# The Enigma Machine and the Bombe: Cryptology during WWII

Lecture notes of Alexander Wood
CSCI 360 Cryptography and Cryptanalysis
awood@jjay.cuny.edu

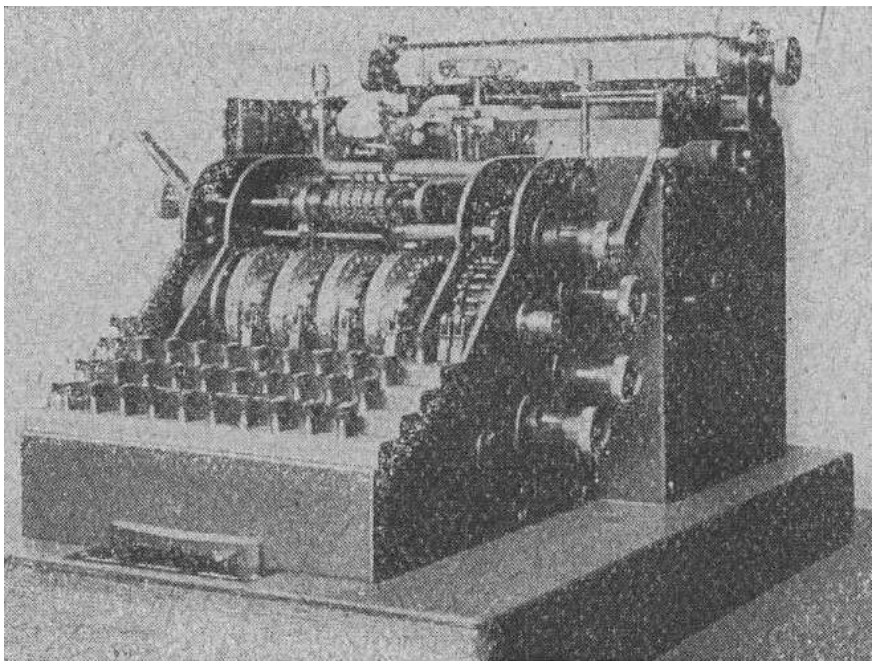
John Jay College of Criminal Justice

# The Enigma Machine

The Enigma Machine was designed by the German engineer Arthur Scherbius. He began manufacturing the machine in 1923, shortly after which it was adopted and manufactured by the German navy, army, and air force.

Arthur Scherbius

# Enigma Model A



from cryptomuseum.com

The first design of the Enigma machine, called Model A, weighed 50 kg and was similar in size to a cash register.

“Enigma” is German for “riddle.”

# Enigma Model B & C


Model D

Model C, with first light-up board

# Portable Enigma

Starting with model C, the Enigma was a portable device which looked similar to a typewriter.


Enigma Model D

Due to the Enigma Machine the German army had the strongest cryptographic cipher which existed at that point in time.

# How Enigma Works

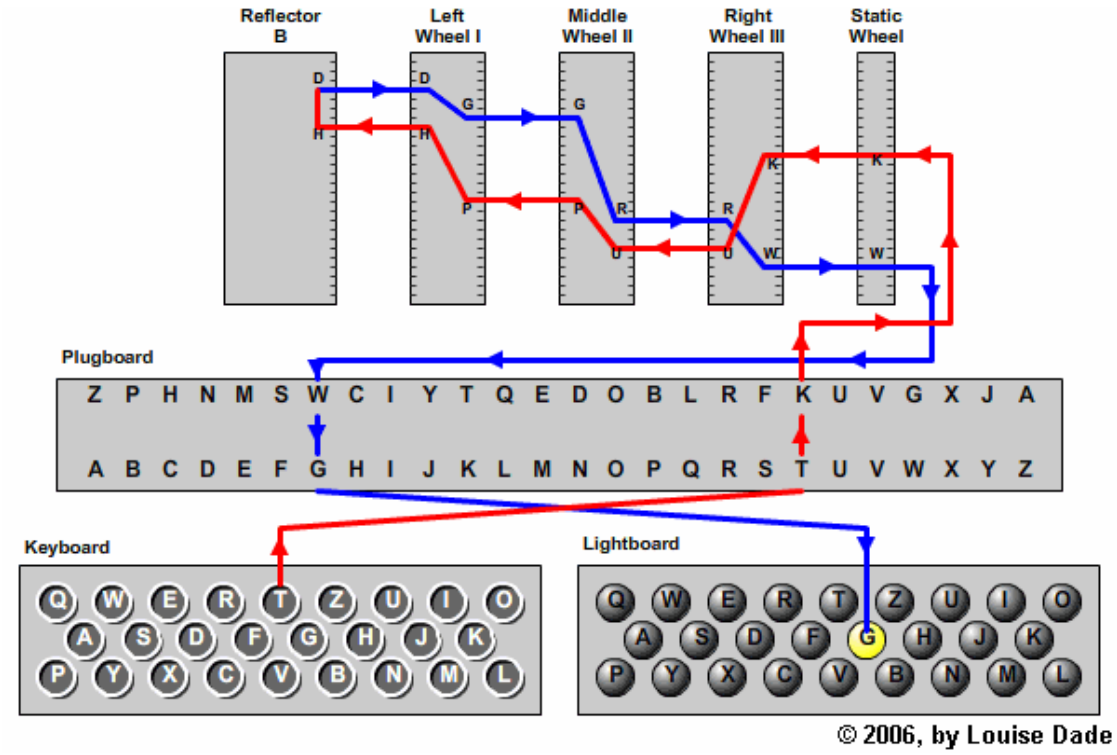
To encrypt a message, starting with the first letter you press down on its key on the keyboard. Above the keyboard, a letter lights up which represents its ciphertext.


It is decrypted using the same process, where typing in the ciphertext letter caused the plaintext letter to light up.

Let's start by watching the following video on how the Enigma machine works:
`https://www.youtube.com/watch?v=ASfAPOiq_eQ`

# The Path

The electrical current sent out by typing in a letter originated at the keyboard and went through several steps: the **plugboard**, the **rotors**, the **reflector**, then back through the rotors and plugboard to the **lampboard**.



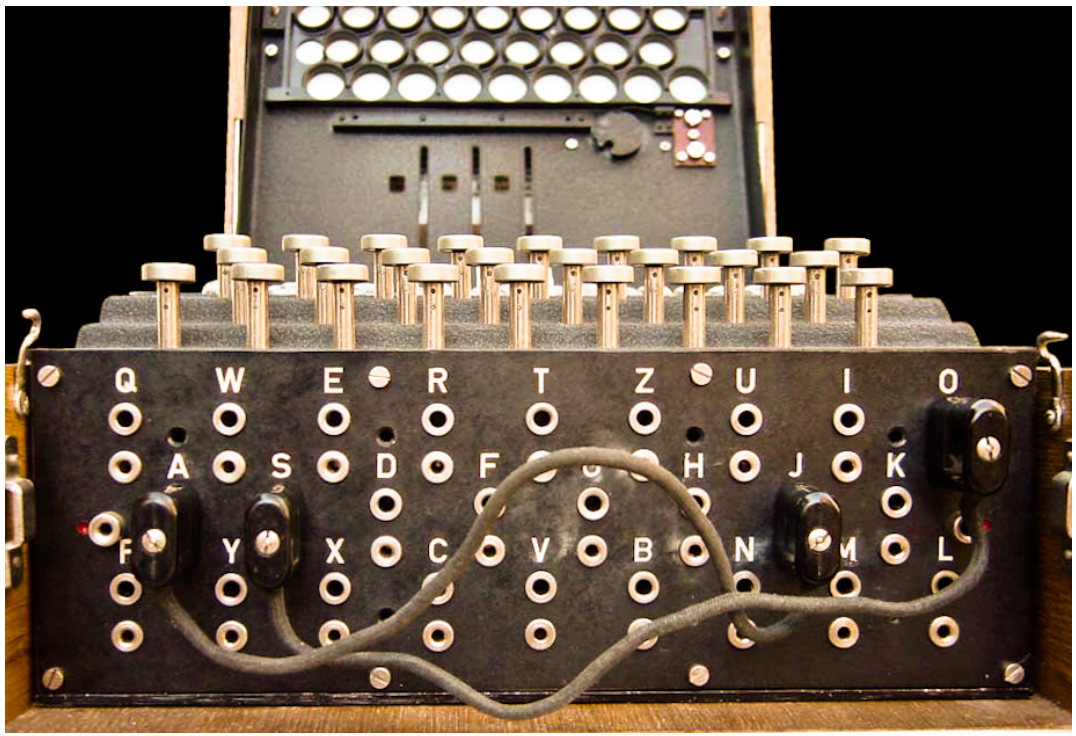

Graphic from: `http://enigma.louisedade.co.uk/howitworks.html`

# Keyboard

Pressing on the letter sends an electrical charge through the machine.

# Plugboard

This signal first goes through the **plugboard**.




The plugboard uses **plugs** to wire up one letter to another, diverting its signal. If ‘A’ is plugged in to ‘F’, then the letter will now be interpreted by the machine as an ‘F’.

# Plugboard

Later versions of the machine used 10 plugs to connect pairs of letters.


**How many ways were there to connect pairs of letters on the enigma machine?**

# Plugboard Combinations

**How many ways were there to connect pairs of letters on the enigma machine?**

There are $\binom{26}{2}$ ways of plugging in the first wire. For each of these combinations there are $\binom{24}{2}$ ways to plug in the second wire, and for each of those combinations there are $\binom{22}{2}$ ways to plug in the third wire, all the way down to $\binom{8}{2}$ ways of plugging in the tenth wire.

After multiplying this out, we must divide by 10!, the number of ways to permute these wires – since the order in which the pairs of wires are selected does not matter.

# Plugboard Combinations

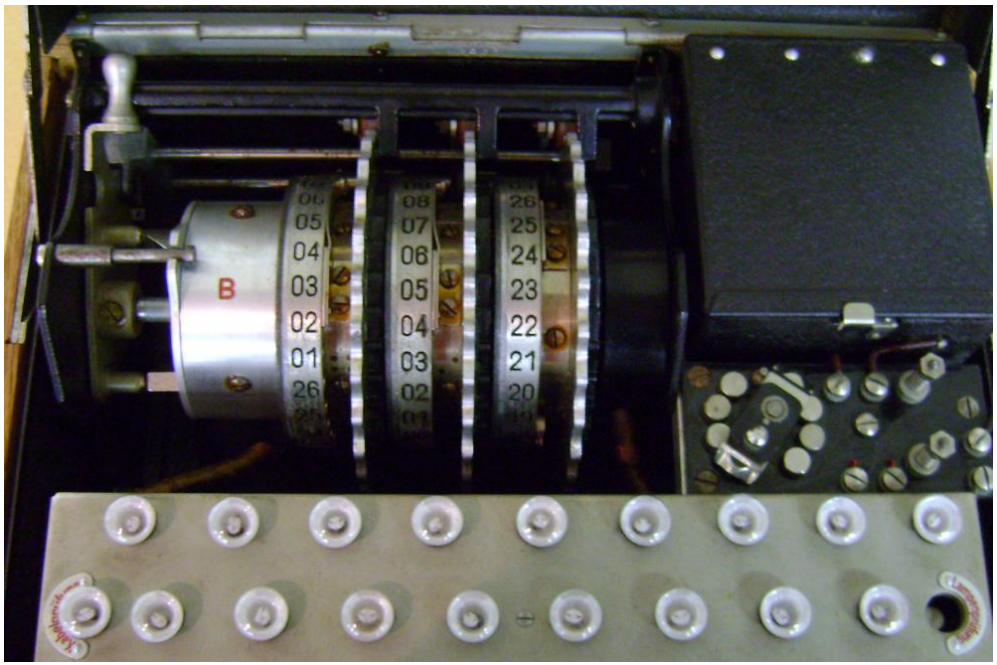
This yields a total of

$$\frac{\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}\binom{14}{2}\binom{12}{2}\binom{10}{2}\binom{8}{2}}{10!}$$

combinations, which works out to be

$$150,738,274,937,250.$$

# Rotors




After going through the plugboard, the electrical charge is sent through three **rotors**. Each rotor permutes the letters, taking it in and outputting a different letter. The letter bounces off a reflector at the end, passes back through the rotors, and then the board lights up with the encrypted output.

# Inserting Rotors

The rotors can be taken out of the machine. The machine has five rotors, and three of these are chosen to go into the three slots. **How many ways are there of positioning the five rotors in the three slots?**

There are

$$5 \times 4 \times 3 = 60$$

ways of choosing the rotors' starting positions.

# Rotor Movement

The machine was designed so that the rotors would... rotate! After typing in the first letter, the first rotor “clicks” and rotates into a second position. It rotates through all 26 positions, then the second rotor “clicks”, and after going through all positions on the second rotor the process repeats again with the third rotor. This leads to

$$26 \times 26 \times 26 = 17,576$$

possible combinations before encryptions begin to repeat!

# Rotor Positions

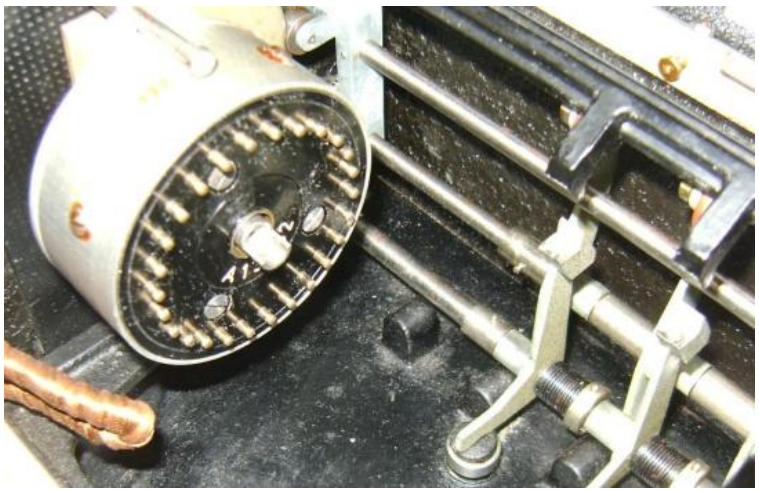
**How many possible starting positions are there for the rotors in the Enigma Machine?**

We use the same calculation as on the previous slide. There are

$$26 \times 26 \times 26 = 17,576$$

possible starting positions for the three rotors in the machine.

# Reflector



After going through the three rotors, the signal hits the “reflector." There are two reflectors in the Enigma machine which are each set up differently – most commonly used was the B reflector. They transform the letter to a different letter and send it back through the rotors in the reverse direction.

# Reverse Journey

The reverse journey works the same way as the forward journey – the signal is sent through the three rotors and permuted three times.

After this the signal is reversed through the plugboard before being sent to the **lampboard**.

# The Lampboard

The lampboard is the final stop for the electrical current – it lights up the lamp for the letter of the ciphertext.


Because of the rotating rotors, you can press the same letter over and over but the letter which lights up changes each time.

# Breaking The Enigma

Marian Rejewski

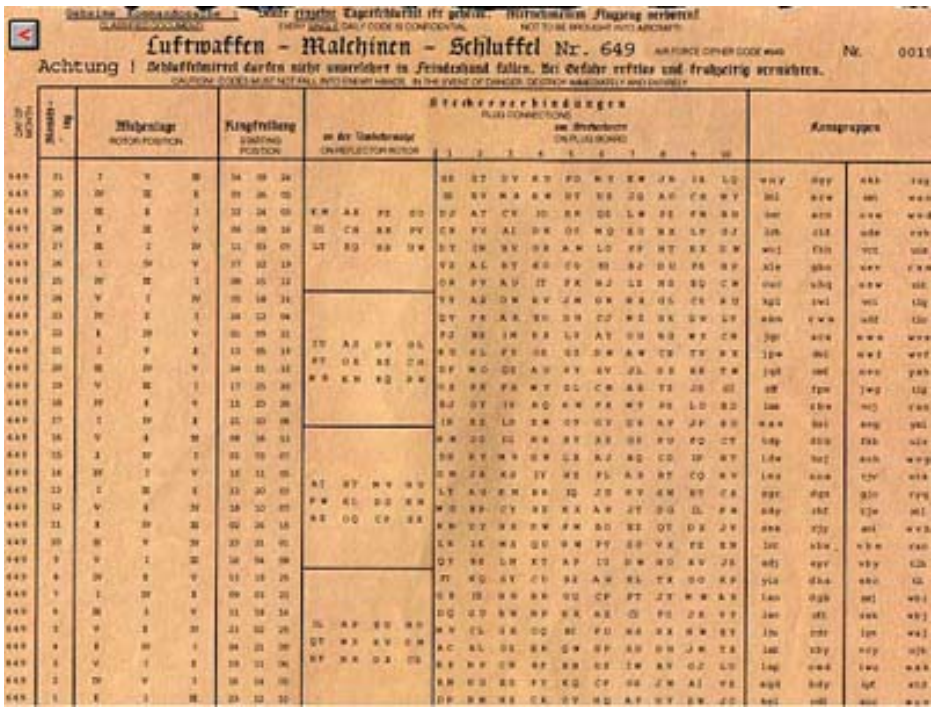
The first attempt at breaking the Enigma was led by Polish cryptanalysts Marian Rejewski, Henryk Zygalski and Jerzy Rozicki at the Polish cipher office **Biuro Szyfrow**. They created a machine called the **Bomba Machine**, which sped up the process of decrypting early Enigma Machine messages. This machine works completely differently from the Enigma.

# Bomba Machine: Exploiting A Weakness

At first the Enigma Machine's key management system was incredibly vulnerable. At the beginning of each message, the randomly chosen message key was encrypted and sent twice. The Polish cryptographers used this in order to deduce the key each day.

When the Germans realized this weakness, they stopped using this key distribution method. This increase in the sophistication of the enigma led to a necessity for a new cryptanalytic attack.

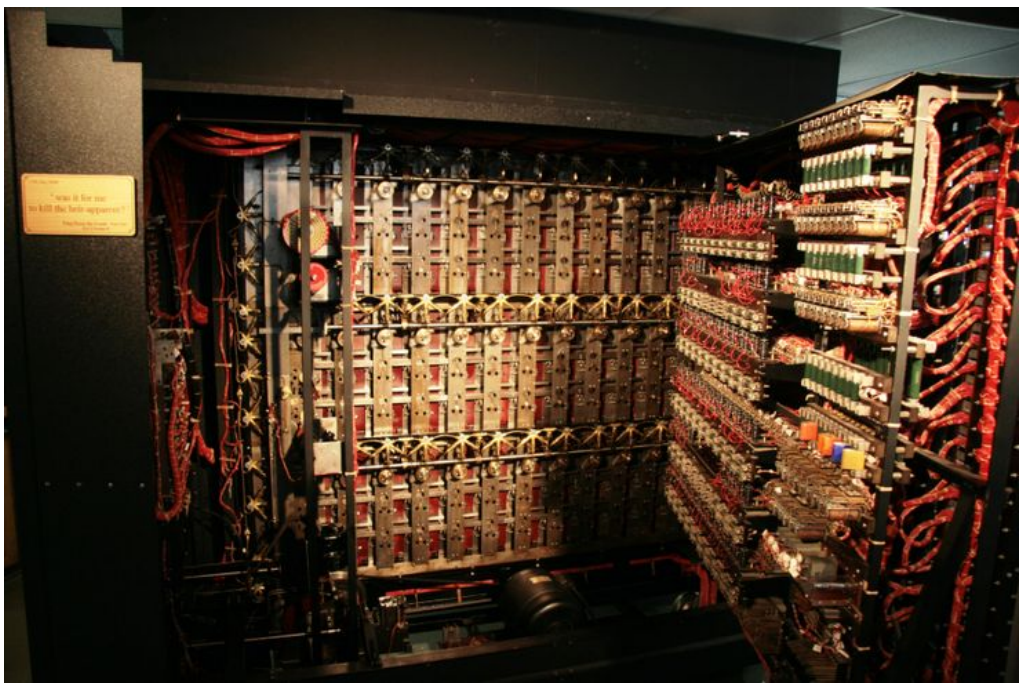
# Key Distribution: Code Books


Luftwaffen - Maschinen - Schlüssel Nr. 649

Achtung!

As this is a private key encryption system, the Germans needed a way of distributing private keys. At the beginning of each moth a **code book/keysheet** was given to the operators of the Enigma machines. This gave the key to be used each day, where the key consisted of rotor and plugboard settings.

# Bletchley Park



The Bombe Machine

The Polish shared information on the mechanics of the Enigma machine with the British in 1939. Cryptographers at **Bletchley Park** designed the **Bombe Machine**, which weighs in at around 1 ton, to crack the Enigma.

# Bombe Machine: Exploiting Another Weakness

The key observation leading to the construction of the Bombe machine was that a letter was never encrypted as itself. Furthermore certain phrases were often included in messages, such as “Wetterbericht” (Weather Report) and “Heil Hitler.” Turing and Welchman designed the Bombe machine using these words along with the aforementioned observation.

Let’s watch the following video on how the cryptanalysts exploited this weakness (start at 34 seconds):
`https://www.youtube.com/watch?v=V4V2bpZlqx8`

# Alan Turing

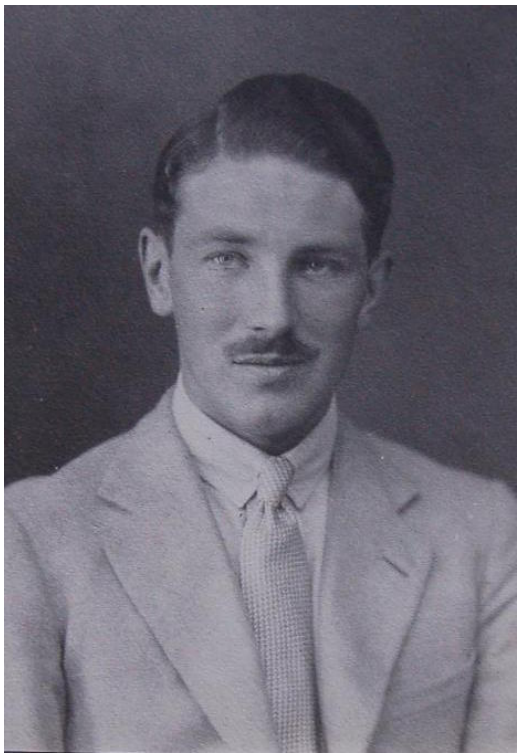

Alan Turing

Alan Turing was one of the main forces behind the design of the British Bombe machine. He was recently popularized in the film **The Imitation Game**.

He is known as “the father of computer science” and is responsible for designing the **Turing machine**, a mathematical model for computing still used today, as well as the **Turing test**, a test for artificial intelligence.

# Other Cryptographers at Bletchley

There were many other people on the team at Bletchley Park. **Gordon Welchman** designed an enhancement to Turing's machine which significantly increased its speed. **Joan Clarke** also played an instrumental role at Bletchley Park – although sexism meant she was paid less and prevented from progressing as far in her career.



# Turing's Death and Legacy

In 1952 Alan Turing was convicted of "gross indecency" after acknowledging that he was a homosexual to the cops while reporting a robbery.

Turing was stripped of his security clearance and banned from consulting with the GCHQ (British intelligence). He was given the choice between chemical castration and prison. He committed suicide in 1954.

In August 2014 the queen posthumously pardoned Alan Turing. In September 2016 this pardon was expanded posthumously to cover all other men convicted of indecency offenses for homosexuality throughout history. This law is known informally as the **Alan Turing Law**.

# References


- Counting plugboard settings: http://www.codesandciphers.co.uk/enigma/steckercount.htm
- How the machine works: http://enigma.louisedade.co.uk/howitworks.html
- History & How it works: https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game
- History: http://cs-exhibitions.uni-klu.ac.at/index.php?id=282
- History: https://plus.maths.org/content/exploring-enigma