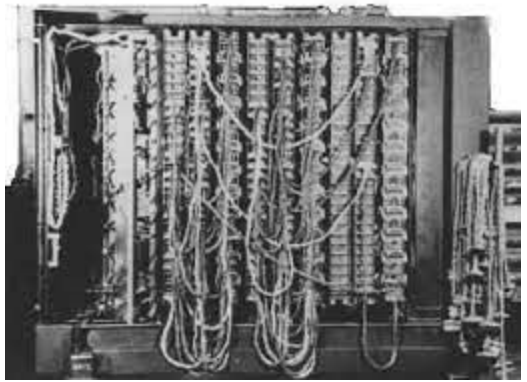
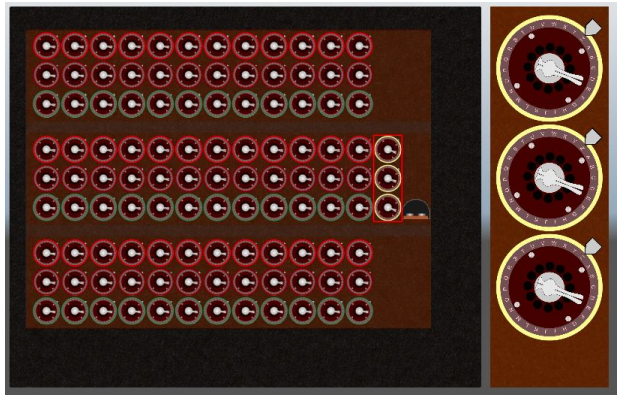
# Cracking the Enigma

Alexander McFarland
Robert Swanson

# Overview

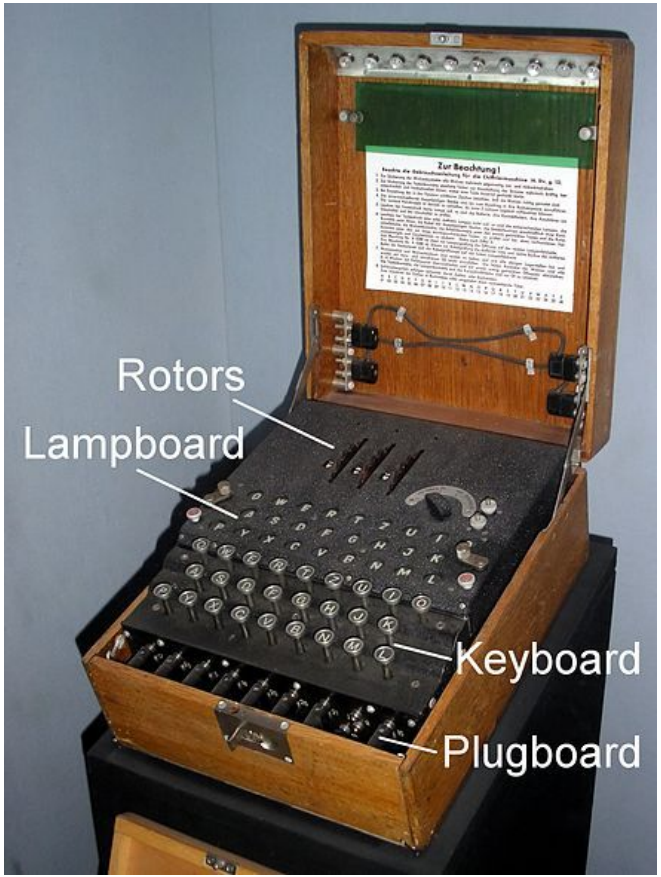
- Enigma Machine Recap
- Historical Context
- Breaking the Enigma
  - Vulnerabilities
  - Bletchley Park
  - Cribs and Menus
  - Banburismus
- The Bombe
- Bombe Simulation





# Enigma Overview

- Mobile enciphering machine originally developed in 1919 as a commercial product
- Polyalphabetic substitution cipher
- Components
  - Keyboard
  - Plugboard (Steckering board)
  - Rotors (Scrabbler)
    - Slower rotors were located further to the left in the machine
  - Lampboard
- Acts as a seeded random number generator



# Enigma Internals

- Pathway of encryption
  - Keyboard to plugboard to rotors to reflector to rotors to plugboard to lampboard
- “Unchanging” components
  - Keyboard to scrambler wiring
  - Rotor and Reflector wiring
  - Turnover notches of the rotors
- Varied components
  - Wheel ordering
  - Ring settings
- Frequently varied components
  - Plugboard settings (steckering settings)
  - Rotor starting positions

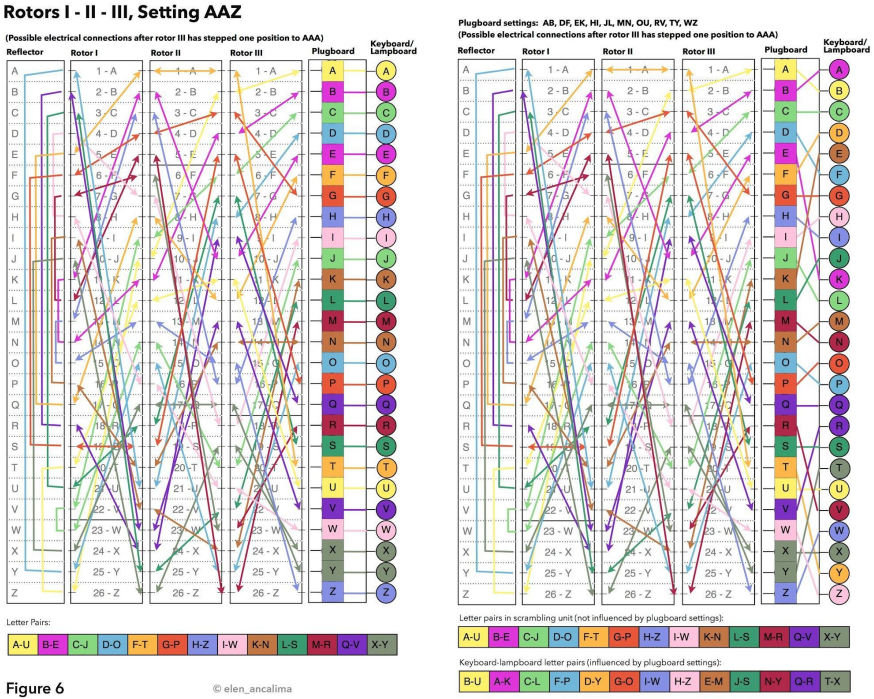



Figure 6 © elen_ancalima

# Enigma Variations

- Army and Air Force
  - 3 rotors out of 8 (originally 5)
  - Worked on in Hut 6 at Bletchley Park
  - Rotor selection and ordering
    - 336
  - Initial rotor positions
    - 26*26*26 = 17,576
  - Plugboard setting
    - 150,738,274,937,250
- Navy
  - 4 rotors out of 8
  - Worked on in Hut 8 at Bletchley Park
  - Rotor selection and ordering
    - 420
  - Initial rotor positions
    - 26*26*26*26 = 456,976
  - Plugboard setting
    - 150,738,274,937,250
  - Many more potential encryptions combined with more robust security requirements for operators made the Naval enigma much harder to break.
    - Over 32x the number of possible starting positions for encryption

# Historical Context

# US and British Bombes

## Great Britain

- *Victory*, the first bombe to arrive at Bletchley Park, came on 18 March 1940
- The next bombe to arrive was called *Agnus Dei*. It came on 8 August 1940 and included a diagonal board.
- 5 bombes were in use in June of 1941, and this number was raised to 15 by the end of the year.
- By 1943, Britain had 49 bombes and by the end of the war, they had 210 bombes in use.

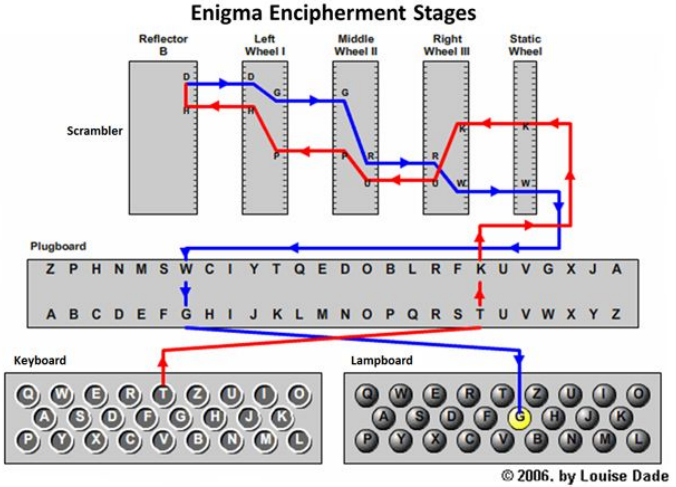
## United States

- The US Navy bombes were constructed in a similar manner to the British bombes, but were much faster.
- The first bombe was completed on 3 May 1943.
- After the US had bombes at their disposal, a transatlantic cable was used to communicate encryption and analysis information between Great Britian and the US.
- Often, Bletchley Park would forward tasks to the US bombes in order to save time, forming a sort of cryptographic cloud network.
- In total, the US produced 121 Navy bombes..

# Bombe:
# Breaking Enigma

# Weaknesses of the Enigma

- No letter could become itself
  - This was a result of the reflector construction and later seen to be one of the primary security flaws in the machine
  - This was important for the construction of menus which would allow steckering hypotheses to be made
- The plugboard was reciprocal
  - Important for the construction of the diagonal board which greatly reduced false stops for the bombes
- Operational error
  - Allowed for the construction of cribs
  - Unlikely that Enigma would have been broken without the substantial operator sloppiness that was present



# Bletchley Park

## General Workflow at the Park

1. Intercepted messages were sent to Bletchley Park, 51 miles NW of London.
2. Messages disseminated by category to various buildings (huts) within the compound. e.g. Hut 6 received army and airforce messages, and Hut 8 received navy messages.
3. The huts would work to decrypt the incoming messages and send them off to other huts (e.g. Hut 4) for analysis.
4. These decrypted messages, known under the codename of ULTRA, were dispatched to the relevant authorities.

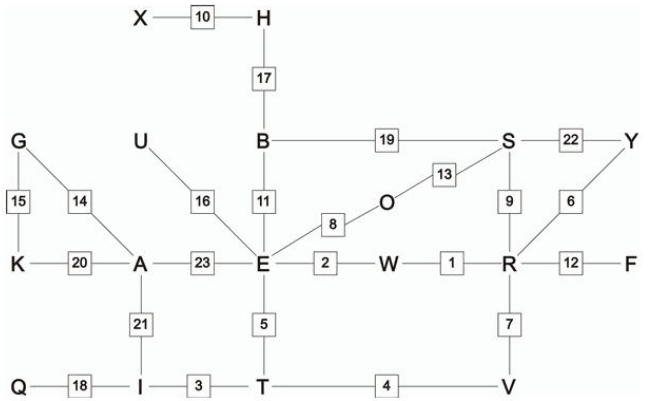
## Decryption Specifics

- The goal was to work out the wheel order, plugboard settings, and rotor starting positions for the enigma settings of the current day.
- First, a crib would be prepared for a cipher text.
- Next, the banburismus technique, devised by Turing, was used to eliminate certain wheel orders and reduce the possible enigma starting positions.
- From here, a menu would be constructed to test a particular steckering pair with the bombe.
- When the bombe produced a stop, provided that the other steckerings and ring settings were known, the encryption was tested using a checking machine known as a *Typex.*

# Cribs and Menus

- A crib is a known or suspected plaintext phrase in the ciphertext.
  - Phrases such as “*Keine besonderen Ereignisse*” or “Wettervorhersage” served as reusable cribs.
  - Determining cribs was critical for the decryption process, as it served as the foundation for working out potential encryption settings of the day.
- A menu is used to test a hypothesis of whether one letter is connected to another on the plugboard of the enigma machine.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R | W | I | V | T | Y | R | E | S | X | B | F | O | G | K | U | H | Q | B | A | I | S | E |
| W | E | T | T | E | R | V | O | R | H | E | R | S | A | G | E | B | I | S | K | A | Y | A |

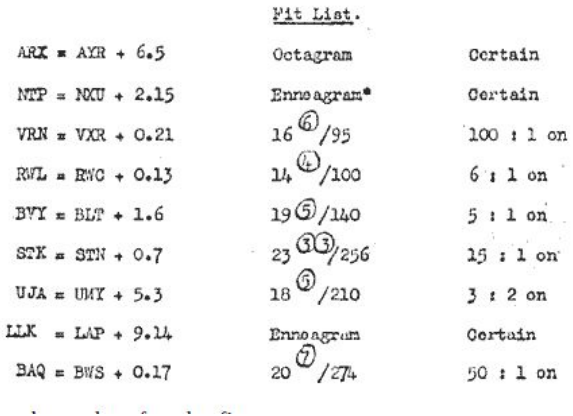


# Example Menu Construction

| **Ciphertext** | O | H | J | Y | P | D | O | M | Q | N | J | C | O | S | G | A | W | H | L | E | I | H | Y | S | O | P | J | S | M | N | U |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Position 1** | | | K | E | I | N | E | B | E | S | O | N | D | E | R | E | N | E | R | E | I | G | N | I | S | S | E | | | | |
| **Position 2** | | | | K | E | I | N | E | B | E | S | O | N | D | E | R | E | N | E | R | E | I | G | N | I | S | S | E | | | |
| **Position 3** | | | | | K | E | I | N | E | B | E | S | O | N | D | E | R | E | N | E | R | E | I | G | N | I | S | S | E | | | |
| | Positions 1 and 3 for the possible plaintext are impossible because of matching letters.<br>The red cells represent these *crashes*. Position 2 is a possibility. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

# Turing's Contribution

- Banburismus was a statistical method for narrowing possible machine configurations.
  - The goal of Banburismus was to avoid using precious bombe time on inefficient menus.
  - This technique utilized sequential conditional probability to determine the likely number of stops per rotor order.
  - In particular, this technique helped determine the starting positions for the two rightmost rotors.
  - This technique fell out of use in 1943 when bombe time was much more readily available.



Fit List.

| | | |
|---|---|---|
| ARX = AYR + 6.5 | Octagram | Certain |
| NTP = NXU + 2.15 | Enneagram* | Certain |
| VRN = VXR + 0.21 | 16 (6) /95 | 100 : 1 on |
| RWL = RWC + 0.13 | 14 (4) /100 | 6 : 1 on |
| BVY = BLT + 1.6 | 19 (5) /140 | 5 : 1 on |
| SZK = STN + 0.7 | 23 (3)(3) /256 | 15 : 1 on |
| UJA = UMY + 5.3 | 18 (5) /210 | 3 : 2 on |
| LLK = LAP + 9.14 | Enneagram | Certain |
| BAQ = BWS + 0.17 | 20 (7) /274 | 50 : 1 on |

Extensive "fit lists" like the one shown above were constantly being created in order to have a metric to compare potential machine settings.

# Bombe Internals

- A bank consists of 3 rotors, which represent the three rotors of an enigma machine.
    - Thus, each bank is the rotor portion of an Enigma machine, where the top rotor is the leftmost rotor.
- There are 36 banks total, arranged in 3 rows of 12 banks.
- On the back of the bombe, menu settings can be configured using a set of pole-jacks.
- Finally, switches on the sides of the bombe are set to test certain steckering hypothesis.
- Finally, there are three panel connectors on one side of the bombe that serves as a reflectors for each of the bank sets.

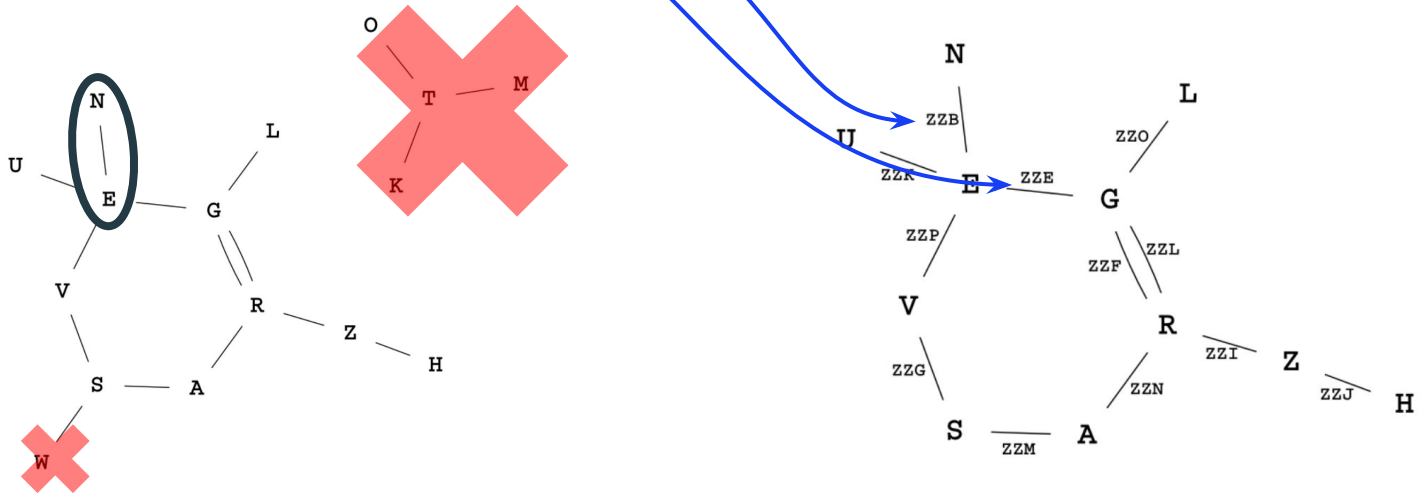
# Using The Bombe

# Step 1: Construct a Graph

| Letter Number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Clear | W | E | T | T | E | R | V | O | R | H | E | R | S | A | G | E |
| Cipher | S | N | M | K | G | G | S | T | Z | Z | U | G | A | R | L | V |

Goals:

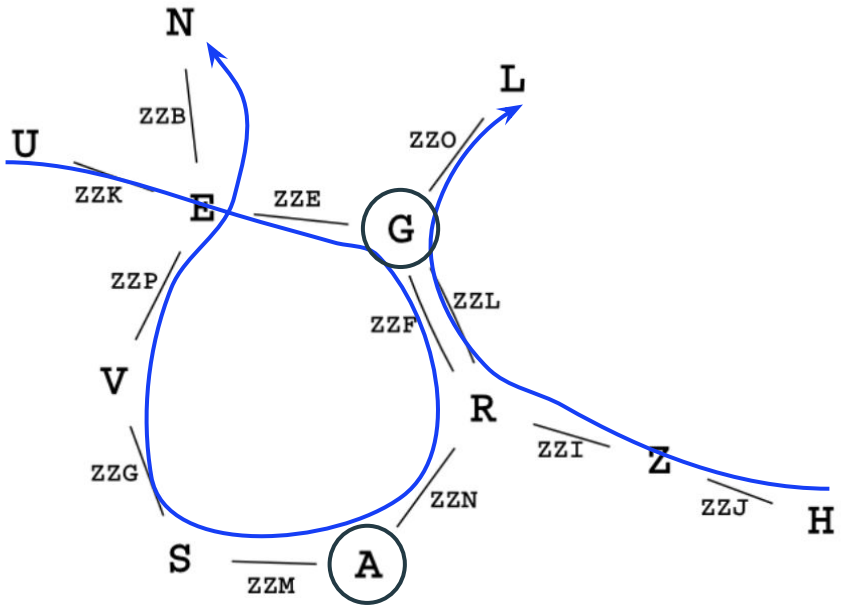
- One connected graph
- As many loops as possible
- ≤ 12 letters (for the 12 banks)



# Step 2: Choose a Route

Goals:

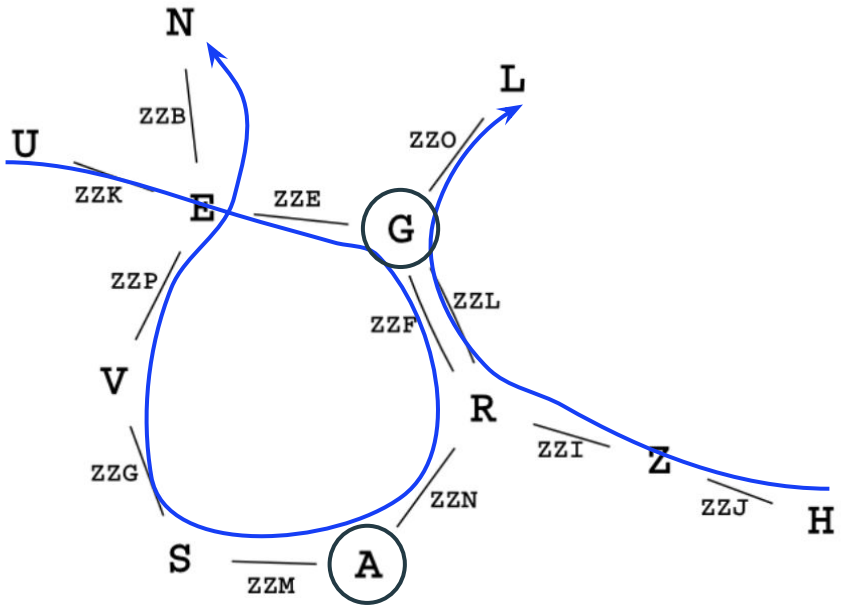
- Minimal number of routes to cover graph
  - U→E→G→R→A→S→V→N
  - Z→H→R→G→L
- Choose Input node thats shared between routes
  - G
- Choose Test Letter (not input or connected to input)
  - A



# Step 3: Create a Menu

This menu will test the hypothesis that **A was connected to G** on the plug board of the Enigma machine. However, due to the clever construction of the Bombe, even if this hypothesis turns out to be false (which is likely) we will still get the correct plugboard connections.

| | |
|---|---|
| 1: ZZK | U: 1 in |
| 2: ZZE | E: (1 out, 2 in), (7 out, 8 in) |
| 3: ZZF | G: (2 out, 3 in), (11 out, 12 in), input |
| 4: ZZN | R: (3 out, 4 in), (10 out, 11 in) |
| 5: ZZM | A: (4 out, 5 in), test entry |
| 6: ZZG | S: (5 out, 6 in) |
| 7: ZZP | V: (6 out, 7 in) |
| 8: ZZB | N: 8 out |
| 9: ZZJ | H: 9 in |
| 10: ZZI | Z: (9 out, 10 in) |
| 11: ZZL | L: 12 out |
| 12: ZZO | |

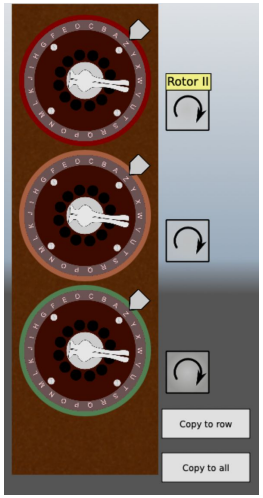


# Step 4: Allocate Bombe Time

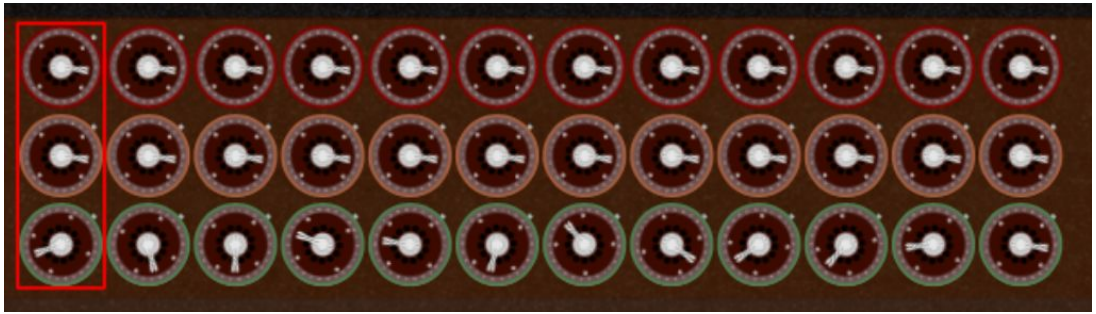
- Many bombes are needed to brute force the rotor selection and order (336 permutations)
- Each bombe can run 3 separate tests at a time (336/3 = 112 bombes)
- 211 Turing-Welchman Bombes were made (source)
- Each bombe testing this menu will be set up the same way except in rotor selection/order
- We will set up with the order we happen to know is correct: II, V, III

Bombe Simulator

# Step 5: Setup the Bombe Front (Rotors)




Configure Rotors Order

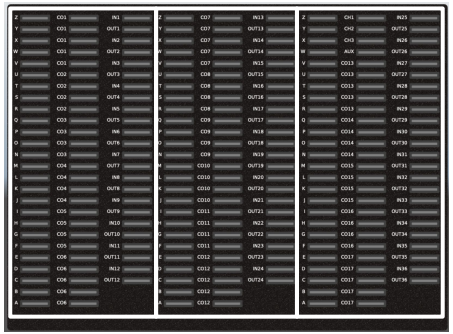


| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z |
| Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z | Z |
| K | E | F | N | M | G | P | B | J | I | L | O |

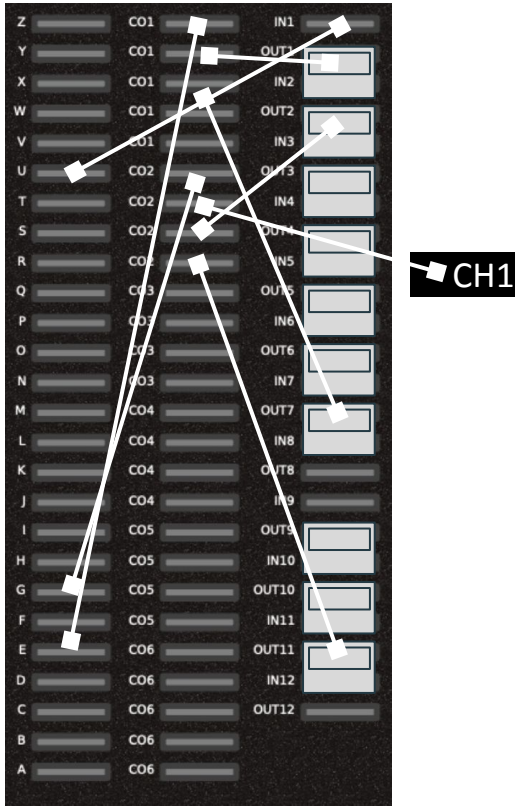
1: ZZK
2: ZZE
3: ZZF
4: ZZN
5: ZZM
6: ZZG
7: ZZP
8: ZZB
9: ZZJ
10: ZZI
11: ZZL
12: ZZO

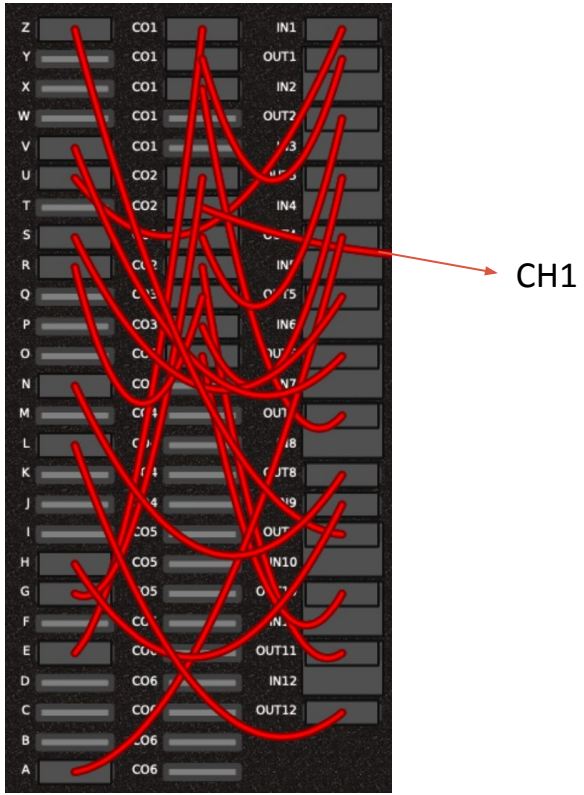
# Step 6: Setup the Back (Diagonal Board)

[Bombe Simulator]

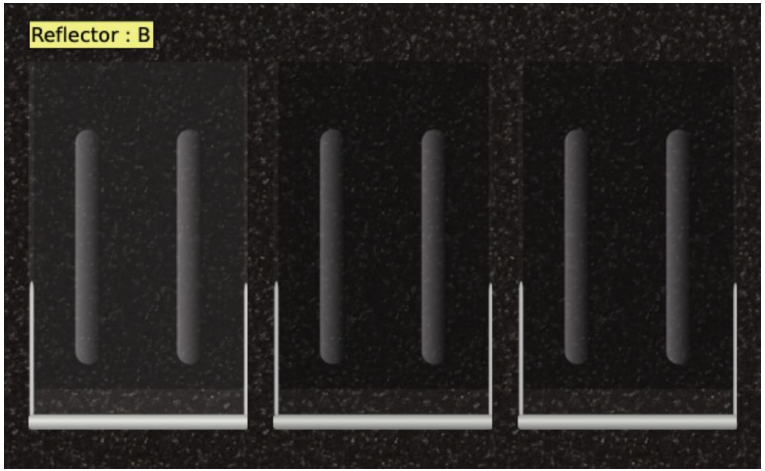


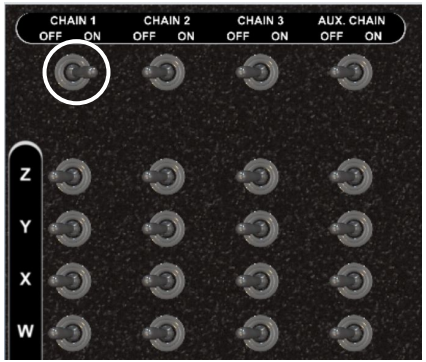
U: 1 in
E: (1 out, 2 in), (7 out, 8 in)
G: (2 out, 3 in), (11 out, 12 in), input
R: (3 out, 4 in), (10 out, 11 in)
A: (4 out, 5 in), test entry
S: (5 out, 6 in)
V: (6 out, 7 in)
N: 8 out
H: 9 in
Z: (9 out, 10 in)
L: 12 out



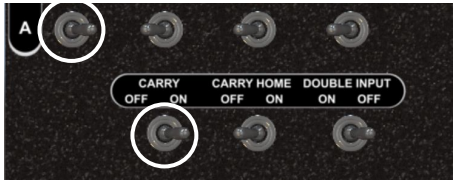



# Step 7: Setup Bombe Sides



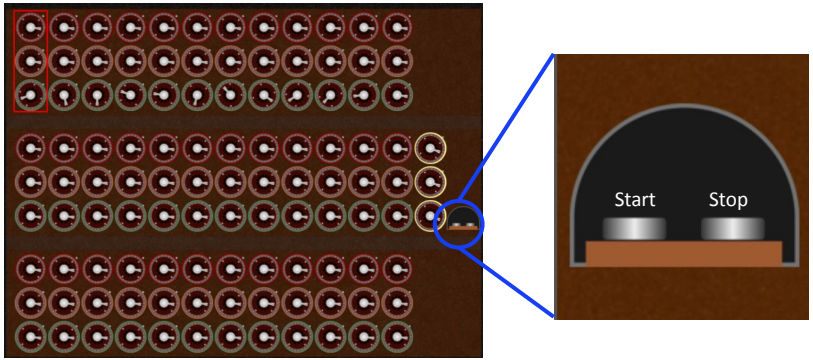




...

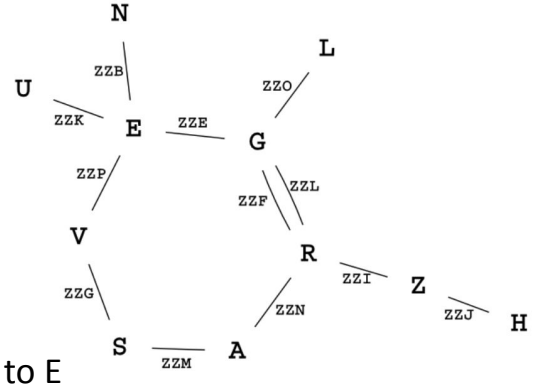


# Step 8: Start It!

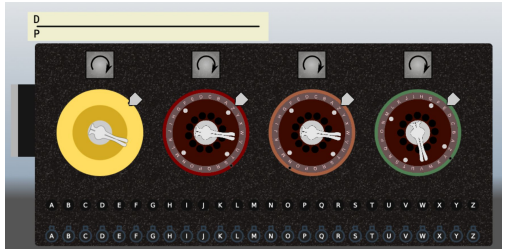
- The fast rotor rotates at 120 RPM
- 26 * 26 * 26 = 17,576 permutations
- 17,576 R / 120 RPM = 146 mins max
- In practice it took 20 minutes to run through the rotor order
- The machine stops when it has a guess




# Step 9: Use Checking Machine




- Find the hypothesis for the steckering of G on the right side (D)
- Find the hypothesis for the ring settings on the front (SNY)
- Setup checking machine rotor order, reflector, ring settings
- Find an edge connected to G (the input), we pick ZZE connecting to E
- Set the checking machine to the edge rotor settings, press what we think is steckered to G (D) and whatever lights up becomes the hypothesized stecker for E
- Using this hypothesis for E, repeat for each connected item and find a hypothesis for each letter
- If you find any repeats on the second row, that would mean that letter (X) is steckered to two letters (A and Z) which is impossible, so we reject our hypothesis
- Continue the machine



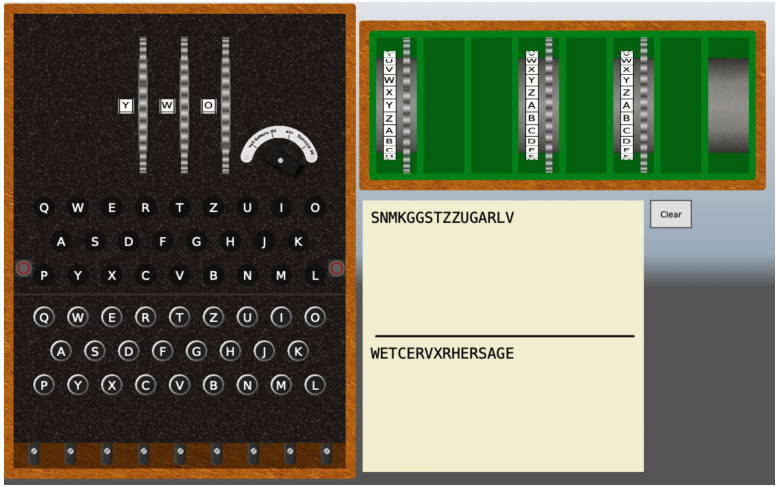
| U | E | G | R | A | S | V | N | H | Z | L |
|---|---|---|---|---|---|---|---|---|---|---|
| W | P | D | P | X | Q | I | T | H | X | O |

# Step 10: Use Enigma

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| U | E | G | R | A | S | V | N | H | Z | L |
| F | T | Q | R | D | S | N | V | M | P | J |

| Letter Number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Clear | W | E | T | T | E | R | V | O | R | H | E | R | S | A | G | E |
| Cipher | S | N | M | K | G | G | S | T | Z | Z | U | G | A | R | L | V |

- Once you find a non-contradictory steckering, test it with the enigma
- Set the rotor order, ring settings (DKX), rotor settings to YWY (to account for build error), and steckers to the hypothesis
- Try to decrypt the message to the crib
  - Cypher: SNMKGGSTZZUGARLV
  - Actual: WET**C**ERV**X**RHERSAGE
  - Expected: WET**T**ERV**O**RHERSAGE



# Step 11: Fix Hypothesis

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| U | E | G | R | A | S | V | N | H | Z | L |
| F | T | Q | R | D | S | N | V | M | P | J |

| Letter Number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Clear | W | E | T | T | E | R | V | O | R | H | E | R | S | A | G | E |
| Cipher | S | N | M | K | G | G | S | T | Z | Z | U | G | A | R | L | V |

- Cypher: SNMKGGSTZZUGARLV
- Actual: WET**C**ERV**X**RHERSAGE
- Expected: WET**T**ERV**O**RHERSA**G**E

- Possibilities for each mismatch
  - The actual and the expected letters should have been steckered togather
  - If contradictory, find who would be enchiphered to expected's (T) partner (C) at the ZZD rotor setting by using the checking machine (I), stecker actual with that letter (C, I)

# Step 12: Fix Hypothesis Beyond Crib

- We can decrypt the crib successfully, but if we continued with further encrypted text, it would probably eventually become nonsense as soon as a rotor turns over, or should have
- We probably have the correct stecker settings, but not the correct ring/rotor settings
- Can try each of the 26 settings per rotor manually (max 52 tries)

# References


- Wikipedia Contributors. “Cryptanalysis of the Enigma.” *Wikipedia*, Wikimedia Foundation, 7 Dec. 2021, en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma.
- Alexander, C.H.O'D. “Cryptographic History.” *Cryptographic History of Work on the German Naval Enigma*, 2007, www.ellsbury.com/gne/gne-000.htm.
- “The Turing Bombe and US Navy Bombe Simulator.” *Turing Bombe Simulator*, http://www.lysator.liu.se/~koma/turingbombe/.