The Electronic Revolution: Part 2

An overview of the computers and computing devices that relied solely on electronic means for completing calculations.

James Tam

World War II: Code Breaking And Computing

The Allies

- British code breaking machines/projects
  - The machines of Bletchley Park ('bombs')
  - The Robinsons
  - The Colossus (and the Colossi!)

The Axis

The enigma machines (but commercial versions were purchased by other nations e.g. Poland->England)

Later: Geheimschreiber (secret writer)

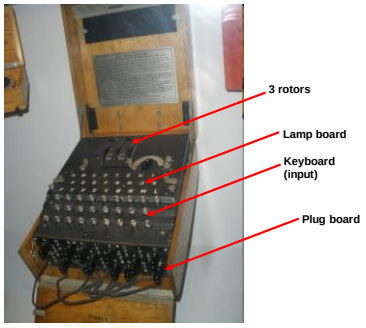
James Tam

The Enigma

- Developed by Germany between the two world wars (WWI: 1914 – 1918, WWII: 1939 – 1945).
- It was designed to convert ordinary language ("plain text") into an encoded ("encrypted form") to be sent via radio or telephone lines.
- There were two version: one for the military and one for business.
  - The commercial machines were made publically available in 1927.
  - The German military began to use the Enigma code on one of their radio stations in 1928.

James Tam

The Enigma: Basic Encryption

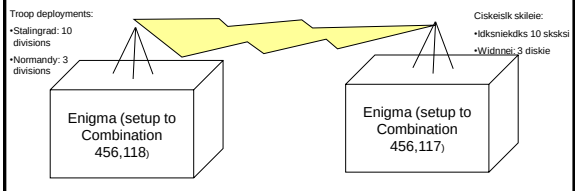


An enigma machine (Imperial War Museum: England) courtesy of James Tam

James Tam

The Enigma: Combinations

- The sheer number of possible combinations (100 billion!) made mere possession of the machines useless.



James Tam

The Allies (British): Decrypting The Enigma Encryption

- Simply possessing one of the Enigma machines wasn't sufficient.
- Nor was it sufficient to know the code settings used for a particular time.
- Poland:
  - When the German military began to broadcast radio transmission (1928) using the Enigma encoded messages. The Polish radio operators alerted the Cipher Bureau.
  - Polish Cipher Bureau: purchased and modified a commercial copy of the Enigma.
  - 1928 – 1931: little headway was made and the project was abandoned in 1931.

James Tam

The Allies (British): Decrypting The Enigma Encryption: 2

- 1932: Martin Rejewski: a mathematician was assigned to study the encryption problem again.

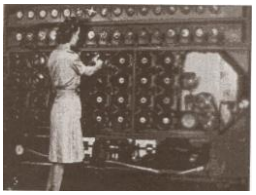
http://ulm.ccc.de

- His initial efforts resulted in some success and additional people were added to the project.
  - ~75% of the German messages were deciphered.
  - "Encryption: technology race" between the Polish and German technological developments.

James Tam

The Allies (British): Decrypting The Enigma Encryption: 3

- 1939: it was evident that war was imminent: the policy of 'appeasement' was not working.
  - The Poles called a meeting of the intelligence agencies of: Poland, France and England.



Polish built bomba("bomb") from "A History of Computing Technology" (Williams)

James Tam

The British Code And Cipher School

- Worked on deciphering the German codes at Bletchley Park outside of London:

- Intelligence work involved a great deal of secrecy:
  - Information was strictly on a "need to know basis" for the people working there.
  - Even now much of the information is still classified "Official Secrets Act": http://www.legislation.gov.uk/ukpga/1989/6/contents

James Tam

The British Code And Cipher School (2)

- The combination of secrecy surrounding the work at Bletchley Park and the code names used, 'work on bombs' resulted in a great deal of confusion.
  - "…but the only thing these bombs destroyed was the German Air Force message security" (Williams).
- What is known:
  - The British constructed several new versions of their own 'bombs' which were based on the Polish original.

James Tam

Alan Turing (1912 – 1954)

- A distinguished British Mathematician from Cambridge
  - He produced distinguished first-rate work (Williams)
- After graduation he remained to work at the college and produced a famous paper:
  - "On Computable Numbers with an Application to the Entscheidungs-problem"
  - His work was known to scholars throughout the world.
  - 1936 he spent the year at Princeton: (Einstein, von Neumann).
- During the war he worked at Bletchley Park as a code-breaker (contributed to the design of the machinery as well as applying his Mathematical knowledge)
  - An eccentric person
  - A 'pure' scholar

James Tam

Image from "History of Computing Technology" (Williams)

Alan Turing (1912 – 1954): 2

- Later events:
  - After his death he was granted a pardon by the British government near the end of 2014 (he was convicted in 1952 and died by poisoning in 1954).
    - https://www.bbc.com/news/technology-25495315 (last accessed 2024).
  - Creation of an extremely prestigious award "ACM A. M. Turing Award"
    - "…sometimes referred to as the "Nobel Prize of Computing"
    - https://amturing.acm.org/ (last accessed 2024).
- For more information: "Allan Turing: The Enigma" by Hodges A. (Simon and Schuster)

James Tam

The Robinsons

- 1942 (mid year): staffing levels at Bletchley Park were such that different sections (groups) were formed.
  - Each section was housed in a 'hut'.

www.bbc.co.uk

James Tam

The Robinsons (2)

- Division of work into huts:
  - Groups would work on different problems in different huts.
  - Alternatively different groups would work on the same problem in different huts but using different approaches.
  - Only the hut supervisors would communicate. (Top Secret: need to know)
- By this time the bombs were too slow to be used in the decryption process and new techniques needed to be developed.
- General Post Office (Telephone Division)
  - Dollis Hill: West London
  - Mr. T.H. Flowers: head of a group working on telephone switching problems.

James Tam

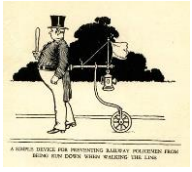
The Robinsons (3)

  - Commissioned: several pieces of machine to be built for the people at Bletchley Park.
  - What the Dollis Hill people thought: designing a new photoelectric paper tape reader to be used in a new telegraph.
- M.H.A. Newman:
  - Envisioned a new machine that could automate a part of the decryption process.
  - Dr. C.E. Wynn-Williams: known for his previous work designed the machine envisioned by Newman

James Tam

The Robinsons (3)

- Machine name: Heath Robinson (unusual device named for an unusual cartoonist).



Copyright unknown

Heath Robinson computer: http://www.rutherfordjournal.org

James Tam

The Robinsons (4)

- Known specifications:
  - Much of the information is still 'classified' but some details have been released.
  - Partly implemented using vacuum tubes and telephone relays.
  - Not a general purpose computer.
  - Evaluate some Boolean operations on information read from two endless loops (punched paper).

James Tam

The Robinsons (5)

- Quickly constructed
  - Unreliable
  - 'Proof of concept': high speed electronic devices could still aid in the decoding process.
  - At least three machines constructed: Heath Robinson, Peter Robinson, Robinson and Cleaver.

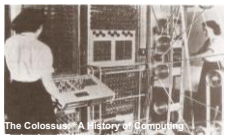
Peter Robinson
http://www.english-heritage.org.uk

Robinson and Cleaver
www.skyscrapercity.com

James Tam

The Colossus, Williams

- Mr. T.H. Flowers (London Post Office: tape reader project)
  - Brought directly into the project as an electronics expert to help redesign the Robinson machinery to make it more reliable (vacuum tubes over relays).
  - A completely new all electronic design (1,500 vacuum tubes) was used.
  - The improved reliability along with the use of electronics over mechanical parts resulted in a significant speed increase ~100:1



  - First used in operation December 1943.

The Colossus (2)

- The first job given to the machine was completed in 10 minutes ("the savior machine" hailed as "The Colossus").
- Some of the known specifications (many still 'classified'):
  - Bi-quinary storage of information in the registers.
  - An internal clock was used to synchronize operations.
  - Controlled by a plug board and wires.
  - Card readers (Robinsons) were used as input.
- Due to foresight and very good planning the second Colossus machine was built in less than a year!
  - Recall first Colossus completed Dec 1943
  - March 1944: Many more! < June 1944

The Colossus (3)

- It's believed that up to ten were fully functional at the end of the Second World War.
- The eventual fate of most the machines is still unknown.
  - One machine was moved to Iran (Russia: Cold War)
- Similar to the Robinsons: the Colossi were required to complete high speed Boolean operations on data read from tape.
- In some ways the forerunner of the modern computer:
  - Because the basic mathematical operations can implemented using Boolean logic, in theory the machines could be general purpose (proof: base 10 multiplication performed),
  - Conditional branching possible: different plug board instructions could be executed depending upon a value stored in one of the registers (still 'classified' so details are sketchy).

Video: British Code Breaking Machine

- Colossus and other code breaking devices developed at Bletchley (last accessed October 2024)
  - https://www.youtube.com/watch?v=_ZJXb_eSvwI

American 'Bombs'

- Few details are available.
- One of the last remaining American 'bomb' code breakers resides at the National Museum of American History (Smithsonian Institution).
  - Copy (identical?) of British machines.
- Other hints at American code-breaking efforts
  - Alan Turing visiting the U.S. during the war (Bell Labs)
  - "…the people who should be knowledgeable in such matters [code breaking efforts] (even if they won't admit it) acknowledge that the Colossi were far in advance of anything available in the States at the time." (Williams)

Option External Video: Overall Summary

- Captures the essence of many machines discussed so far and some others that will be covered in a later section (last accessed 2024).
  - https://www.youtube.com/watch?v=qundvme1Tik

After This Section You Should Now Know: All Sections

- What is the difference between electronic and mechanical/electro mechanical computing devices
- What were the three main categories of electronic computers
- What was the first electronic computer (partially and fully completed)
- The technical specifications of the first electronic computers
- The general appearance and cost/resources used in the building of the first electronic computers
- The history behind the names of the first electronic computers
- Who were the people behind these computers and what were some of the major events in their lives
- What were the approximate dates/time frames of significant developments in the mechanical monsters

James Tam

After This Section You Should Now Know: British

- The Enigma: who developed it, what was it used for, how did it work
- The British code breaking machines
  - What were the 3 categories or families of code breakers
  - The events leading up to the development of the machines at Bletchley Park
  - The events leading up to the development of the Robinson machines and the technical specifications of these machines
  - The events leading up to the development of the Colossus and the second Colossi
  - The technical specification of the Colossi
  - What were the American code breaking efforts during the second world war

James Tam

References

- "A history of computing technology", Michael R. Williams 2nd Ed (IEEE 1997)
- "Allan Turing: The Enigma" by Hodges A. (Simon and Schuster)
- https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/crypto-almanac-50th/The_Breaking_of_Geheimschreiber.pdf

James Tam

Copyright Notice

James Tam