The Enigma-E Project

John Dean, K0JDD

Enigma-E

- A fully functional electronic version of the German Enigma Cipher Machines used during WWII
- Emulates M3 (Armee) and M4 (Kriegsmarine) Models
- M3/M4 Rotor wheels I II III IV V VI VII VIII (Simulated in software)
- M4 Greek Wheels Beta and Gamma (Simulated in software)
- Fully Functional plugboard
- Available in Kit form
- User provided case

John Dean, K0JDD

John Dean, K0JDD

Enigma-E

- Developed 2000/2001 in the Netherlands to be sold by museums in kit form as a fund raiser
- Based on the PIC16F873/876
- Retail cost is about $225
- www.cryptomuseum.com/kits/

Enigma Machine Origins

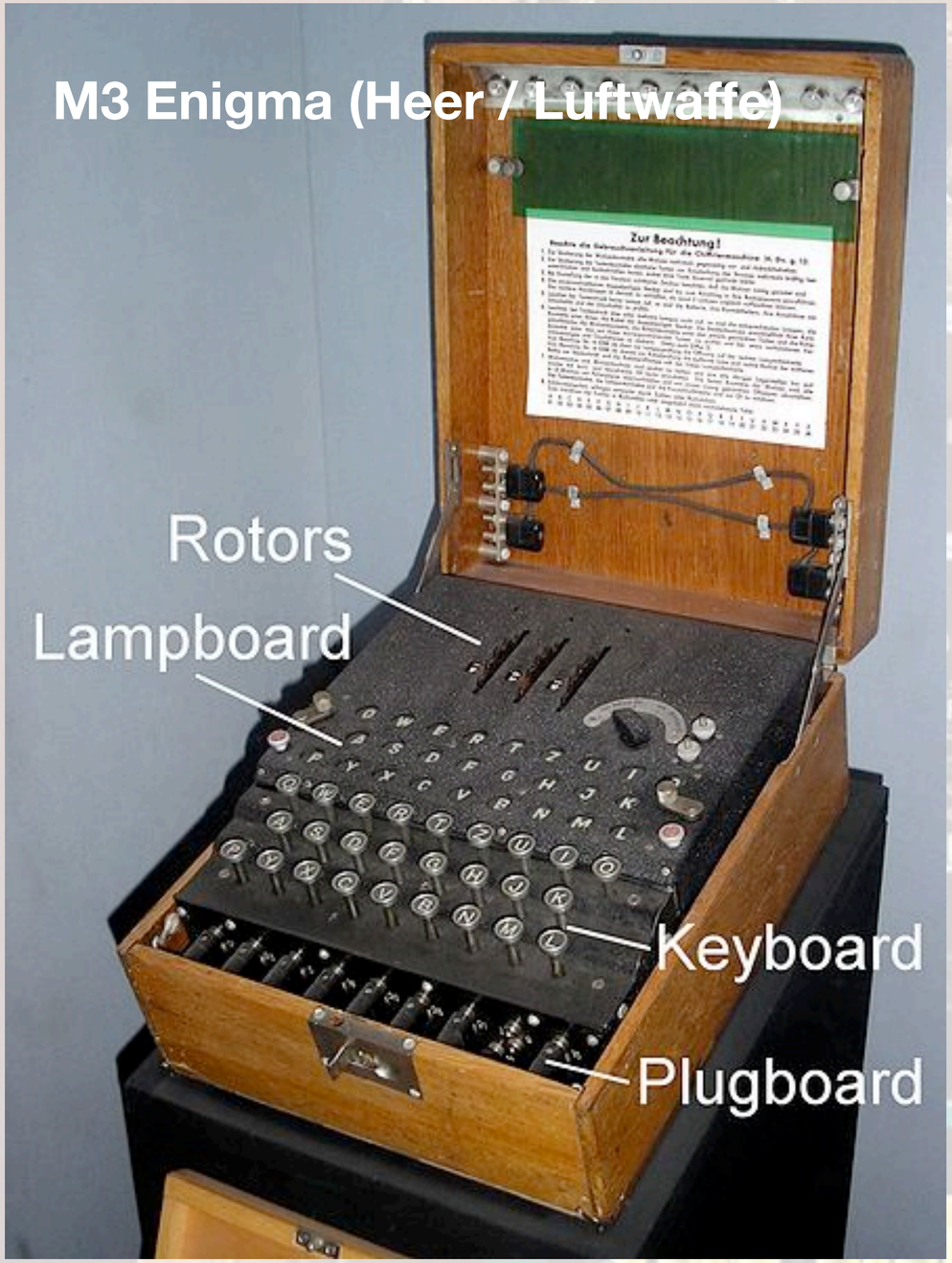
- The Enigma machine was invented by the German engineer Arthur Scherbius at the end of World War I. The German firm Scherbius & Ritter, co-founded by Arthur Scherbius, patented ideas for a cipher machine in 1918 and began marketing the finished product under the brand name Enigma in 1923, initially targeted at commercial markets.

- Early models were used commercially from the early 1920s, and adopted by military and government services of several countries, most notably Nazi Germany before and during World War II.

Operating Theory

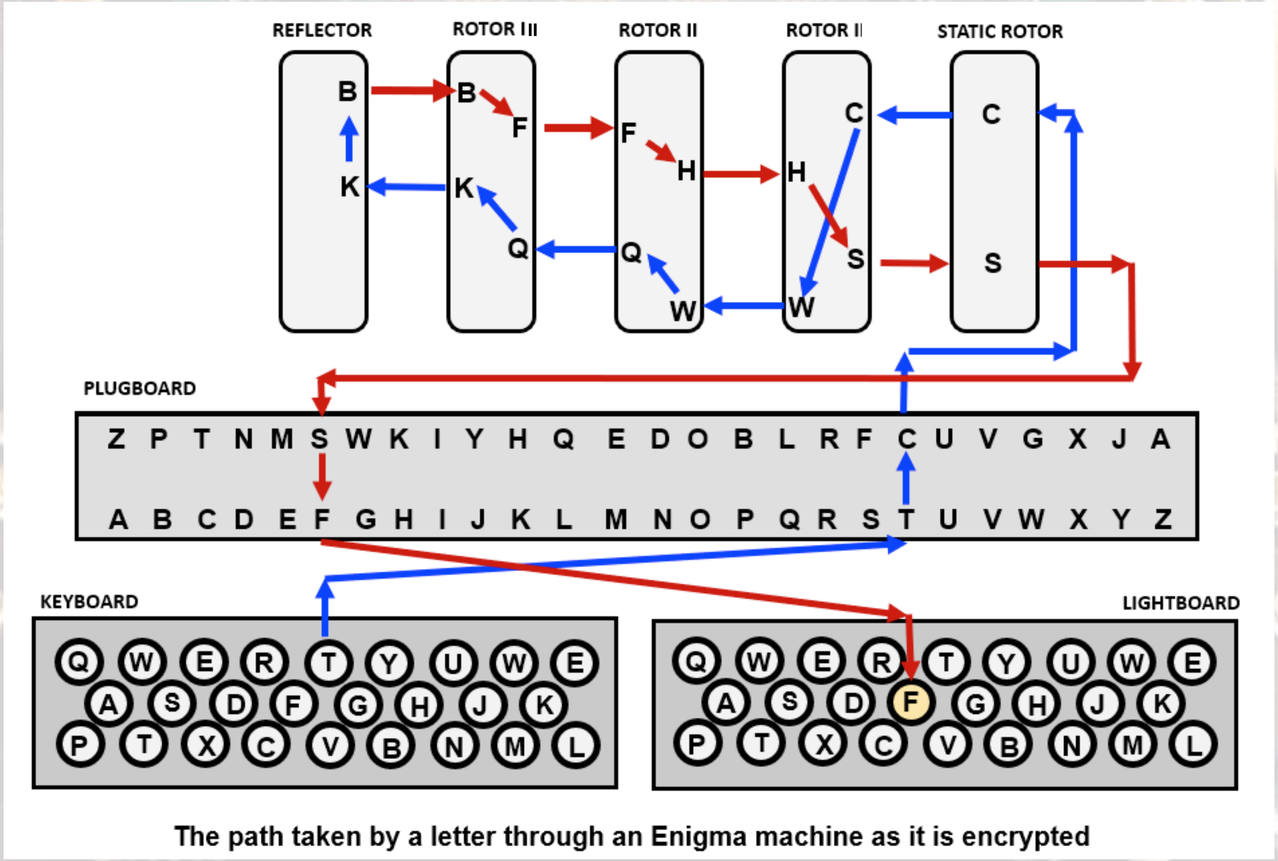
- The repeated changes of electrical path through an Enigma scrambler implement a symmetric polyalphabetic substitution cipher that provides Enigma's security.
- Major Components
  - Keyboard (Tastatur)
  - Lamp panel (Lampenfeld)
  - Plug Board (Steckerbrett)
  - Static Rotor (Eintrittswalze)
  - Stepping Rotors (Walze)
  - Reflector (Umkehrwalze)

M3 Enigma (Heer / Luftwaffe)



M4 Enigma (Kriegsmarine)

When You Push a Key



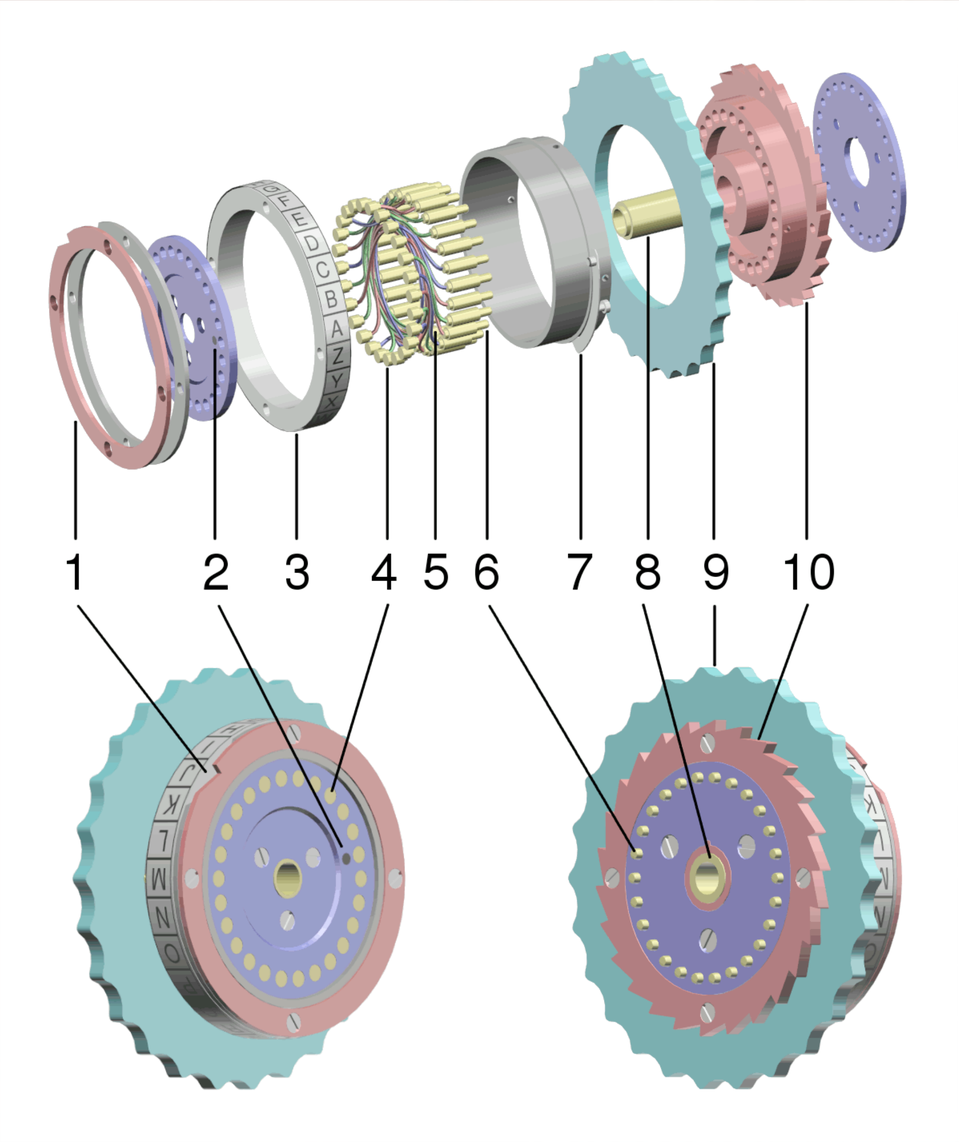
The path taken by a letter through an Enigma machine as it is encrypted

Rotors

- Rotor Construction
  - 26 contacts on left side
  - 26 spring loaded pins on right side
  - Adjustable ring with 26 letters or numbers
  - Internal wiring in a scrambled yet known pattern
  - Ratchet teeth for stepping on R
  - Notch for adjacent rotor turnover on L

- M3 used 3 out of 5 rotors (as many as 8 by 1946)

- M4 used 3 out of 5 rotors plus a thinner reflector wheel coupled with a Greek wheel to get 4 rotors



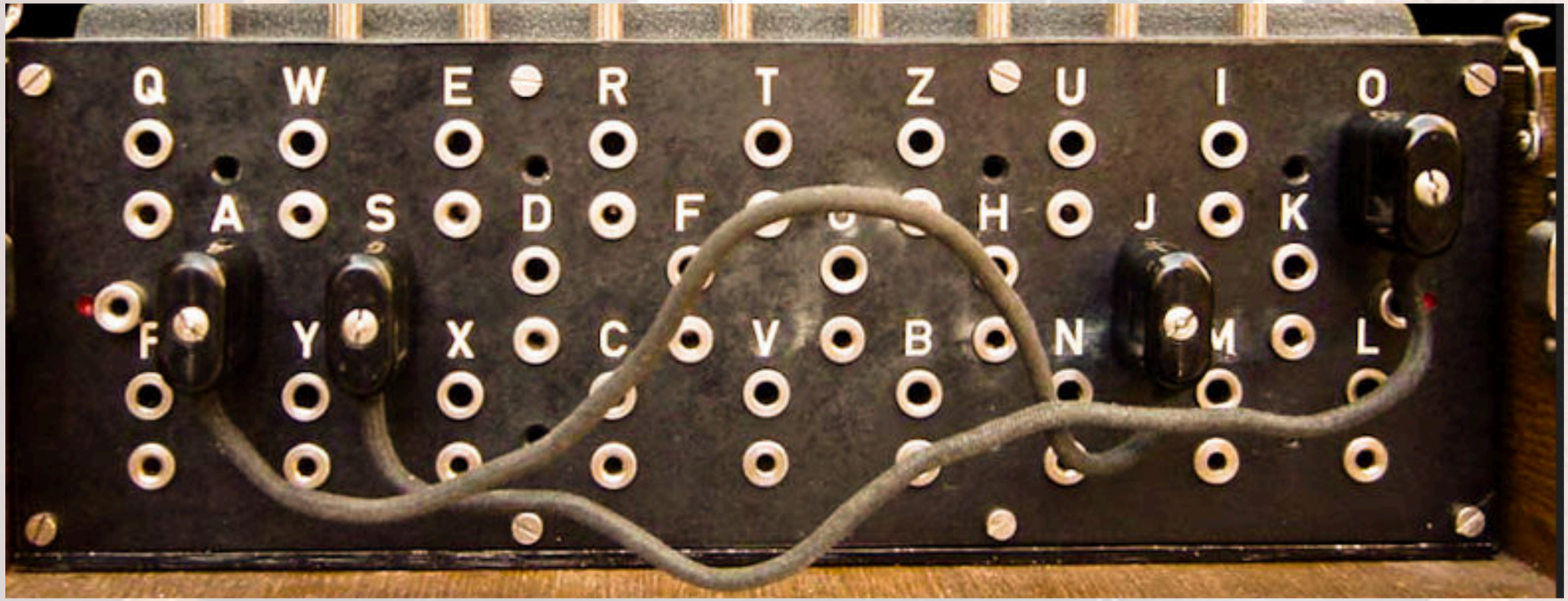
Exploded view of an Enigma machine rotor:
1-Notched ring,
2-Dot marking the position of the "A" contact,
3-Alphabet "tyre" or ring,
4-Electrical plate contacts,
5-Wire connections,
6-Spring-loaded pin contacts,
7-Spring-loaded ring adjusting lever,
8-Hub, through which fits the central axle,
9-Finger wheel,
10-Ratchet mechanism

John Dean, K0JDD

Plug Board

- 26 double sockets on the panel arranged in the QWERTZ keyboard order
- Zero to 13 cables with double-pin jacks can be inserted into the panel. Each cable swaps one pair of letters
- Letters with no cables are ’self-steckered’

Plug Board

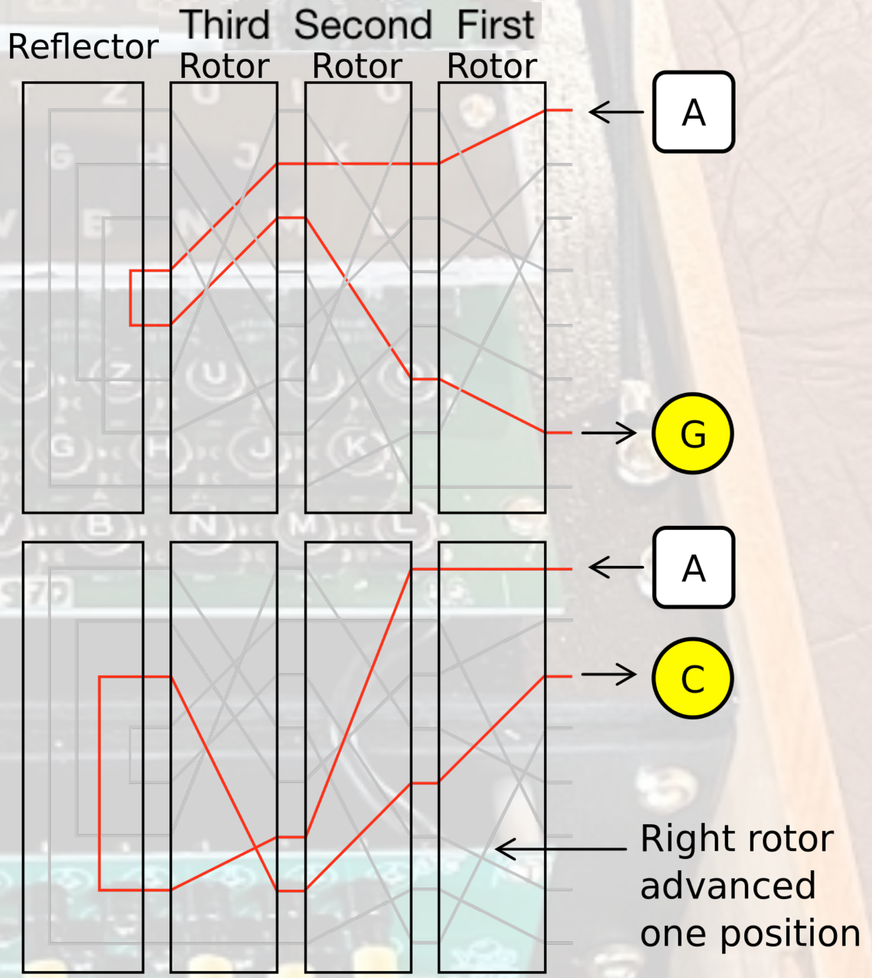


Two Stecker cables AJ SO

Pressing Keys

Pressing a key STEPS the first rotor, creates an electrical circuit, and lights a lamp

Pressing a key twice in a row will NOT yield the same results

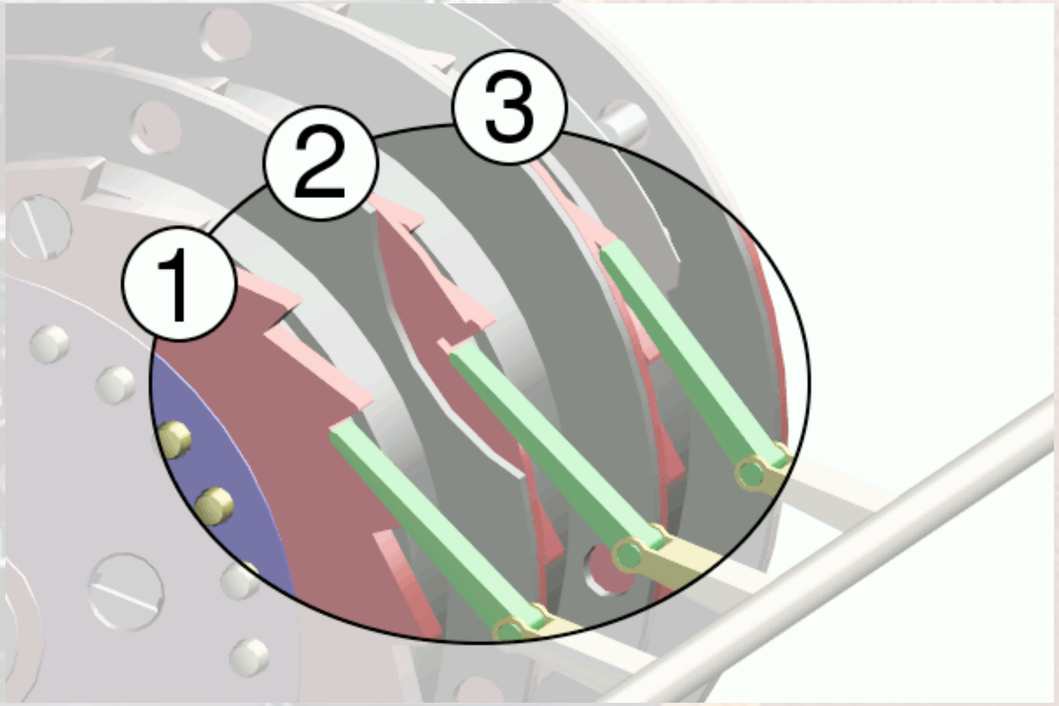


Stepping and Turnover

- The first rotor steps one position every time a key is pressed
- Notches on the rotors provide for the second and third rotors to turn over (step) each time the rotor to their right completes one full revolution
- Double stepping of the second rotor occurs when turning over the third rotor

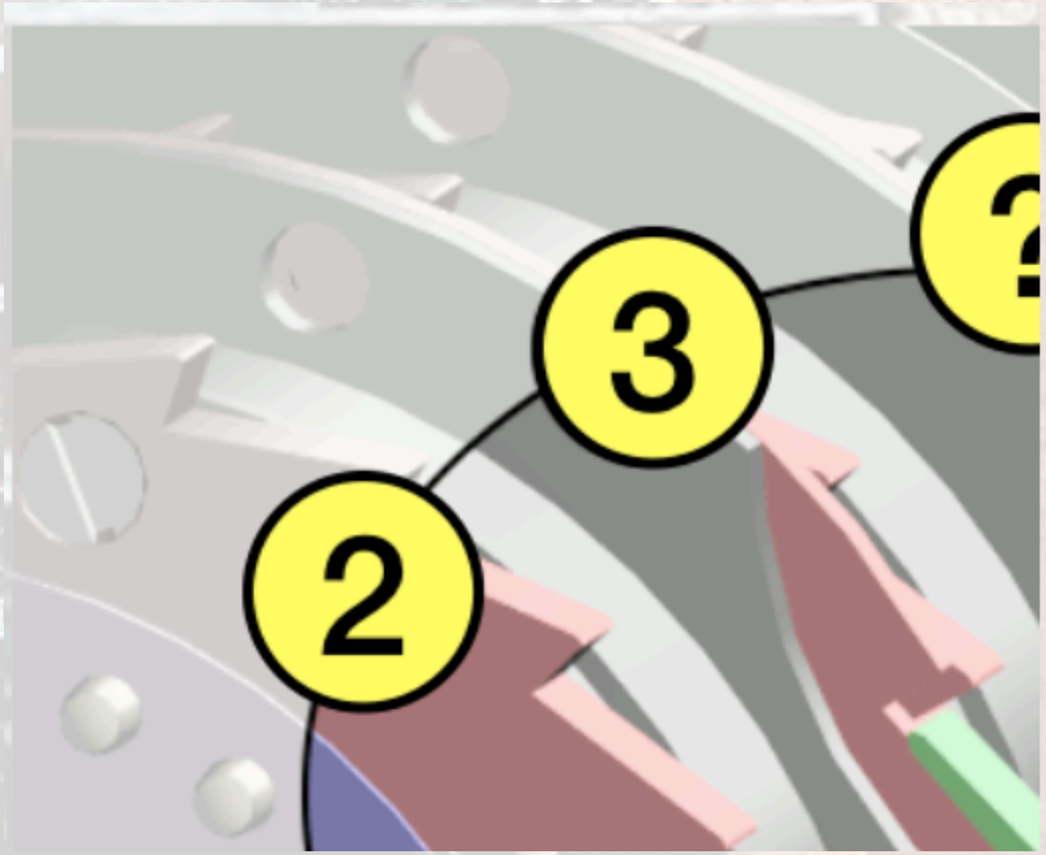
Pawls, Ratchets, and Notches

For the first rotor (1), which to the operator is the right-hand rotor, the ratchet (red) is always engaged, and steps with each keypress. Here, the second rotor (2) is engaged, because the notch in the first rotor is aligned with the pawl (green); it will turn over with the first rotor. The third rotor (3) is not engaged, because the notch in the second rotor is not aligned to the pawl, so it will not engage with the rachet.



Double Stepping

Here, the third rotor is engaged, because the notch in the second rotor is aligned with the pawl. The pawl will push the third rotor by the ratchet and the second rotor by the notch causing both rotors to step (Double Step)



Enigma Setup

- Wheel order (Walzenlage) – the choice of rotors and the order in which they are installed
- Ring settings (Ringstellung) – the position of each alphabet ring relative to its' rotor wiring
- Plug connections (Steckerverbindungen) – the pairs of letters in the plugboard that are connected together
- Which reflector to use (Umkehrwalze)

How Many Permutations!?

- The Enigma transformation for each letter can be specified mathematically as a product of permutations.

- The encryption transformation for a three rotor machine can then be described as:

$$E = P\left(\rho^{n} R \rho^{-n}\right)\left(\rho^{j} M \rho^{-j}\right)\left(\rho^{k} L \rho^{-k}\right) U \left(\rho^{k} L^{-1} \rho^{-k}\right)\left(\rho^{j} M^{-1} \rho^{-j}\right)\left(\rho^{n} R^{-1} \rho^{-n}\right) P^{-1}.$$

- Three rotors from a set of five (5x4x3), multiplied by each of the 3 rotor settings with 26 positions (26^3), multiplied by the plugboard with ten cables connected [26! / (6! x 10! x 2^10)], the military M3 Enigma has 158,962,555,217,826,360,000 different initial settings! (That's nearly 159 million, million, million.)

Code Books

- Codebooks were used to communicate the daily settings
- Delivered monthly/kept under lock and key
- Settings changed at Midnight Berlin Time
- Different levels of each command authority used different code books, therefore different daily settings

Geheim!

Sonder-Maschinenschluessel Januar

Nicht im Flugzeug mitnehmen!

Datum	Walzenlage	Ringstellung	Steckerbrett	Kenngruppen
31.	IV V I	12 15 18	GK OS CX WZ IU AF BY HM TD VL	fkt vxe ref iam
30.	IV III V	04 07 14	JH FW SU EP DV OK QM TI RG YA	mjt deo arx rhp
29.	V III II	10 20 22	OT LX GK HA EU JW VF YN CZ QI	xew lhn obi jxt
28.	I II IV	11 08 19	QY AN VE BT KL MS HO DC RP XW	ous jnv iqz vfi
27.	IV II V	16 09 20	BC TG DM AH VL UK FN XJ OI ZQ	cow avw xsf ali
26.	IV I II	04 06 24	OW FI TB KH AR ZX GE YM NL PJ	bqs lkk wvt jpe
25.	I II IV	11 01 16	PZ DG FV ST EQ BO NU YH KL RJ	hrx mnj fwf qzb
24.	V III IV	19 06 11	RS YG HU NM EX FT JC WI DP AL	nso wij jpw tte

Encoding a Message

- Set up the machine to the Daily Key
- Type in three(four) random letters - this is the Message Key- repeat the message key (it is encoded and sent twice!)
- Change the wheels to the Message Key
- Type in the remainder of the message

Decoding a Message

- Set up the machine to the Daily Key
- Type in the first six(eight) letters of the message which reveals the Message Key (sent twice!)
- Change the wheels to the Message Key
- Type in the remainder of the message except the last six(eight) characters which are a repeat of the message key encoded with the daily key (sent twice again!)

Enigma-E Kit

- Over 300 Components / Over 900 solder points
- 5.5 Hours assembly time plus 10 hours for the case
- 2/3 scale of a real mechanical Enigma
- Produces Audible Morse Code*
- Can be connected to a PC via RS232 port*

John Dean, K0JDD

Demonstration

- You are the radioman on U-516 in Norway on 16 April 1945 and have received a TOP Priority message

- The Signals Officer has set up your Enigma M4 machine to the daily key:
  UMKC // c215 // ASOD // AMZI
  AD LR ZJ XI BU KV SW FH EN MY

- Decode the message key (first eight characters)

- Change the rotor settings to the message key

- Decode the remainder of the message

Demonstration

HRQN SMAD LVIO DMMW JLKN

GSRJ VNLC IKGT MRDB IDAW

YLIK IFIF CMCG HRQN SMAD

Demonstration

HRQN SMAD LVIO DMMW JLKN
ASTV ASTV

GSRJ VNLC IKGT MRDB IDAW

YLIK IFIF CMCG HRQN SMAD
ASTV ASTV

Demonstration

HRQN SMAD LVIO DMMW JLKN
ASTV ASTV DERF UEHR ERIS

GSRJ VNLC IKGT MRDB IDAW
TTOT XDER KAMP FFGH TWEI

YLIK IFIF CMCG HRQN SMAD
TERX DOEN ITZX ASTV ASTV

Demonstration

The Führer is dead.

The fight continues.

Dönitz.

Vulnerabilities

- Code Book Security and Distribution
- A letter can not be encoded to itself
- Words common across many messages leading to the use of cribs (‘Wetter’ reports, ‘Heil Hitler’, etc…)
- Poor security procedures (i.e.sending message keys multiple times in fixed locations in the message) and bad habits/ laziness of individual radio operators (using the same message key in multiple messages, or the same messages keys in a recurring pattern over time)
- Hubris. The Germans believed Enigma to be unbreakable through the end of the war. Dönitz was incredulous when he was told about the code breaking after the war.

Code Breaking by the British

- Message Interception (HF was Britain's best Friend)

- Cryptanalysis
  - Frequency Analysis
  - Cribs

- Bombes and Wrens
  - 200 Bombes and 2,400 Wrens

  Bombe tries all 17,576 combinations of the rotor wheels at high speed looking for a certain word or pattern - stops once the key is found - average time to solve was 20 minutes machine time

- Translation and Classification

- Secure Distribution on a need to know basis

- Repeat every 24 hours…

- Over 10,000 personnel working on this in England alone…
  In secrecy…

Interesting Facts

- The Poles were reading ALL of the German Military Enigma I traffic before the war. They supplied the British and French with everything they knew just before Poland was overrun.
- The British were able to read MOST of the German Military Enigma M3/M4 traffic from 1940 onwards. This information source had the code name ULTRA and was closely guarded and distributed to only a select few

Interesting Facts

- The Allies had to be VERY careful on how they used the information they had, lest they tip off the Germans that the code was broken. (See disputed claims about Bombing of Coventry)
- Cover stories were always arranged when information was acted upon (i.e. Send over a scout plane and make sure they are spotted an hour before you start the attack on the target)

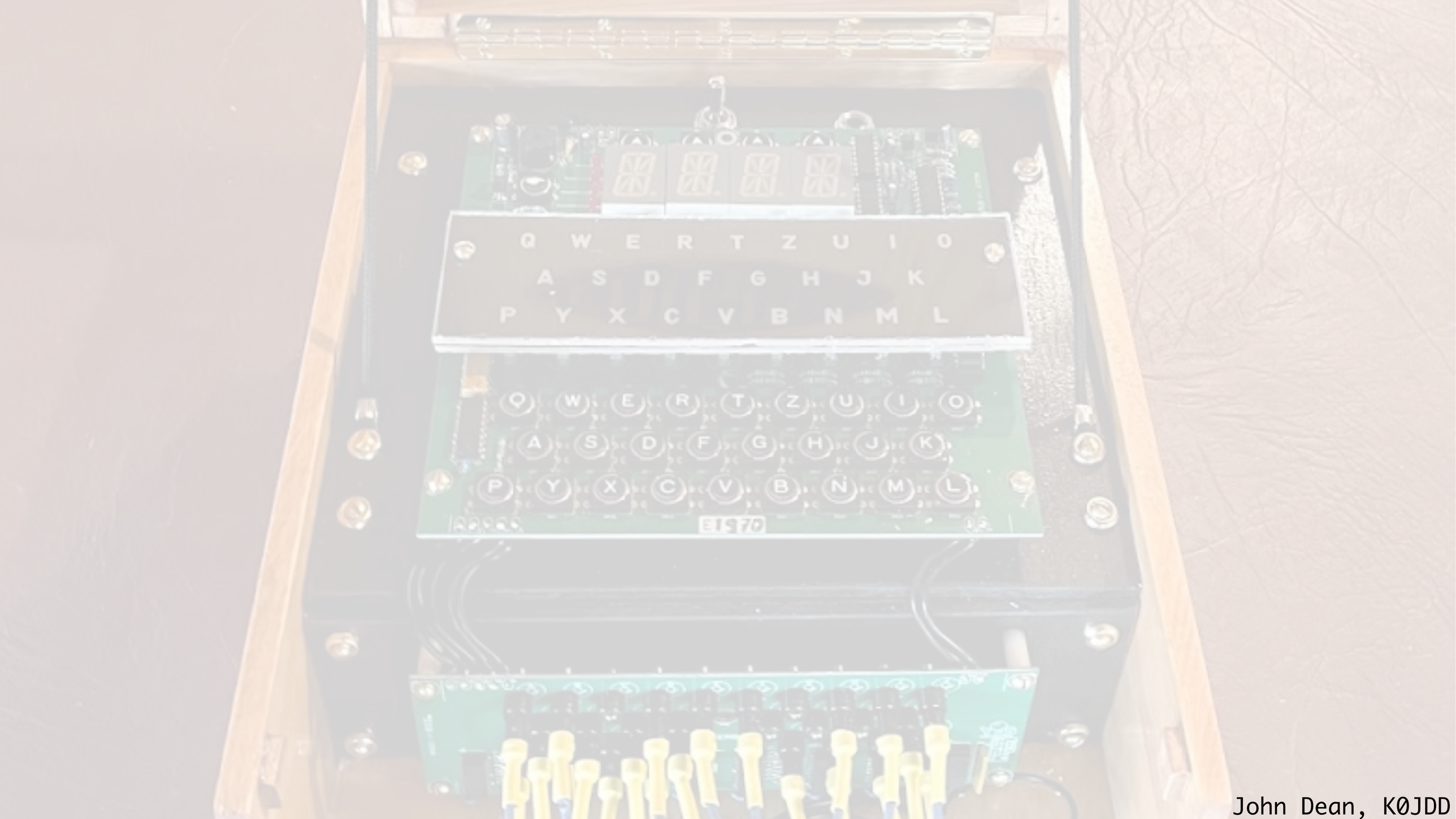
Resources

Google Search for “Enigma Machine”

Enigma Simulators Online
https://www.ilovefreesoftware.com/06/featured/free-online-enigma-simulator-websites.html

The Hut Six Story: Breaking the Enigma Codes
Welchman, Gordon ISBN 10: 0070691800 / ISBN 13: 9780070691803

The Ultra Secret
Winterbotham, F. W.ISBN 10: 0440190614ISBN 13: 9780440190615



John Dean, K0JDD