# 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

AN I



# 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

1

"Window settings" of "M-C-K"



#### Encode a letter

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

2003, 1	KNI	AA	JTI	Input/
Reflector I	LTI	B J pr	K XI	Output
A	M O G	C D 🖨	LV	↑ A
BI	N W ⇔	D KI 🚓	MZ	В
	In VIA	FSB	NN	С

## "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, Zygalski, Rejewski) break the 3rotor 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

DITIE COLLEGE

ODSILKBO

the president product the local star in Access of a supervise approache of our that on country of the converger from county has not be successible would be better of the begins There for our one the informities inside the double dispersions the school is not not others and the children of hothers for grant appart Addressed registers algebra barts for allesses through works much drawn with strend a surrounger. 10 damage the environment of all other the Decam, a stand approach that many no protoger of four la INTERN LANDAR NO. PARTY

Then on a communication to produce, so hands account that is not I for the house . For they that the shine of the for a product point to be been hand to be a set of the set of th polare making making and kingd of stations your like. Once simple probefore in the many time in here I part every better a her burning day to many conductor in the 1 affect prove entertaile trach denter. Your that examinmonths and ensure assumption of plane where . For example, first durate should be a based server houses, moral times firsts of Parce hollows, these thereas the short off the bark to over agains known reprinting this 1-2-3-Log-A-L-Ball . Comments

An even mate complicated system is to turn the wheel as An even strength of president chights, which are trainenthened invanients, for successful and provide the first strategies of the second strategies when for a key second over learness have the word FRANK stands for well several truth every mass however this key word, explores can be alights different solutions the solution between them have, there five, there concentration of the property of the second given by the key manufact which as briefly thereight your case over and all such as it was a of yary. Write a little distribution in make poly-alphabetic codes that one at and the processing the second. They derived not be true compliances income transformer of well for fourth to encode and the only spice \$2. wathout a lot of econes.

3.84



The decise was here recented by Later Bartons Advert, a advertelle sendory bishess sectation ( 11m minings on confer from partiand here the ratio "Further of Washings & Symposium 1 for shak was enterenated some times to been continues. For proved an Alberts thek are a pression in a base I was your serviced over 14 the relatest and reach t in the history of exception option

sly in Coldiana's prosentation writing?

A 19 10 10

the picture, lost write it set of X hottow ad that explanational (

#### mman Jefferson's Wheel Cipher

By ingration method of construction a polyalphabetic ripher, with the out of many induiting dicks, was investigating insure others there. Thereiser Joffersons, the thread press. shout of the United States Jefferson's "wheel support on he collect it, must be wreather wheels of the same and, recorded on any treas read, reach school with a second-dect algituder account its erfage. The first illustration, reproduced form David Kabac's brock, shows a 25-wheel evening case and by the U.S. Army-





T





#### Swiss, NEMA (New Machine)





#### Hagelin CD-57



#### Hagelin CX-52 RT (Random Tape)

a.



#### Reihenschieber

1

