A Glimpse of the History of Cryptography

Cunsheng Ding
Department of Computer Science
HKUST, Hong Kong, CHINA

Part II: Machine Ciphers

Enigma

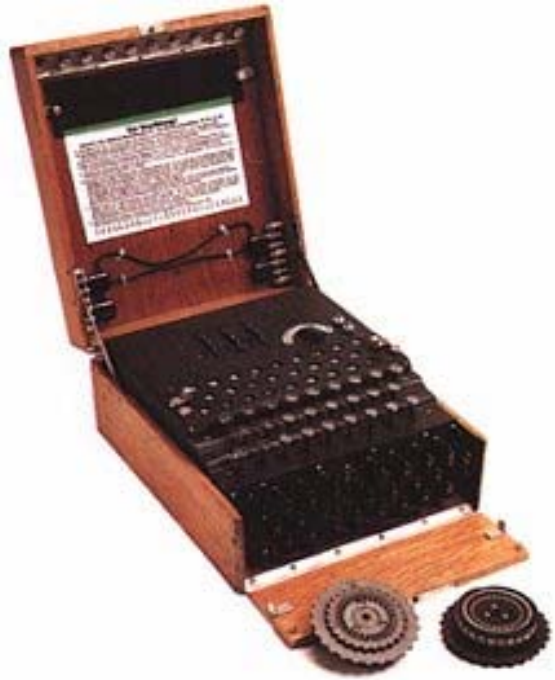
- Before war broke out in 1939 the Germans had planned a special way of keeping their communications secret. The army, navy and air force were told to encode their messages using cipher machines called ENIGMA.

Enigma

- Enigma could put a message into code in over 150 MILLION MILLION MILLION different ways.
- The Germans believed that no one could crack the Enigma code. But the Allies knew that if they could, they would be able to find out their enemy's military secrets.

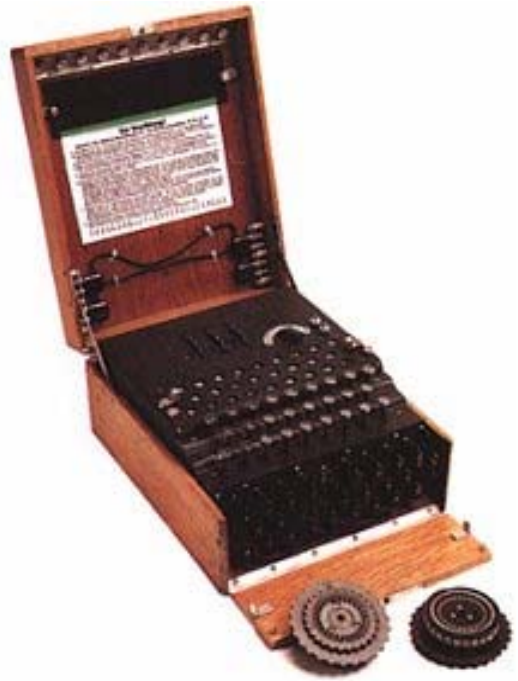
Enigma

- The Enigma machine looked like a typewriter in a wooden box. An electric current went from the keyboard through a set of rotors and a plugboard to light up the 'code' alphabet.



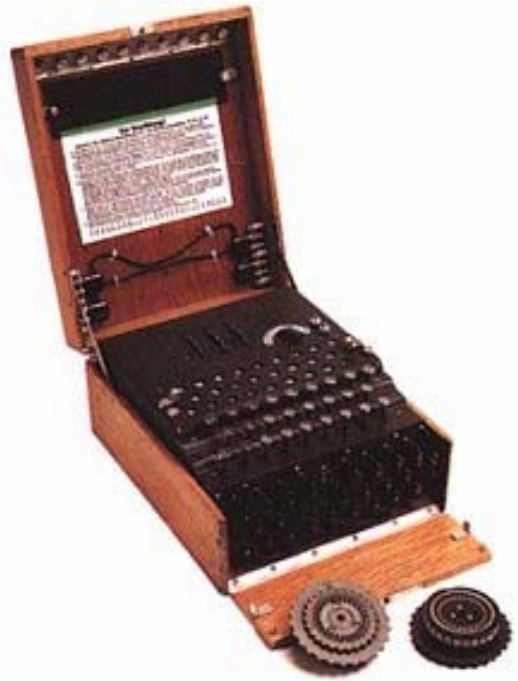
Enigma

- At least once a day the Germans changed the order of the rotors, their starting positions and the plugboard connections. To decipher a message sent using Enigma, you had to work out exactly how all of these had been set.



Enigma

- In the 1930's Polish cipher experts secretly began to try to crack the code. Just before war broke out they managed to pass models and drawings of Enigma to British and French code-breakers.
- Later Enigma was broken.

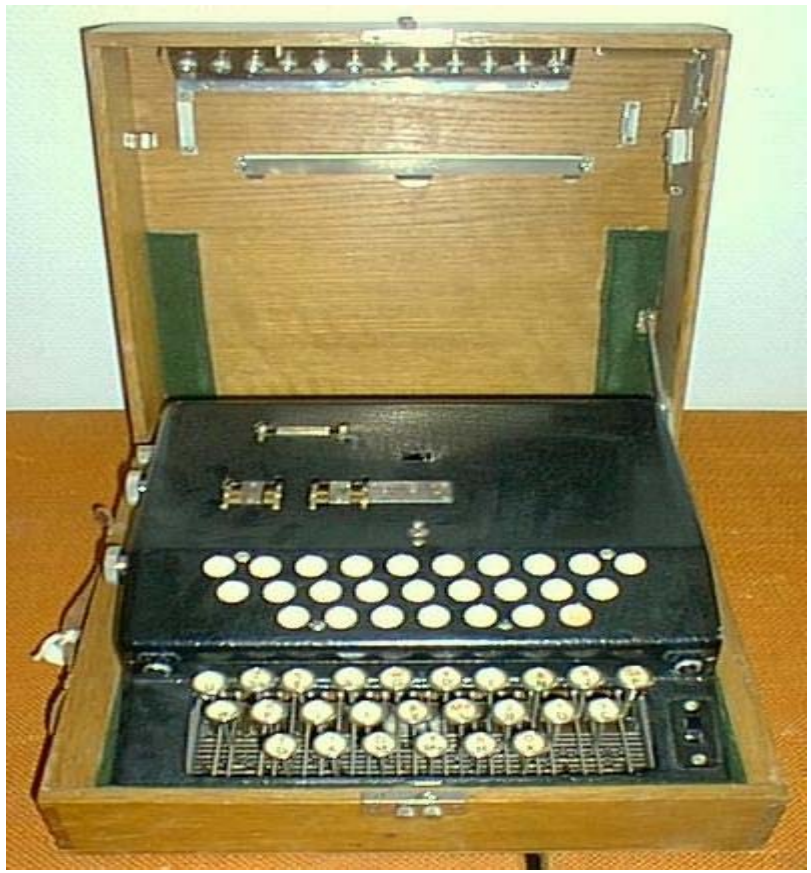


Sigaba

- It was suited for fixed station secure communications, and used by U.S. for high-level communications, was the only machine system used by any participant to remain completely unbroken by an enemy during World War II.

B-21 Machine by Boris Hagelin

- Patterned on the Enigma and produced for the Swedish General staff, Boris Hagelin of Sweden developed the B-21 machine in 1925. It also had the capability to be connected to an electric typewriter.

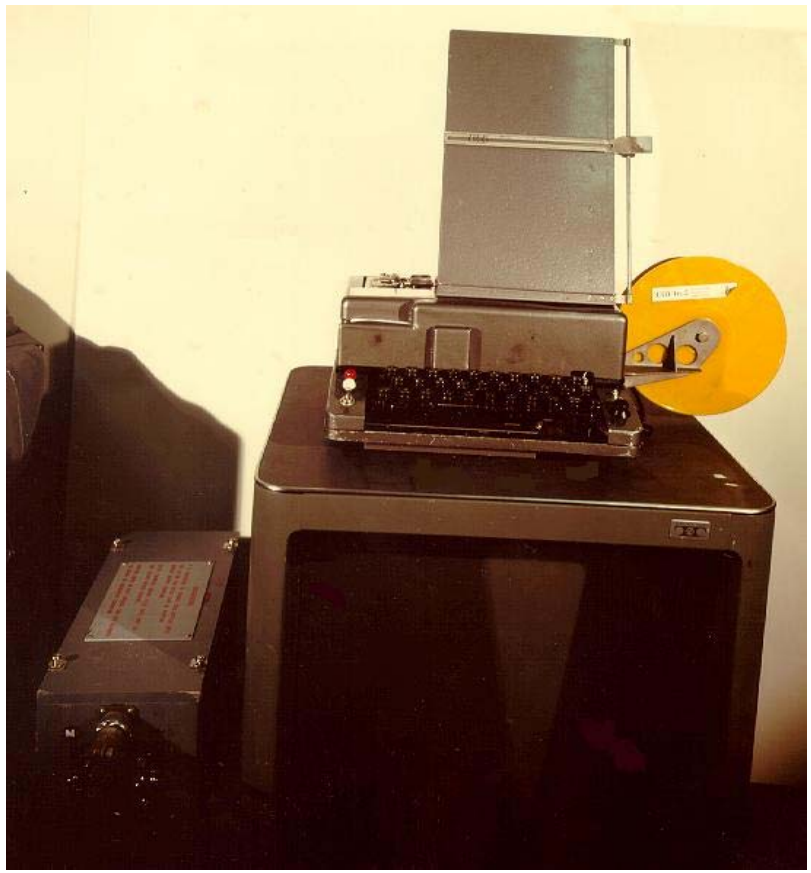


BC-38 by Crypto AG Zug

- Boris Hagelin of Sweden developed a long line of cipher systems, beginning with the B-21, B-211, C-35, C-36, C-38 (which later became America's M-209).

BID 590 (Noreen)

- The BID 590 was a British built crypto machine and was used by Canada's foreign service communicators at various diplomatic missions to communicate with various government departments.



H-4605 (Crypto AG)

- The Crypto AG H4605 was designed as an off-line, keyboard operated cipher machine with twin printing (of cipher and plain text) system with automatic 5-letter grouping. It's a solid piece of equipment, almost 'battleship grade'.

Japanese "Enigma" Rotor Cipher Machine

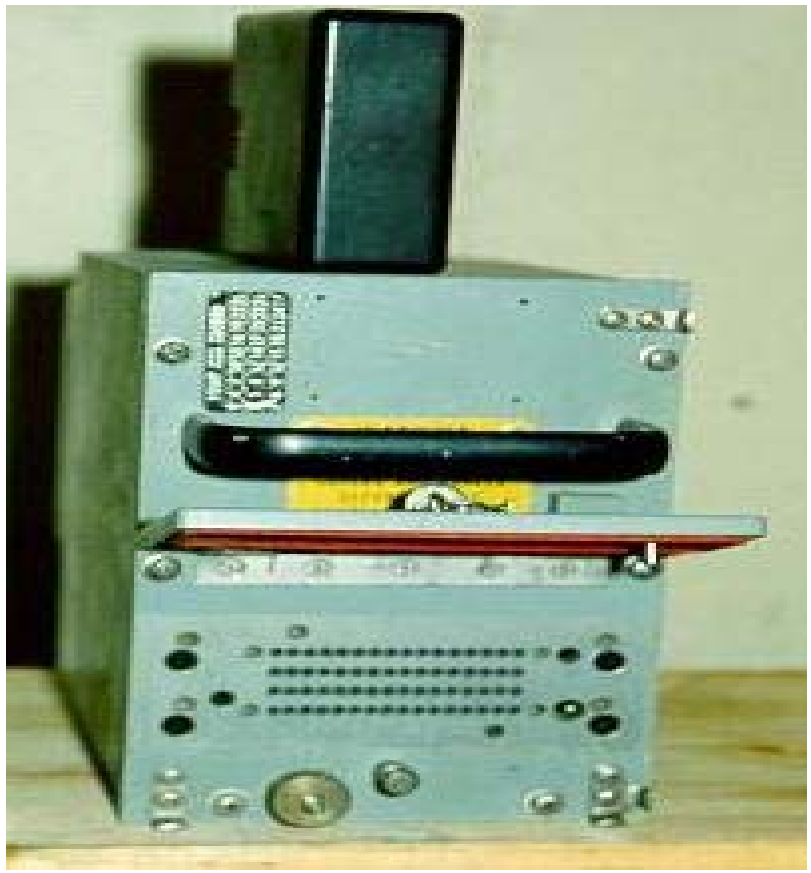
Produced by Germans for Japanese

Japanese Purple machine

- Electromechanical stepping switch machine modelled after Enigma
- Used telephone stepping switches instead of rotors
- Purple was broken with the help of MAGIC.
- Pearl Harbor attack preparations encoded in Purple, decoded hours before attack.

KY-28 (Nestor)

- The KY-28 was an analog, voice encryption device based on transistor circuitry and was the shipboard/airborne member of the NESTOR family of equipment.



Racal-Milgo 64-1027C Datacryptor

- The Racal-Milgo 64-1027C Datacryptor was used to send and receive secure data via computer. This is the commercial version of the KG-84, and has ability to be loaded via the KYK-13 Fill device.

The "Clock Cryptograph"

- It is basically a nicely implemented Wheatstone cipher disk. It was in active use in the Danish armed forces from 1934 (or a little earlier) until around 1948.

People in Breaking Codes

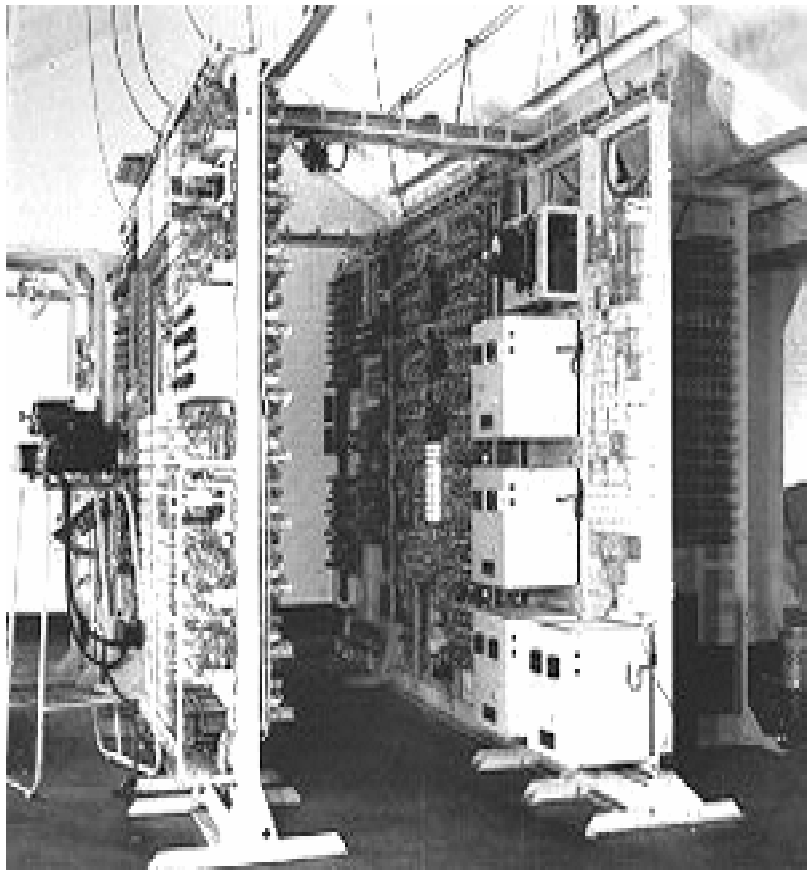
- Bletchley Park was the home of the secret Government Code and Cypher School. This was the centre of British code-breaking during the war.

People in Breaking Codes

- The code-breakers in Bletchley Park were specially chosen from among the cleverest people in England. Some were brilliant mathematicians or linguists.
- Alan Turing, a Cambridge mathematician and code-breaker who helped to invent one of the world's first computers at Bletchley Park.

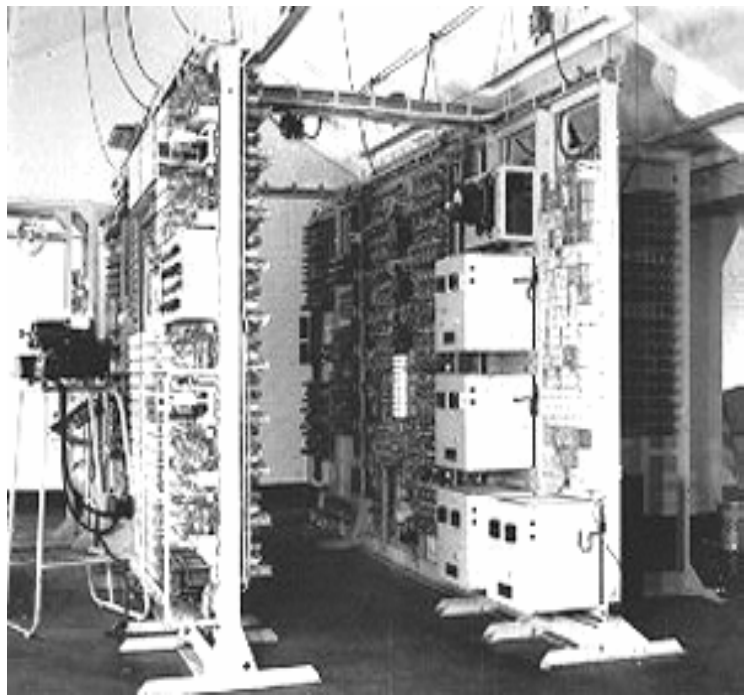
Computer and Code Breaking

- Colossus was built for the code-breakers at Bletchley Park by post office engineers in 1943.
- One of the earliest computers.



Computer and Code Breaking

- The computer was as big as a room - 5 metres long, 3 metres deep and 2.5 metres high - and was made mainly from parts used for post office telephone and telegraph systems.



Computer and Code Breaking

- This Cray XMP was donated to the museum by Cray Research, Inc. It denotes the newest era of partnership between NSA and the American computer industry in the employment of computers for cryptologic processes.

Cipher Machines and Software Somulation

- http://frode.home.cern.ch/frode/crypto/