Enigma Machine

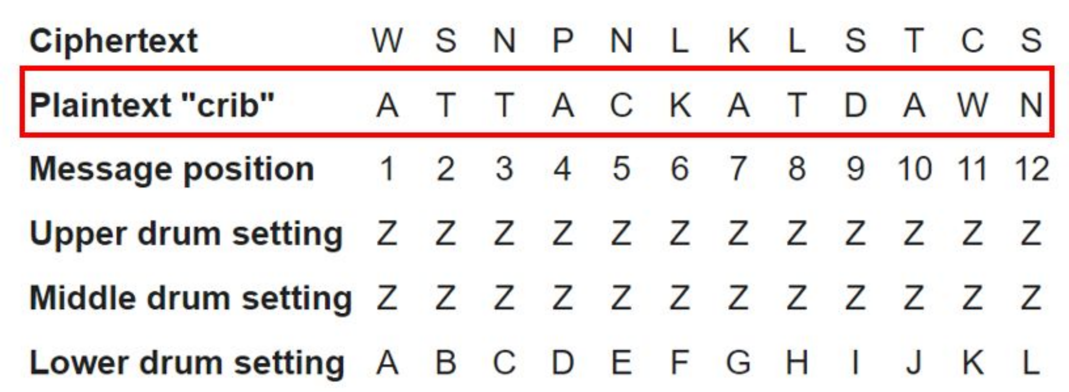
Breaking Germany’s Code

Shihwei Lin, Connor Claborn, Austin Espinosa, Edgar Tapia Maldonado

UC RIVERSIDE

- Introduction
- Alan Turing
- Enigma Machine
  - Mathematical Method
    - Encryption
    - Decryption
- Bombe Machine
  - Mathematical Method
    - Encryption
    - Decryption

Introduction



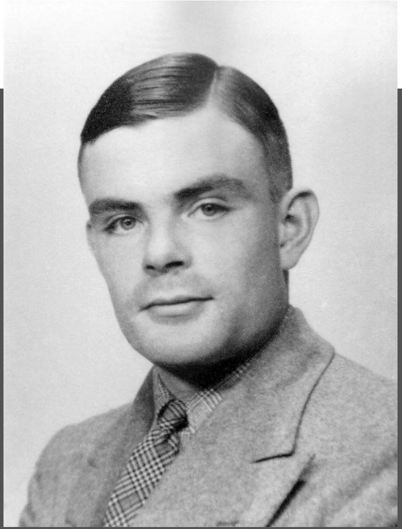
Ciphertext	W	S	N	P	N	L	K	L	S	T	C	S
Plaintext "crib"	A	T	T	A	C	K	A	T	D	A	W	N
Message position	1	2	3	4	5	6	7	8	9	10	11	12
Upper drum setting	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Middle drum setting	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Lower drum setting	A	B	C	D	E	F	G	H	I	J	K	L

- The Enigma machine and the Bombe machine are two fascinating technological inventions that played critical roles in the Second World War.
- The Enigma machine was a cipher machine used by the Germans to encrypt their military communications.
- On the other hand, the Bombe machine was developed by Alan Turing to decipher the encrypted messages sent by the Germans.

UC RIVERSIDE

Alan Turing

- Alan Turing was a British mathematician, logician, and computer scientist who played a critical role in breaking the German Enigma code during World War II.
- Turing is considered to be one of the founders of computing and artificial intelligence.
- Although Turing's contributions to computing and code-breaking were not recognized during his lifetime, he is now considered one of the most important figures in the history of computing and a hero in the victory against the Germans in World War II.



UC RIVERSIDE

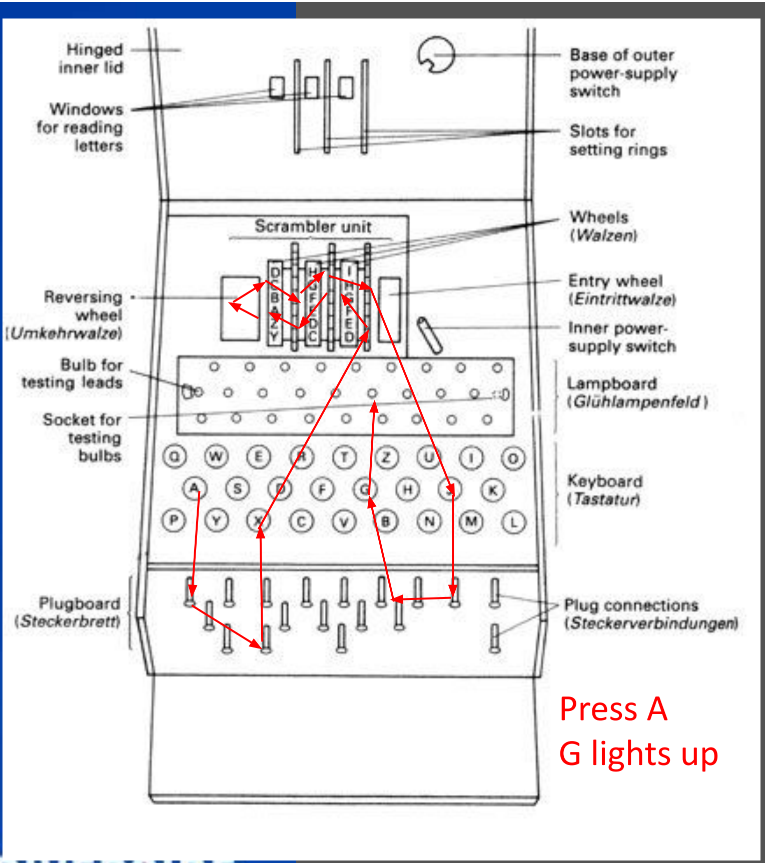
Enigma Machine

- The Enigma machine made it difficult for anyone to intercept and understand messages sent by producing a different cipher for every letter typed.
- The Enigma machine used a series of 26 rotors (each rotor corresponded to a letter in the alphabet) that were set in different positions to encrypt each letter of the message.
- To decrypt a message, the recipient needed to know the initial rotor positions and plugboard settings used by the sender (Key).
- Decrypting without these keys was a difficult and unbreakable–Germans believed–since there were over 1.5 x 10^{23} possible settings for the Enigma machine.

How the Machine Works

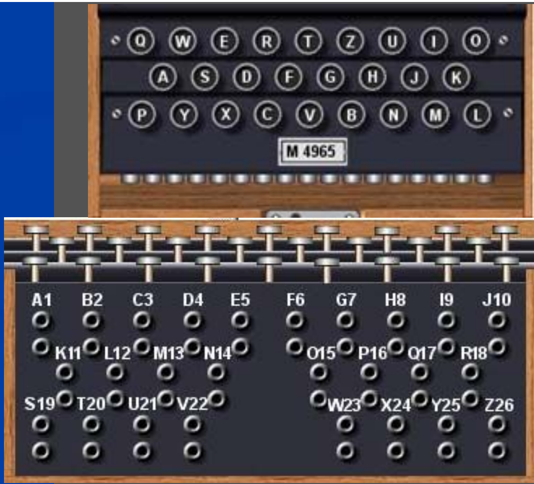
1) A single key is pressed, completing an electrical circuit
2) Travels to plugboard as one letter comes out as another
3) Travels to the rotors, changed three times by the three rotors
4) Changed one more time in the reflector
5) Travels back through the rotors, changing three more times
6) Goes to plugboard and changes letters one more time
7) Signal travels to lampboard and lights up output letter completing the cipher

Total of 9 possible changes!



Press A
G lights up

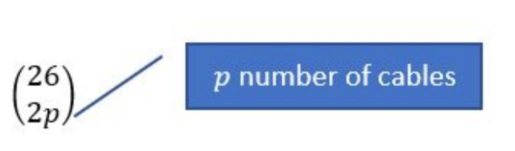
Mathematical Methods: Plug Board


Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
M 4965
A1 B2 C3 D4 E5 F6 G7 H8 I9 J10
K11 L12 M13 N14 O15 P16 Q17 R18
S19 T20 U21 V22 W23 X24 Y25 Z26

As mentioned before, the Enigma machine has 26 sockets for each of the letters in the alphabet. The plugboard connected each of these sockets with cables.

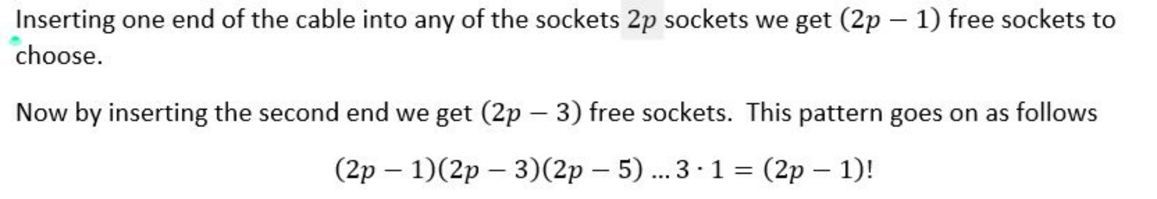
So we have 26 sockets and 13 cables.

Total number of cable combinations are…



$\binom{26}{2p}$

p number of cables

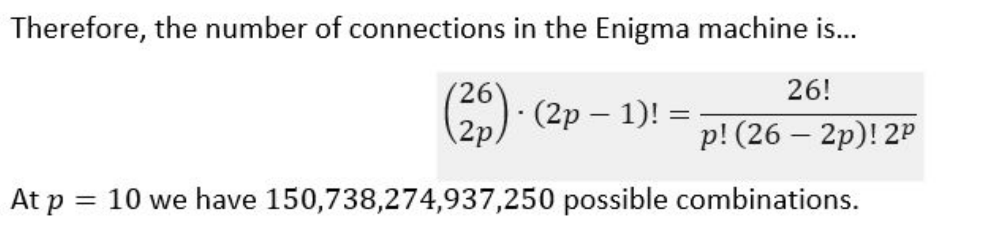


Inserting one end of the cable into any of the sockets $2p$ sockets we get $(2p-1)$ free sockets to choose.

Now by inserting the second end we get $(2p-3)$ free sockets. This pattern goes on as follows

$$(2p-1)(2p-3)(2p-5)\ldots 3\cdot 1=(2p-1)!$$

10 plugs were typically used during the war so p=10 here



Therefore, the number of connections in the Enigma machine is…

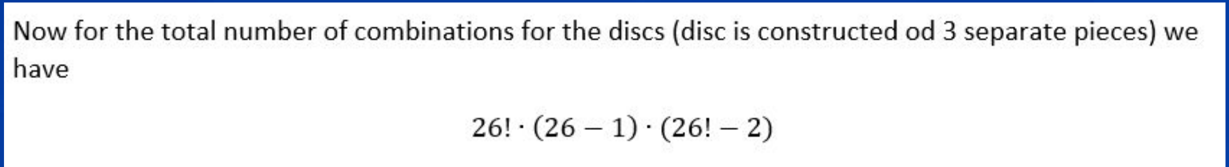
$$\binom{26}{2p}\cdot(2p-1)!=\frac{26!}{p!\,(26-2p)!\,2^p}$$

At $p=10$ we have 150,738,274,937,250 possible combinations.

Mathematical Methods: Rotors

-Set of 3 ordered rotors out of 5 total: 5 * 4 * 3 = 60 possible combinations

-For a single rotor, there 26! possible wirings, but this was impractical to manufacture, so set wirings were used. But if wirings were completely random:

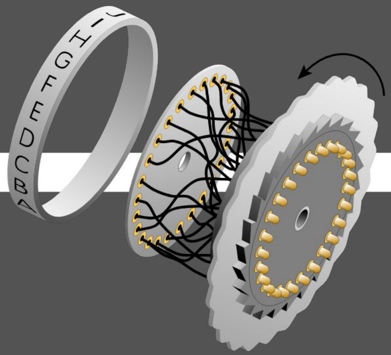


Now for the total number of combinations for the discs (disc is constructed od 3 separate pieces) we have

$$26! \cdot (26-1) \cdot (26! - 2)$$

-Internal rotation position: 3 rotors can start at any of 26 starting positions so 26*26*26 = 26^3 = 17,576 combinations for the internal rotation positions

-Position of notched rings: Only two rings need to be set with their notch rings 26*26 = 26^2 = 676



Mathematical Methods: Putting it all together

-Plugboard with 10 wires: 150,738,274,937,250

-Set of 3 ordered rotors out of 5 total: 60

-Internal rotation position: 17,576

-Position of notched rings: 676

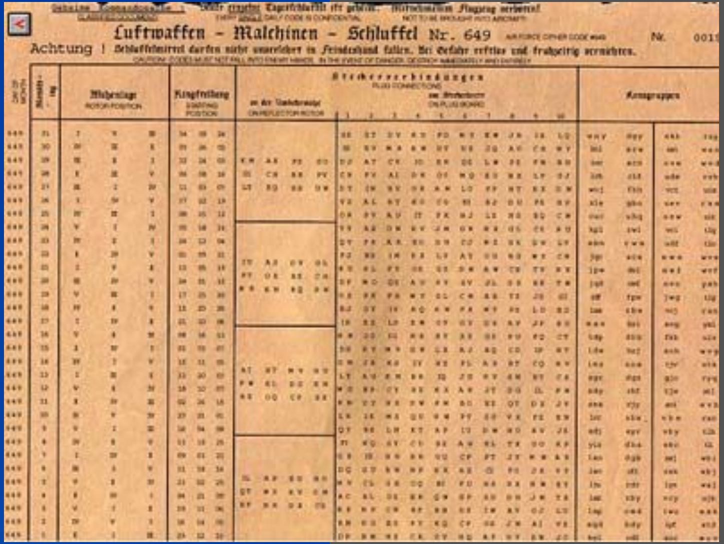
-Reflector: Only 1 possible combination

Together: 150,738,274,937,250 * 60 * 17,576 * 676 * 1

≈ 1 * 10^{23} possible settings!!!

-Thought this was enough to be unbreakable

1 * 10^{23} = 100,000,000,000,000,000,000,000



Luftwaffen – Maſchinen – Schlüſſel Nr. 649

Achtung !

German Key Sheet: Had the one out of 1*10^{23} combinations changed each day

How the Code was Cracked

- In order to decipher such a large number of combinations, Alan Turing and his team would need to implement a machine in order to crack the over 1 x 10^{23} possibilities the code could be for that day.
- Enter the Bombe containing 36 enigma equivalents that could run multiple jobs simultaneously.
- Implementation of digital circuits in order to greatly increase the rate of comparisons, finding contradictions in possible combinations, allowing for even faster speeds, recording previously ruled out combinations

UC RIVERSIDE

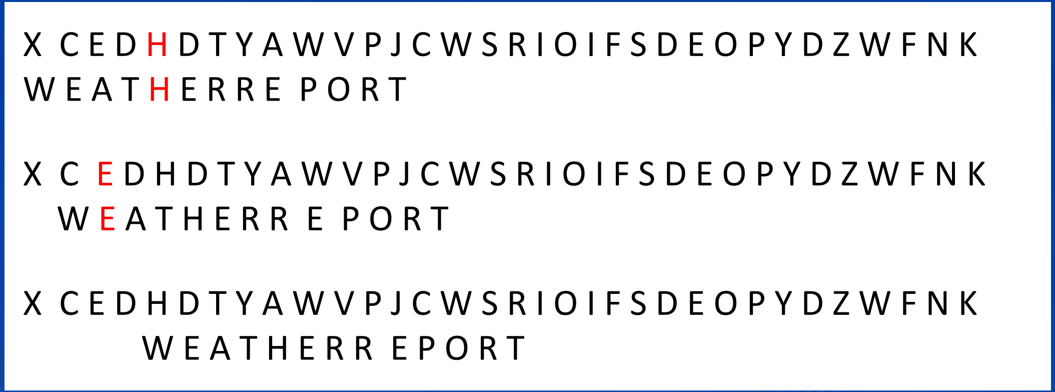
Cracking the Code: Brute Force

- The core of the Bombe’s methodology was a simple brute force approach.
- With no optimization, brute force would have the machine checking every possibility one by one until the correct sequence is found. The correct sequence would include the correct three rotors in the correct positions, all three with exact rotations, and all 10 wires plugged into the corresponding 20 letters on the plugboard.
- All of this would need to be determined within one day as the enigma settings were changed daily so any previous combinations were proved worthless.
- Serious optimizations to brute force would be needed because if not, $\Theta(n)$ algorithm, so in this case, 1 out of $1 * 10^{23}$ to get correct solution.

0 0 0 0	Incorrect
0 0 0 1	Incorrect
0 0 0 2	Incorrect
…	
2 3 0 4	Correct

Cracking the Code: A Weakness?

- One of the flaws of the enigma machine is that a letter can’t be encoded to itself.
- This allowed for a new optimization technique: cribs
- Cribs were words or phrases that you knew would appear in the plain text of the encrypted message.
- Example: Weather Report



```
X C E D H D T Y A W V P J C W S R I O I F S D E O P Y D Z W F N K
W E A T H E R R E   P O R T

X C E D H D T Y A W V P J C W S R I O I F S D E O P Y D Z W F N K
  W E A T H E R R   E   P O R T

X C E D H D T Y A W V P J C W S R I O I F S D E O P Y D Z W F N K
        W E A T H E R R   E P O R T
```

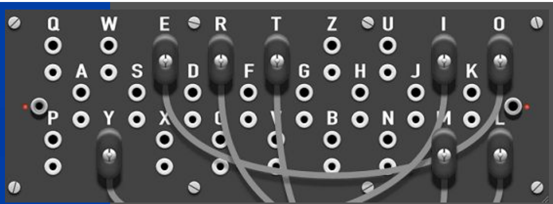
H mapped to H

E mapped to E

Possible Combination

- Could test possible settings against crib, allowed incorrect sequences to be thrown out much faster.

Cracking the Code: Strecker Values



- The main culprit for increasing amount of combinations is the plugboard. Finding these plugboard combinations, called strecker values, were very time consuming.
- Example of Optimization: Press T on keyboard,
  - We can guess P(T) is connected to P(A), goes through rotors, comes out P(P) so we can deduce P(P)-P(E)
    - More tests of rotor combinations:
    - Press T, G Lights, P(T)-P(A), goes through rotors, comes out P(K) so we can deduce P(K)-P(G)
    - Press T, B Lights, P(T)-P(A), goes through rotors, comes out P(X) so we can deduce P(X)-P(B)
    - Press T, G Lights, P(T)-P(A), goes through rotors, comes out P(T) so we can deduce P(T)-P(G)
  - We deduced T-G are connected, but we assumed T-A. It can’t be both so CONTRADICTION!
  - So T-A is wrong, and once we find the contradiction, all other deductions, K-G and X-G are also wrong so they don’t need to be checked again. Decreased amount of comparisons and increased efficiency greatly.
  - Also performed through electrical circuits in the Bombe, comparisons almost instantaneous.

Could go through all rotor combinations in 20 minutes!

UC RIVERSIDE

Cracking the Code: Checking Sequences

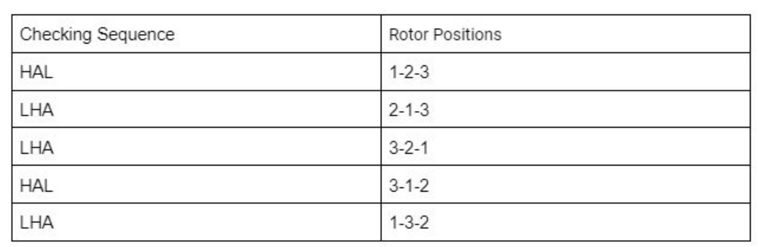
- Checking sequences were repeating patterns of letters that appeared in the encrypted message.
- These patterns were used to identify the positions of the rotors in the Enigma machine.
- By comparing the positions of the rotors in different parts of the message, the Bombe machine could deduce the correct rotor order.
- The technique was especially useful for decrypting messages that had been enciphered with a message key, as the rotor order would be reset for each message.
- The use of checking sequences helped to greatly speed up the decryption process, as it allowed the Bombe machine to eliminate incorrect settings more quickly.

UC RIVERSIDE

Cracking the Code: Checking Sequences

If a ciphertext message was encrypted with an Enigma machine, we can identify the rotor order by detecting recurring letter sequences like "HALHALHAL" (where "HAL" is the check sequence).

- First, we divide the ciphertext into groups of three letters, since the Enigma machine encrypts three letters at a time. and note the positions of the checking sequence "HAL" in the ciphertext.



Checking Sequence	Rotor Positions
HAL	1-2-3
LHA	2-1-3
LHA	3-2-1
HAL	3-1-2
LHA	1-3-2

- Look for patterns in the rotor positions that appear in the table.
- We can test each possible rotor order by trying all possible plugboard settings and seeing which one produces the correct decrypted message.

Cracking the Code: Banburismus

- Banburismus was a cryptanalytic process of finding overlapping encryption cycles
- This could be accomplished by using the German navy codes which had the same initial rotor positions, or indicators, for a given set of days. Normally no two enigma codes had the same initial positions for the rotors, but it was possible that the rotors for one message would become aligned to the initial positions of another message partway through a message, thus the two messages were “in depth” with each other
- In regular language, if two sentences in English and German were to be written next to each other there is a good chance that the same letter would appear next to each other in both sentences. This principle was then taken and applied between messages by comparing messages that differed only by the third indicator/rotor
- For example: Message 1 - T J I U L D G V Matching same letters within +/- 25 offsets

  Message 2 - I K R D G B M Z

- This message pair is in depth with 6 letter overlap

UC RIVERSIDE

Cracking the Code: Banburismus (Continued) Scritchmus

- After a message pair is found, an equation is derived that represents the varying letter offset from the third indicators, so if the Message 1 initial position indicators are RNS and Message 2 is given as RNK, then from the messages in the example get that S = K + 3 or M1 = M2 + offset
- They then string together multiple message pair equations together to produce a chain to solve an “end wheel alphabet” (the combinations in which the chain fits in the alphabet)
- For example if there is s = k + 3, k = a + 3, a = f - 2, giving the chain “a - f k - - s”
- Then the chain is incrementally compared with the alphabet without self-ciphering or reciprocal combos

a - f k - - s	a - f k - - s	a - f k - - s
a b c d e f g…	…f g h i j k l…	a b c d e f g h…
Not possible	Not possible	Possible solution

Where the number of possible solutions is

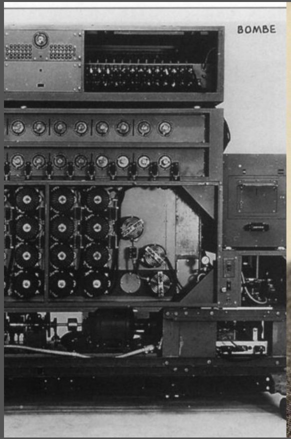
$$P = \{\textstyle\sum^{26}_{i=1} (x_{i+a(1)} * \ldots * x_{i+a(n)}) \mid x_{i+a(n)}=\{x_{b(z)}=0\},x=1\}$$

Where a(n) is the position of the letter in the chain (starting at 0 and including dashes as unused positions) and b(z) is the position of the letter from the chain in the alphabet (starting with A at 1)

This gives 10 possible solutions to decode this message

Conclusion: Enigma and the Bombe

The Bombe machine was a crucial invention during World War II. It helped the Allies decode secret messages sent by the German military using the Enigma machine. Its invention became a significant milestone in cryptography and it had a significant role in ending the war by providing critical intelligence about Germany’s military plans and strategies. The Bombe machine’s success further advancements in computing technology and cryptography, shaping the era of information security. Today, the Bombe machine, and Enigma machine stand as a testament to the ingenuity and perseverance of those who worked diligently to crack the Enigma code and played a significant role in bringing an end to World War II.



Questions

1. If each enigma machine came with a set of 10 rotors and required 5 to be inserted at once, how many possible rotor arrangements are there?

2. What was the role of the Enigma machine during World War II and how did the Allies manage to crack its codes?

3. What was the process of operating and programming the Bombe machine, and how did it differ from the Enigma machine?

Sources

"Alan Turing." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 6 Mar. 2023, https://www.britannica.com/biography/Alan-Turing.

"Exploring the Enigma." *Plus Maths*, 1 Mar. 1970, https://plus.maths.org/content/exploring-enigma.

"How Did the Enigma Machine Work?" *YouTube*, YouTube, 11 Dec. 2021, https://www.youtube.com/watch?v=ybkkiGtJmkM.

Prasad, Kalika, and Munesh Kumari. "A Review on Mathematical Strength and Analysis of Enigma." *ArXiv.org*, 17 Apr. 2020, https://arxiv.org/abs/2004.09982.