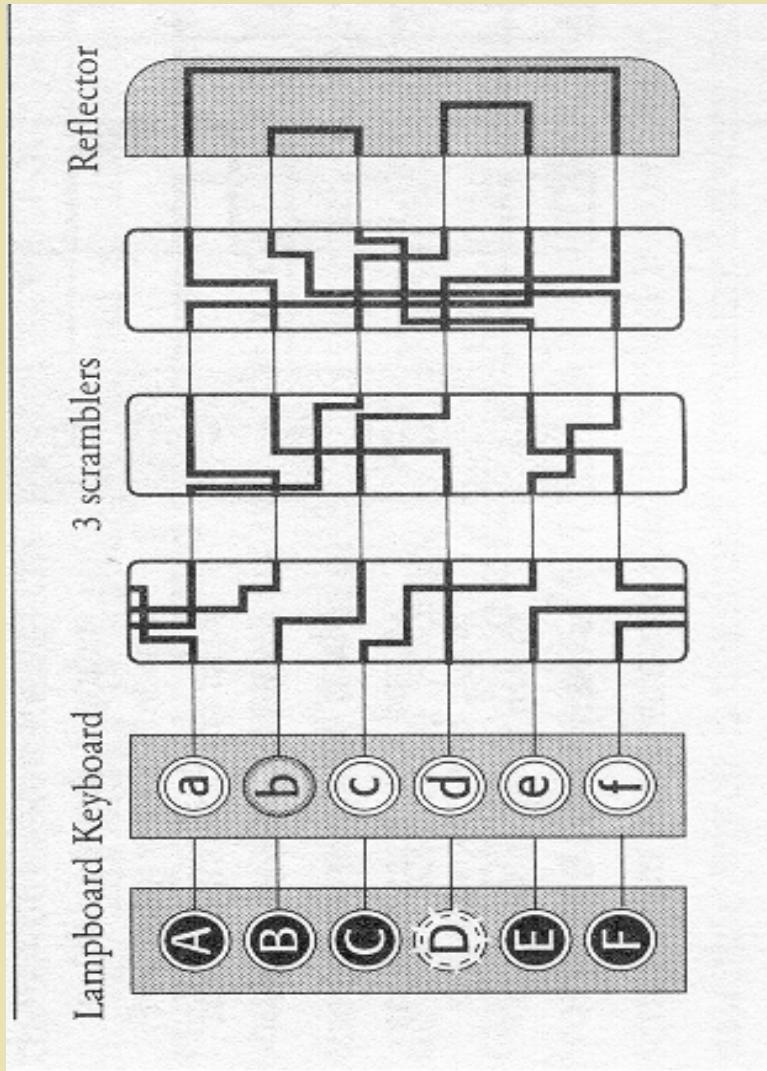


How Enigma Works



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



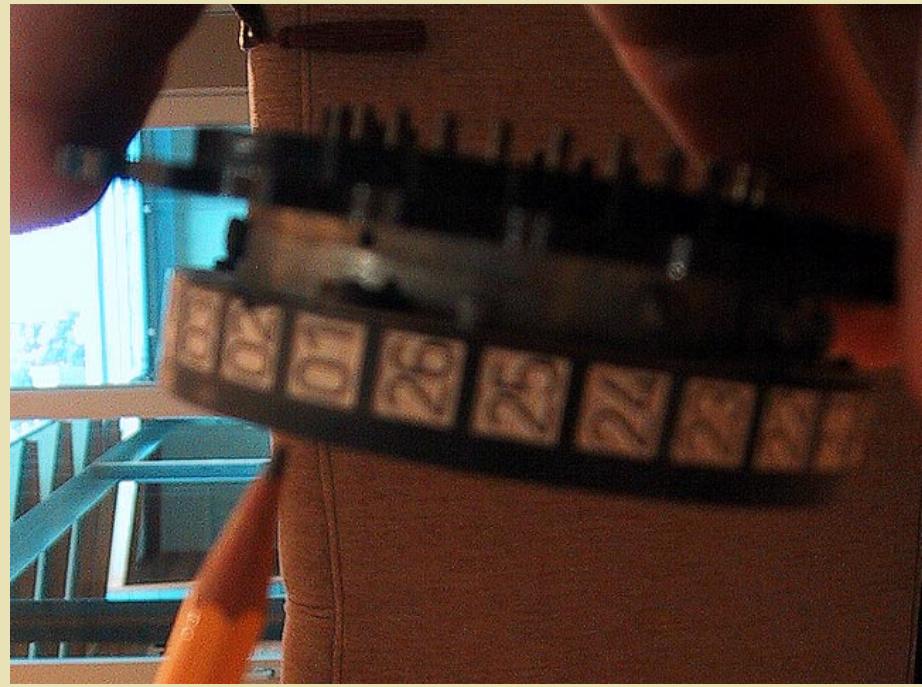
Setup: Select (3) Rotors

- ◆ We'll use I-II-III



Setup: Rotor Ring Settings

- ◆ We'll use A-A-A (or 1-1-1).

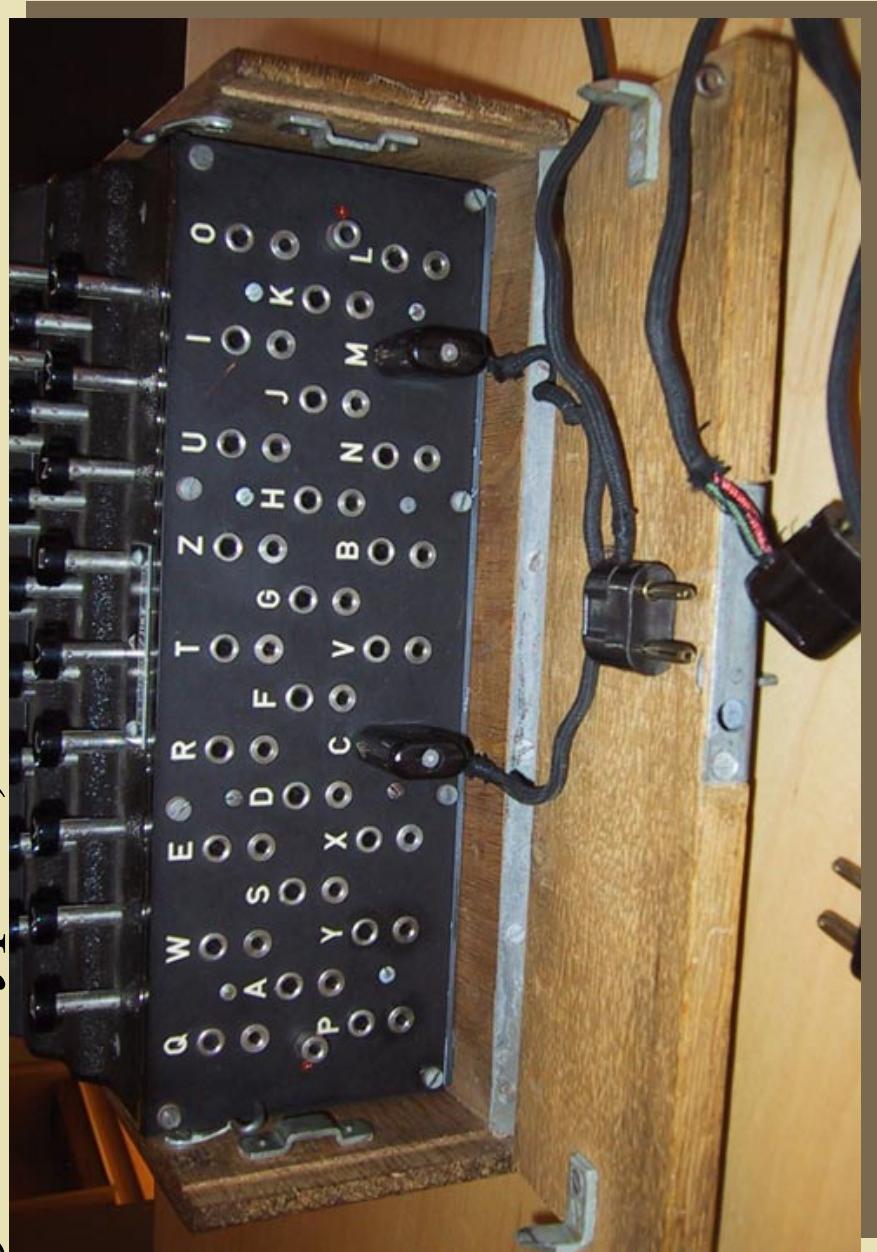


Rotor Construction



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 do our chosen message key “M-C-K” (13-3-11).
- ◆ Type body of message:
**“ENIGMA REVEALED” encodes to
“QMJJDO 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:
“QMJJDO 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.



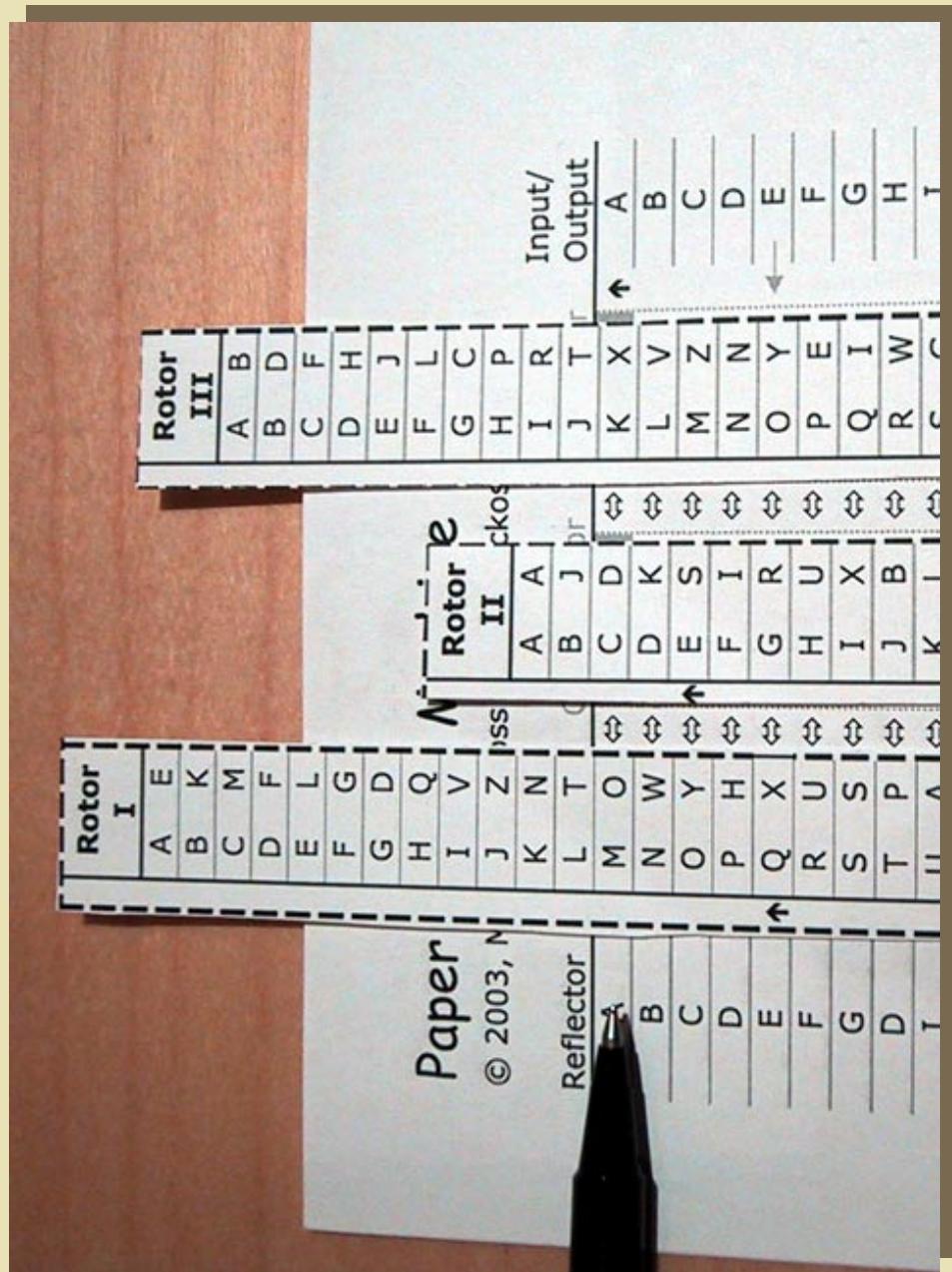
Sample Encode

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



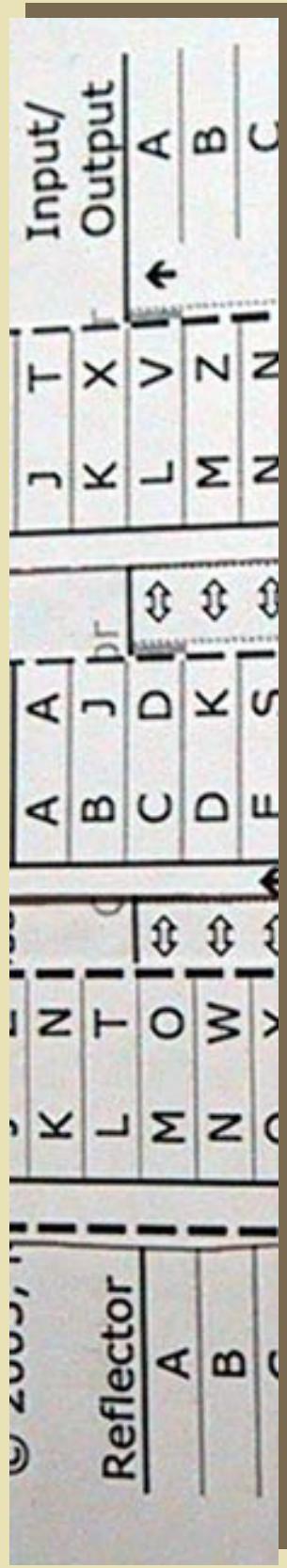
Initial Setting

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



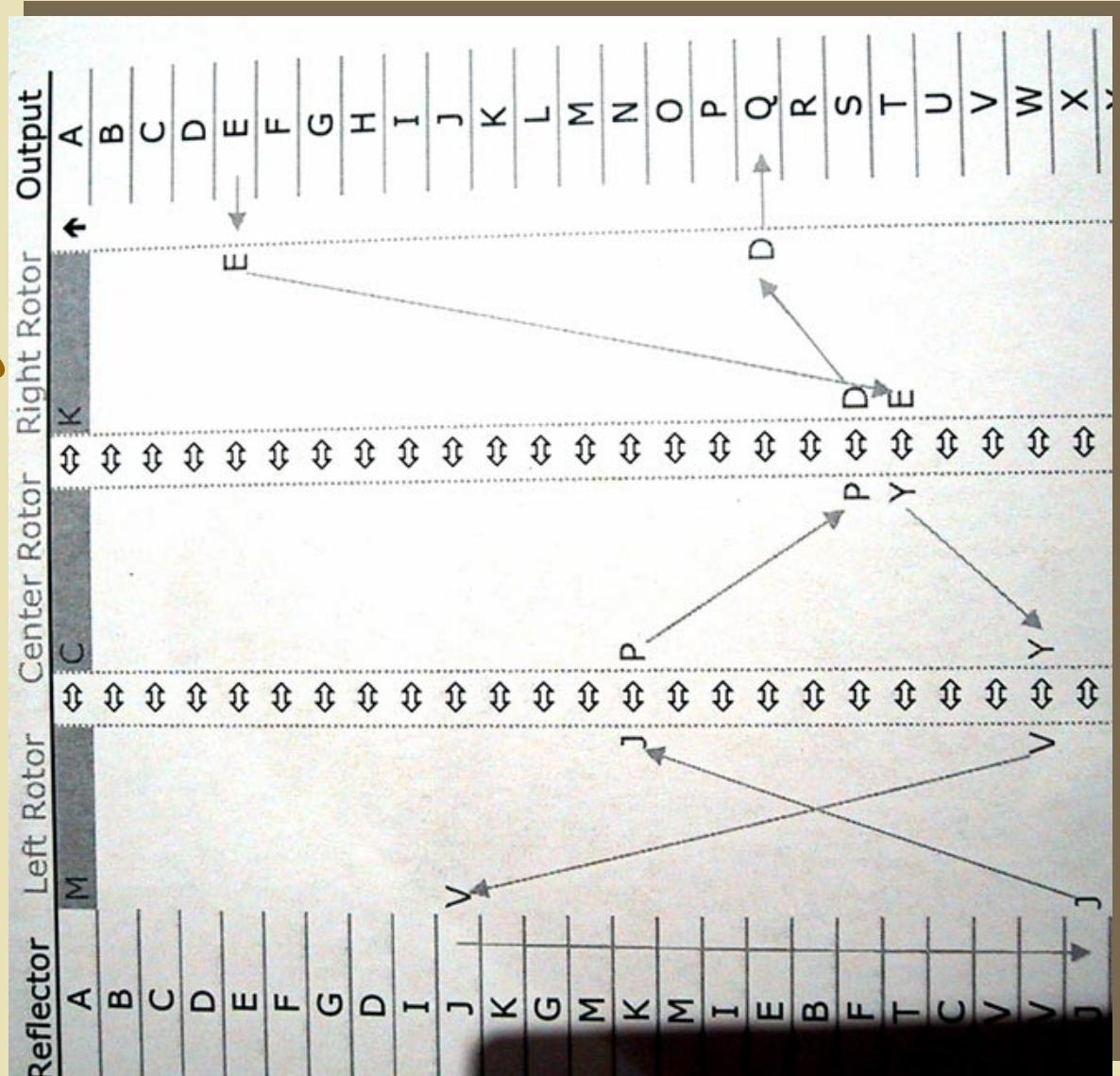
Encode a letter

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



“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 (Rozyczki, Zygalski, 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

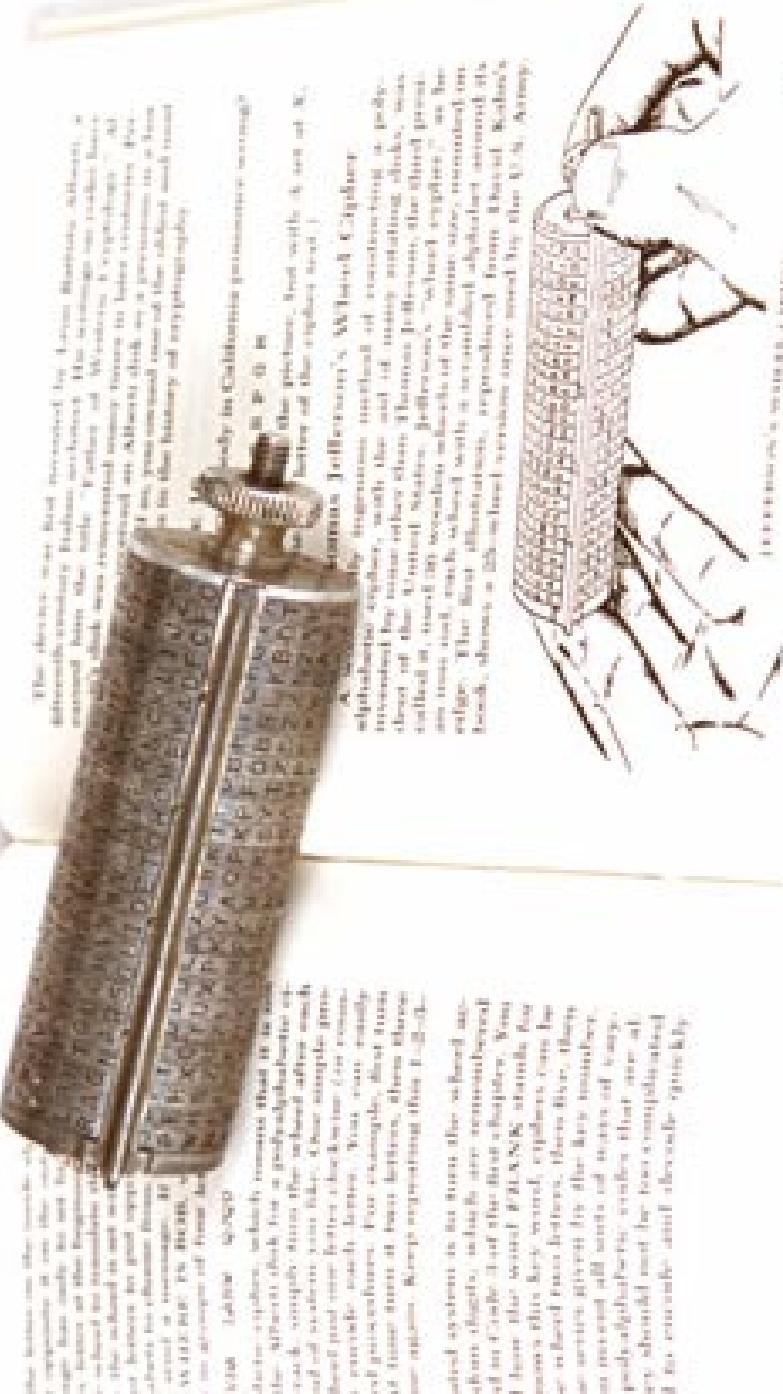


Vulnerabilities

- ◆ 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-94 Cipher Device



the consequences of such a course. I can assure you, without exaggeration, that under the circumstances, there would be no other way to stop the Chinese from getting involved in our affairs than by threatening to do so ourselves. There has been a certain amount of talk about the possibility of a Chinese invasion of Korea through the Soviet Union, but I don't think that there is much likelihood of that. The Chinese are more interested in getting into Korea themselves, and I don't think they would be likely to do so unless they were compelled to do so by us.

If there is an uncommunicated difference between the two countries about the treatment of the displaced persons, it is probably best to leave this question to the International Conference on Refugees.

For many years we have observed systems in which the so-called *coexisting* state is a mixture of coexisting liquids, and they are often called *two-phase* systems. In such a system there is a liquid phase and a gas phase, and it is often assumed that the liquid phase is the more dense. This is not necessarily true, however, because the two phases can be interchanged by heat or pressure. There may, therefore, be two coexisting liquids which differ in their densities, and still remain as separate and distinct phases. For example, when water is heated, it becomes lighter than air, and the two substances intermix. This is called *convection*. The same effect can occur when water is cooled, and the two substances intermix. This is called *conduction*.

This observation has received the following interpretation. In the first place, it is evident that the number of individuals in each species of *Microtus* is proportional to the amount of food available to it. The amount of food available to a given species will depend upon the amount of food available to all other species, as well as upon the density of the population.

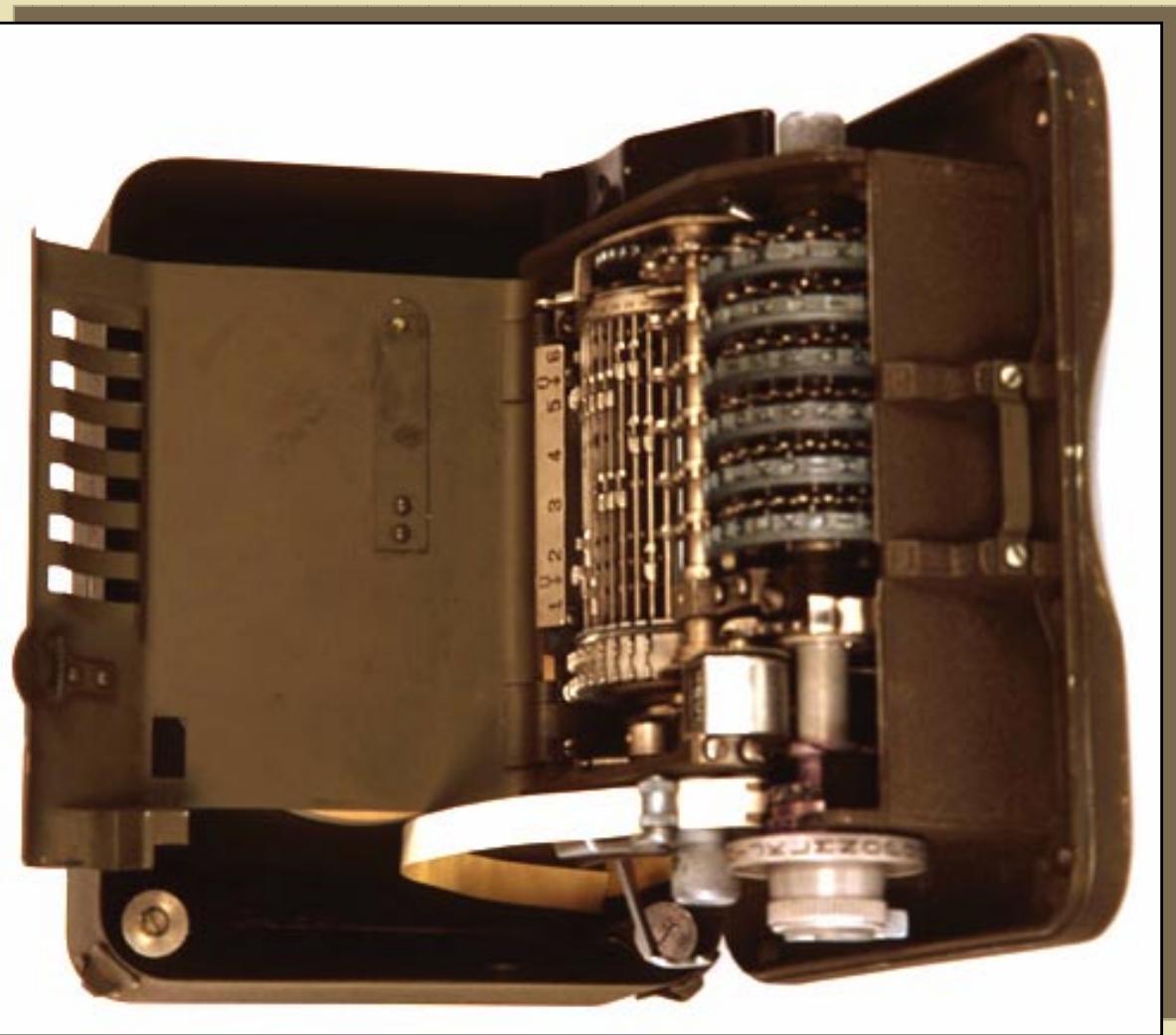
order to facilitate measurement, we will
use μ as the
mean thickness. Each weight, m_1 , m_2 , and m_3 ,
is measured at three different times, t_1 , t_2 , and t_3 .
The mean thickness, $\bar{\mu}$, is then calculated as
$$\bar{\mu} = \frac{m_1 t_1 + m_2 t_2 + m_3 t_3}{m_1 + m_2 + m_3}$$

the most prominent being the *Californian*, which has a large number of stations, mostly along the coast, extending from San Francisco to the Oregon border. The *Alaska* has stations in Alaska, British Columbia, and the Yukon, and also a few in the interior of the continent. The *North American* has stations in the interior of the continent, and also a few on the coast. The *South American* has stations in Chile, Argentina, and Brazil. The *Australian* has stations in Australia, New Zealand, and Tasmania. The *Antarctic* has stations in the Southern Ocean, and the *Arctic* has stations in the Northern Ocean.

四

卷之三

US Army, M-209 (Hagelin)





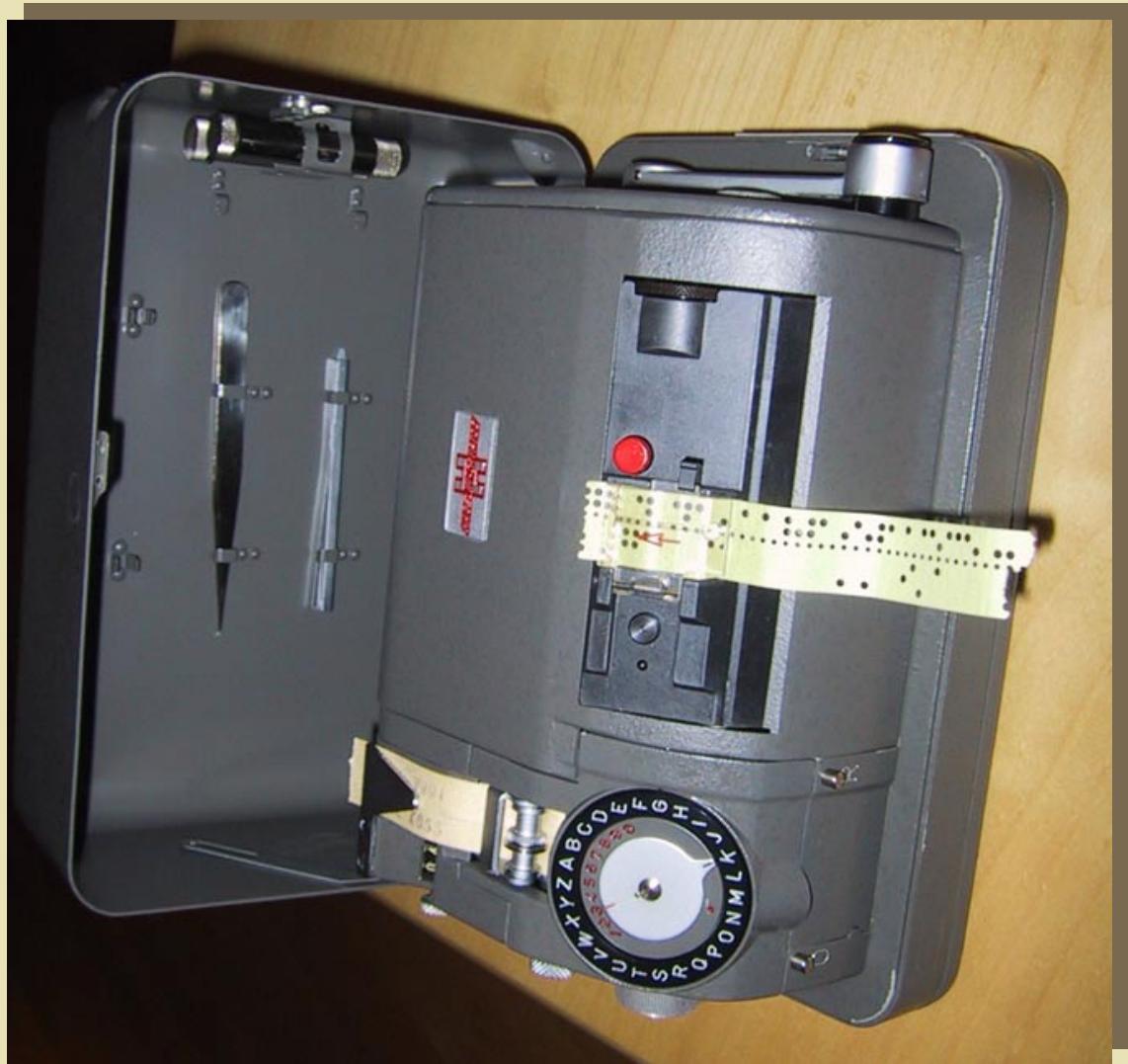
Swiss, NEMA (New Machine)



Hagelin CD-57



Hagelin CX-52 RT (Random Tape)



Reihenschieber

