

Bombe Project

(assuming prior discussion of enigma machine by other group)


Preliminary Research

[Bombe Simulator](#) | [Documentation](#)

Misc Links

- [Enigma Simulator](#)
- [The Turing-Welchman Bombe](#)
- [Enigma Sim from Hibschan](#)
- <http://accordingtobenedict.com/film-tv/enigma-chapter-4-how-does-the-machine-work-part-2/>
- [Banburismus](#)
- <http://www.ellsbury.com/bombe4.htm>
- <https://github.com/NationalSecurityAgency/enigma-simulator>
-

Videos

- <https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/case-study-ww2-encryption-machines>
- [The Enigma Machine Explained - YouTube](#)
- [Turing's Enigma Problem \(Part 1\) - Computerphile - YouTube](#)
- [Tackling Enigma \(Turing's Enigma Problem Part 2\) - Computerphile](#)
- https://youtu.be/kj_7Jc1mS9k?t=847
-  [Flaw in the Enigma Code - Numberphile](#)
- [Breaking Codes and Finding Patterns](#)
 - [Permutations - Minute 28](#)

Historical Background

Rotors I - II - III, Setting AAZ

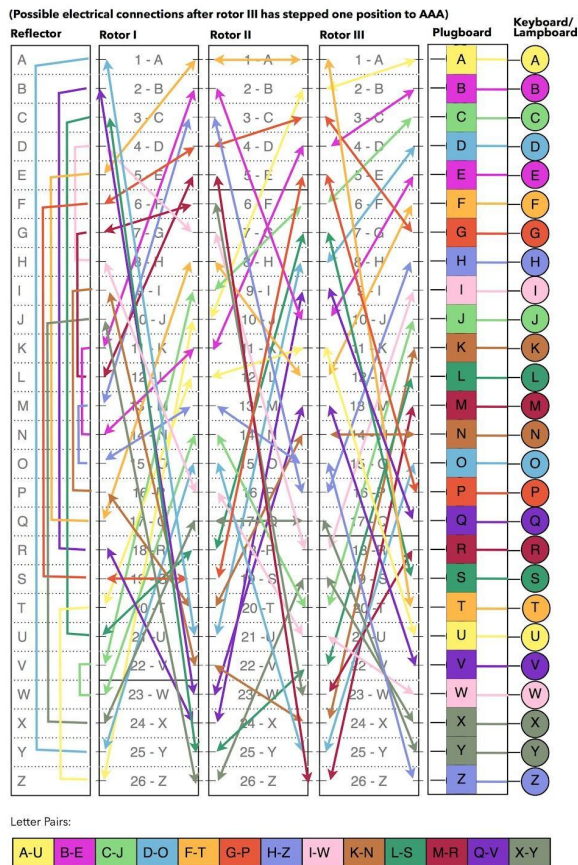
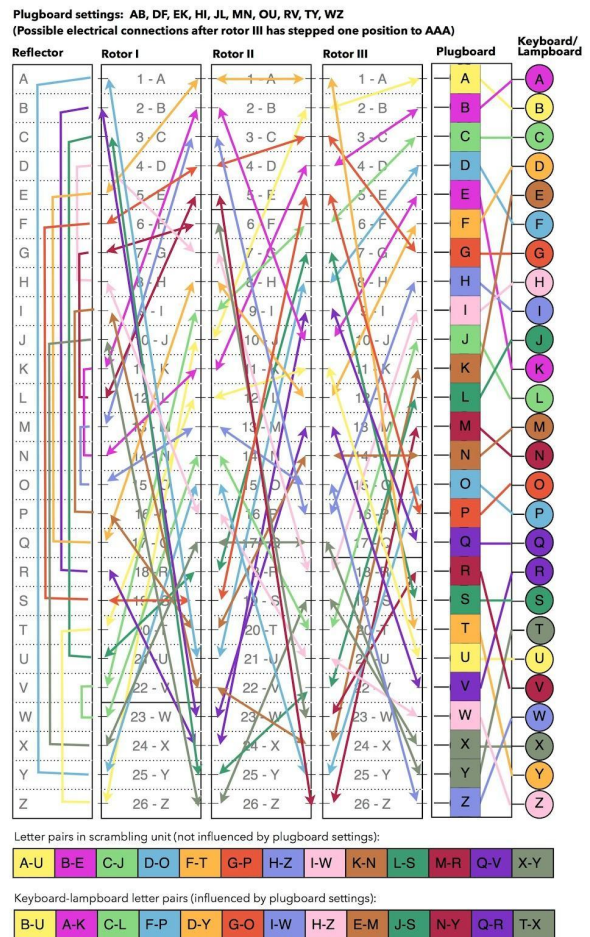
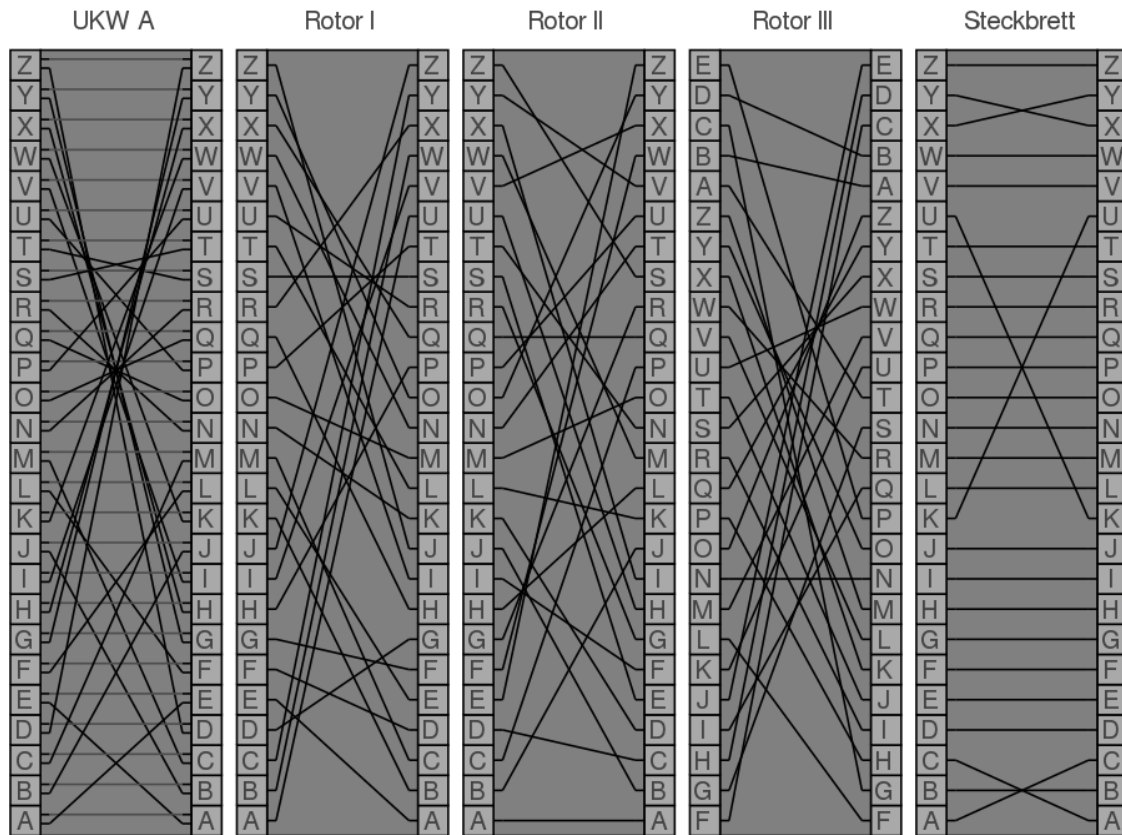


Figure 6

© elen_ancalima





- Different Kinds of Enigma Machines
 - Original mean for commercial use
 - Army/Air force use (3 rotors out of 5) (hut 6)
 - Naval use (3 or 4 rotors out of 8) (hut 8)
- 80 ish bombs made in Britain
- 100 ish bombs made in US
- Atlantic cabling connecting them to the US "cryptographic cloud"

Math

Alex

- Things you need to know about the configuration to decrypt message
 - Which of the 8 rotors are in use?
 - In what order?

- What is the ring setting for each rotor?
- Message setting?
- Plugboard settings
- Code cracking and statistics
 - Vigenere cipher
 - Broken with Kasiski method
 - Takes advantage of occurrences of repeated strings in the cipher which indicates that repeated plaintext words were encrypted by the same key letters
 - Coincidence index
 - William Friedman
 - Looking for “in depth” messages
 - Enigma
 - mechanical “one time pad”
 - Hardwired so that letter does not encrypt itself
 - Alan Turing
 - “The Applications of Probability to Cryptography”
 - Conditional probability and weighting evidence
 - Decibans
 - Measure amount of information
 - Used to build up measure of weight of evidence in favor of a hypothesis
 - Like Bayesian inference
 - Quantify support for one model over another
 - New evidence updates prior beliefs, rather than overwrite them.

LIKELIHOOD

The probability of “B” being True, given “A” is True

PRIOR

The probability “A” being True. This is the knowledge.

$$P(A|B) = \frac{P(B|A).P(A)}{P(B)}$$

POSTERIOR

The probability of “A” being True, given “B” is True

MARGINALIZATION

The probability “B” being True.

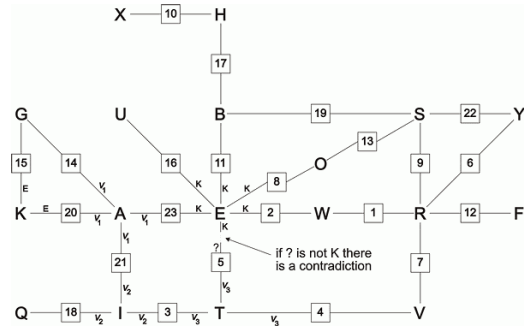
- Used for weighting evidence

| decibans | exact value | approx. value | approx. ratio | accurate ratio | probability |
|----------|--------------|---------------|---------------|----------------|-------------|
| 0 | $10^{0/10}$ | 1 | 1:1 | | 50% |
| 1 | $10^{1/10}$ | 1.26 | 5:4 | | 56% |
| 2 | $10^{2/10}$ | 1.58 | 3:2 | 8:5 | 61% |
| 3 | $10^{3/10}$ | 2.00 | 2:1 | | 67% |
| 4 | $10^{4/10}$ | 2.51 | 5:2 | | 71.5% |
| 5 | $10^{5/10}$ | 3.16 | 3:1 | 19:6, 16:5 | 76% |
| 6 | $10^{6/10}$ | 3.98 | 4:1 | | 80% |
| 7 | $10^{7/10}$ | 5.01 | 5:1 | | 83% |
| 8 | $10^{8/10}$ | 6.31 | 6:1 | 19:3, 25:4 | 86% |
| 9 | $10^{9/10}$ | 7.94 | 8:1 | | 89% |
| 10 | $10^{10/10}$ | 10 | 10:1 | | 91% |

- Bigrams and trigrams

Cracking methods:

- *"The task confronting Dillwyn Knox and Alan Turing, the primary British cryptanalysts, was to determine the particular settings of the Enigma machine used to encipher a particular message. Turing and Knox considered three possible methods of attack:"*
 - Ciphertext-only analysis
 - Discriminant attack
 - **Probable-phrase attack**
 - Find the crib (plaintext) for that day's traffic
 - Guess that a particular phrase appears in the message.
 - Line up guessed phrase with cipher text where there are no duplicate letters - this is the crib.
 - Determine which of the 107 sextillion(?) configurations give encryption of crib as seen in the message.
 - "Turing realised that some of these transformations have implications for other transformations and thus can be fed back into themselves to confirm consistency, or, more decisively, to demonstrate a contradiction."
 - Test a stecker hypothesis:



- c. "Turing realised that it was possible to represent loops of implications with electrical circuitry and that therefore it was possible to mechanise the search for those rotor orders and positions which satisfy the consistency conditions. The machine which he designed to perform this task is called the Turing bombe."
- d.

Engineering

Rob