The Enigma Machine

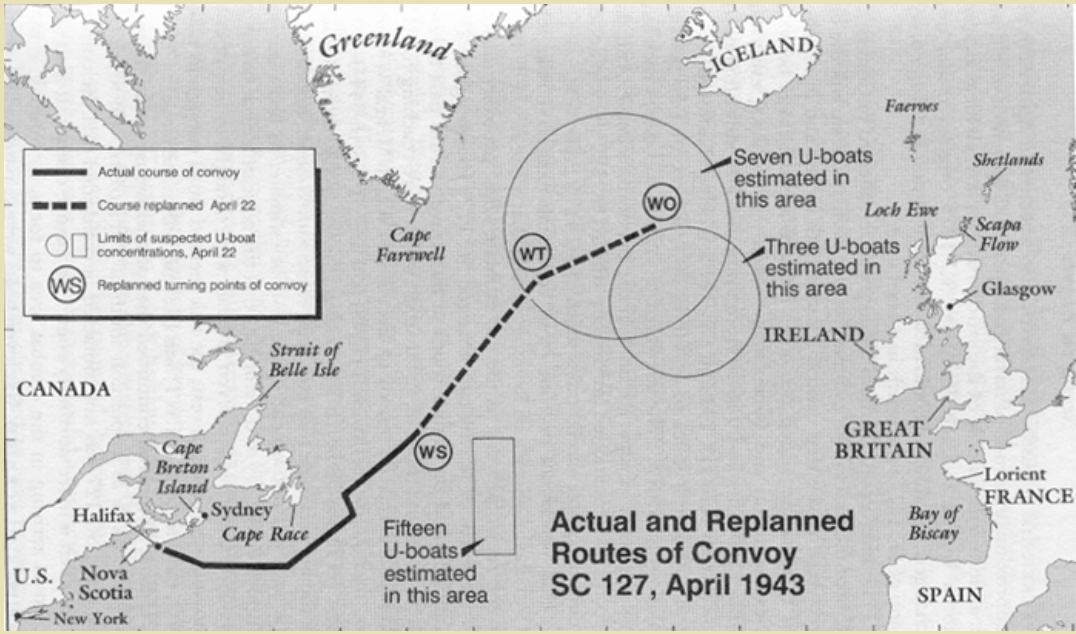
Overlake School

January 16, 2002

Mike Koss

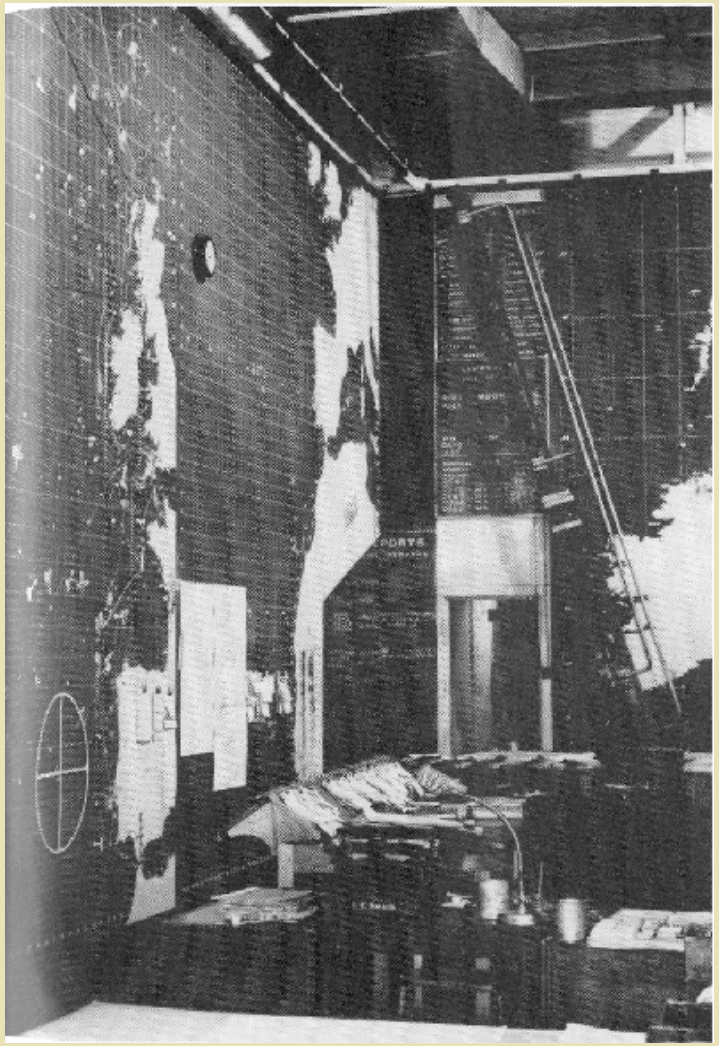
Battle of the Atlantic - World War II

- The Germans used submarines to try to stop the Americans from sending war supplies to the British.



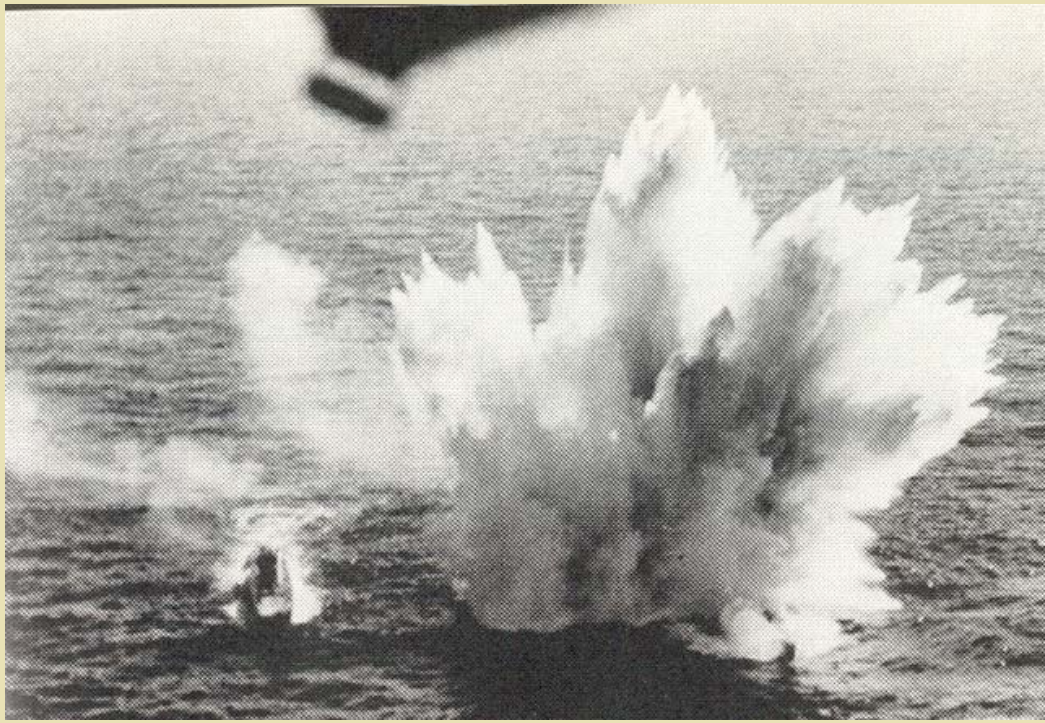
Submarine Tracking

- The British tried to keep careful track of submarine locations to keep shipping convoys out of harms way.



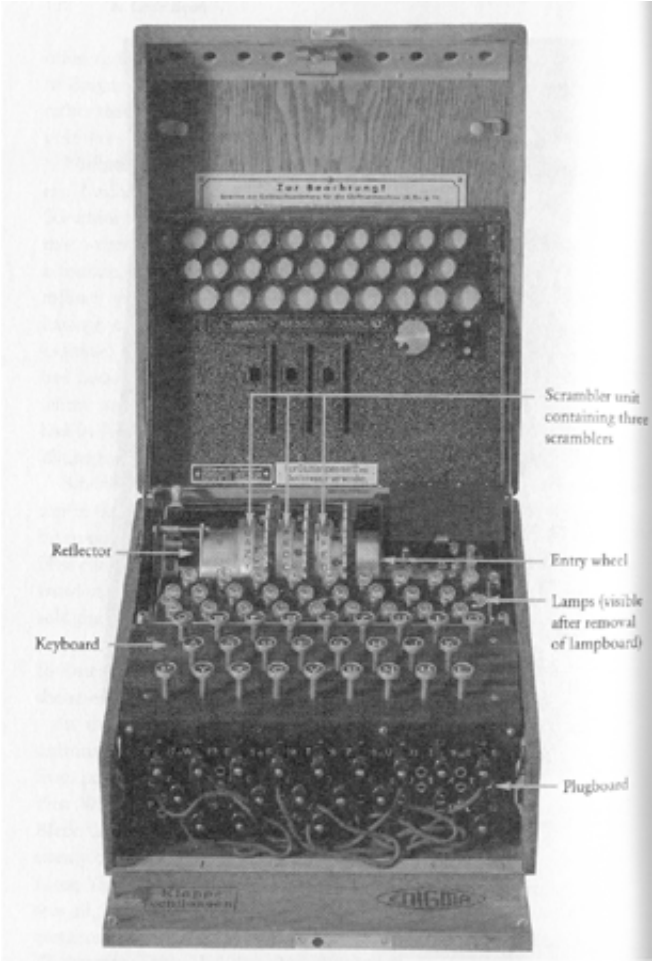
Communication Secrecy

- The Germans needed a way to secretly communicate with their submarines.



The Enigma Machine

- The Germans adapted a machine for encoding all military communications which they believed to be unbreakable…but…

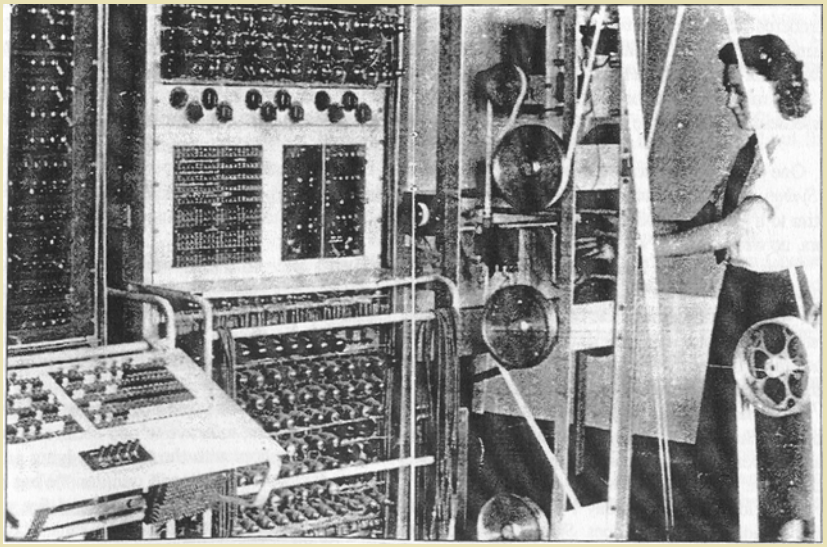


Code Breakers of Bletchley Park

- The British assembled a team of mathematicians, crossword puzzle geniuses, and clerks to break the German codes.

First Computers Invented

- Along the way, they invented the world's first digital stored program computer to help them crack the hardest German codes.



Colossus

Demo: Sending an Enigma Message

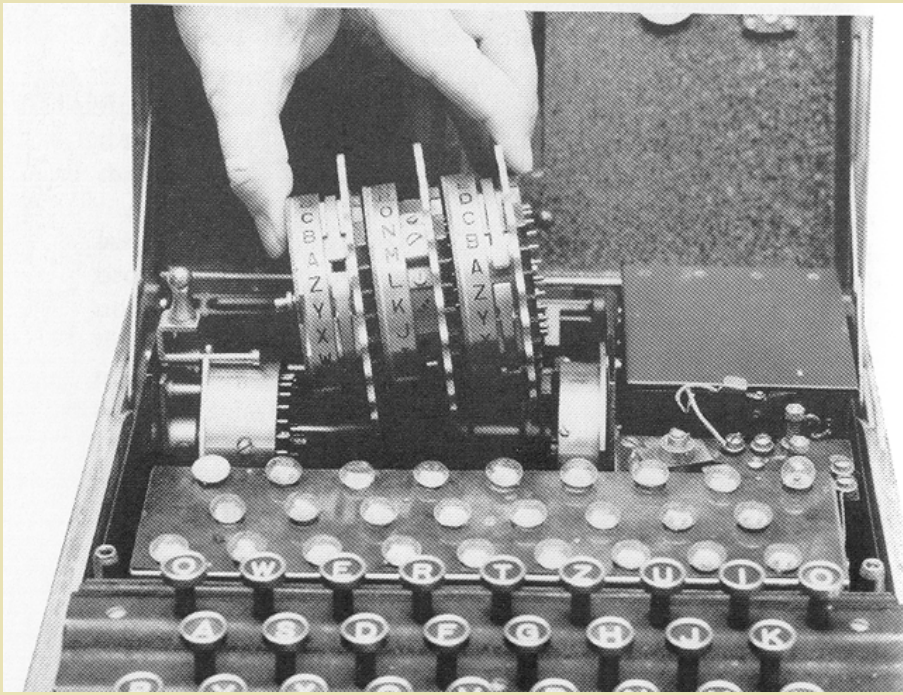
- Set up today's rotor settings from the published (secret) code book.
- Chose a three-letter message key.
- Encode the message key (twice: e.g., XYZ-XYZ).
- Set rotors to message key setting.
- Encode the message.

Demo: Receiving an Enigma Message

- Set up today's rotor settings from the published (secret) code book.
- Decode the first 6 letters of the message to get the message key.
- Set the rotors to the message key setting.
- Decode the contents of the message.

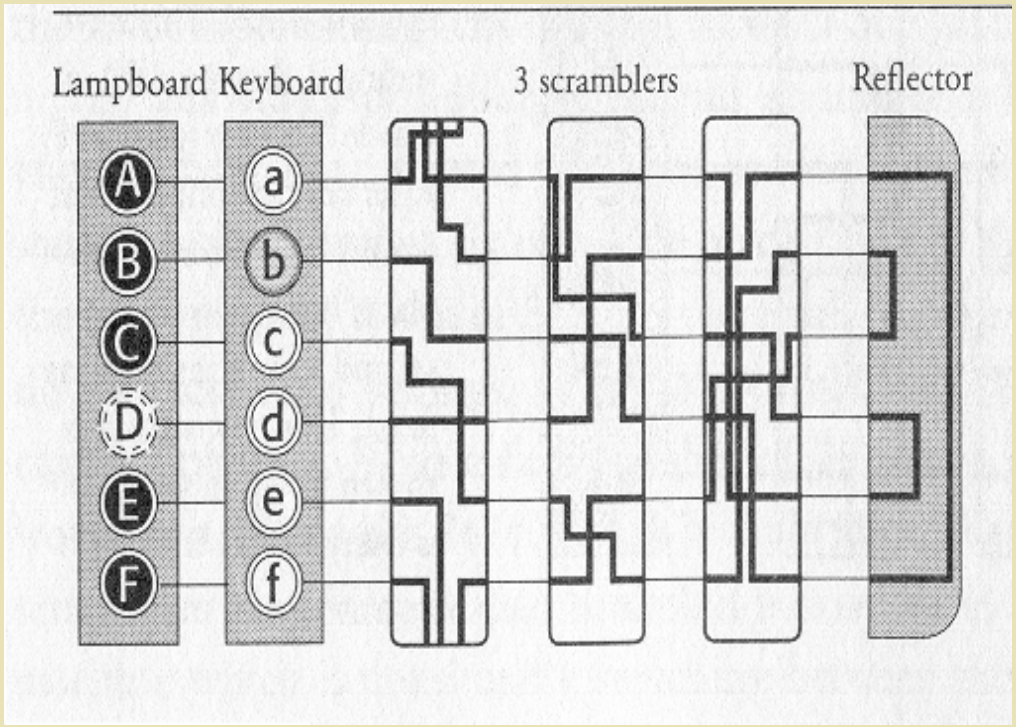
How Enigma Works

- Enigma uses a system of 3 or 4 “rotors” that electrically connect a keyboard to a “lamp-board”.



Scrambling Letters

- Each letter on the keyboard is connected to a lamp letter that depends on the wiring and position of the rotors in the machine.



Other Machines

- M-94: United States – Thomas Jefferson patented, used in civil war through WW II.
- M-209: United States – used by WW II paratroopers.
- NEMA: Swiss “New Machine” – a better Enigma.