

# SYMMETRISCHE VERSCHLÜSSELUNGSVERFAHREN II - ALAN TURING UND DIE ENTSCHLÜSSELUNG DER ENIGMA



Maxi Sieber  
Christian-Weise-Gymnasium Zittau

# Gliederung

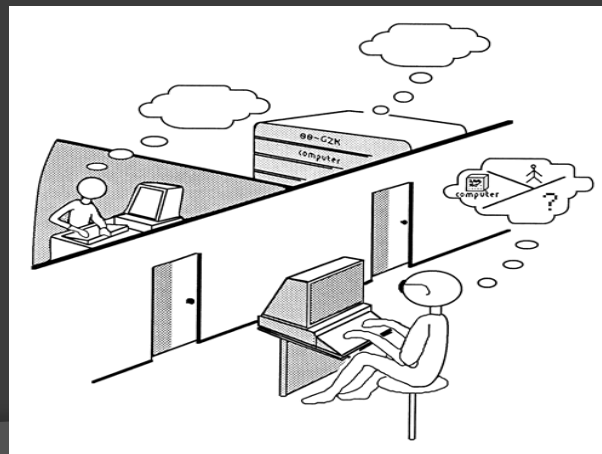
- Turings Leben
- Wissenschaftliche Leistungen
- Aufbau und Funktionsweise der Enigma
- Turings Leistung bei der Entschlüsselung der Enigma

# Turings Leben

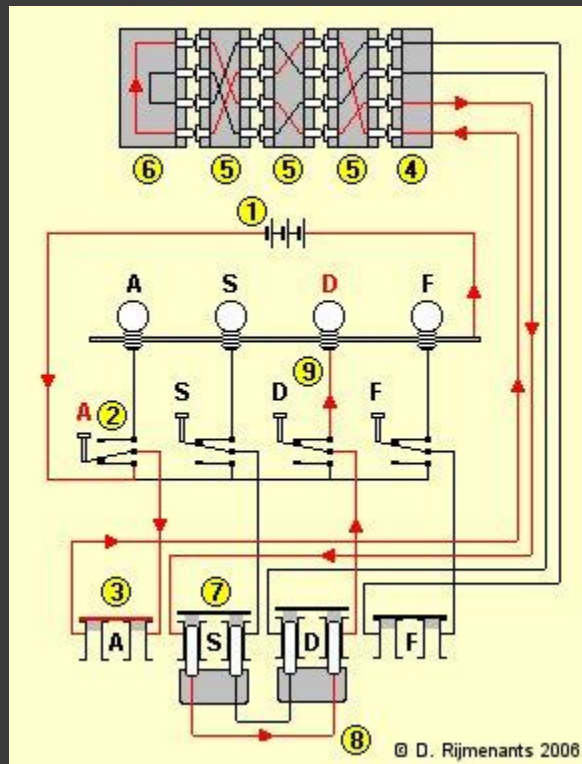
- \* 23. Juni 1912 in London
- wuchs bei Freunden der Familie und Kindermädchen auf
- Besuch der Sherborne School, sein starkes Interesse an Naturwissenschaften wurde deutlich
- 1931-1934 Mathematikstudium am King's College in Cambridge
- ab 1939 Mitwirken beim britischen Geheimdienst in Bletchley Park; Entschlüsselung der Enigma; Entwürfe eines Computers am Londoner National Physical Laboratory
- 1948 Dozent in Manchester; beschäftigte sich mit künstlicher Intelligenz
- 1952 Homosexualität (damals strafbar) wurde bekannt; Hormontherapie als Strafe und verlor die Anstellung beim brit. Geheimdienst
- beging Selbstmord am 07. Juni 1954 aufgrund von Depressionen

# Wissenschaftliche Leistungen

- 1936 Aufsatz „On Computable Numbers“ -> theoretische Grundlagen für die Entwicklung von Rechenmaschinen
- 1936 Turing-Maschine -> Ausführung mathematischer Operationen, Grundlage für moderne Computer
- Dechiffrierung der deutschen Verschlüsselungsmaschine „Enigma“ im 2. Weltkrieg
- 1948 Turing-Test -> Wenn ein Mensch nicht unterscheiden kann, ob er mit Mensch oder Maschine kommuniziert, ist die künstliche Intelligenz von Maschinen entstanden



# Aufbau und Funktionsweise der Enigma



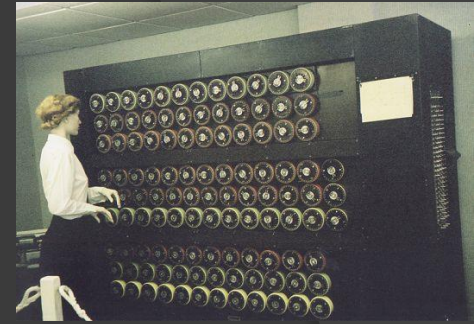
- Maschine zur Verschlüsselung von militärischen + zivilen Nachrichten
- 1918 von Arthur Scherbius entwickelt
- ab 1925 von Dt. Wehrmacht und Regierungsstellen verwendet
- Batterie (1), Tastatur (2), Steckerbrett (3,7,8), Walzensatz (4,5,6), Lampenfeld (9)
- Buchstabe wird eingegeben, Strom gelangt über Steckerbrett zur Eintrittswalze, durchläuft Walzensatz und wird wieder reflektiert, Lampe mit verschlüsseltem Buchstaben leuchtet auf
- Walzen drehen sich ähnlich wie ein Kilometerzähler

# Enigma Simulator

- ◎ <http://www.ostfalia.de/cms/de/pws/seutter/kryptologie/enigma/Simulation/Simulator/simulation.html>



# Turings Leistung bei der Entschlüsselung der Enigma



- unbekannt für die Briten:
  - Welche drei der fünf Walzen wurden ausgewählt?
  - Welche Verkabelung lag vor?
- Turing entwickelte die Turing-Bombe (Grundlage war die polnische Bomba)
  - mehrere, hintereinander geschaltete Enigmas
  - Alle möglichen Schlüssel wurden getestet, basierte auf Wörtern, die mit größter Wahrscheinlichkeit im Text vorkommen würden („cribs“)
- Ausschluss vieler Möglichkeiten, da ein Buchstabe nie mit sich selbst verschlüsselt sein konnte
- Turings Erfolge verkürzten den Krieg laut Historikern um bis zu zwei Jahre

# Quellenangabe

- <http://sgwiki.com/images/5/56/Image00011.jpg>
- <http://malte-goebel.suite101.de/der-biss-in-den-zyankali-apfel-a71262>
- <http://www.nzzfolio.ch/www/d80bd71b-b264-4db4-afd0-277884b93470/showarticle/d8fadef7-3ec3-4d72-9c97-36d970eef77c.aspx>
- <http://www.natur-struktur.ch/ai/images/turingtest.gif>
- [http://www.it.fht-esslingen.de/~schmidt/vorlesungen/kryptologie/seminar/historie/Me\\_Tu.html](http://www.it.fht-esslingen.de/~schmidt/vorlesungen/kryptologie/seminar/historie/Me_Tu.html)
- <http://de.wikipedia.org/w/index.php?title=Datei:TuringBombeBletchleyPark.jpg&filetimestamp=20080414054358>
- <http://enigma.hs-weingarten.de/gallery/enigma-original/enigma.jpg>
- <http://www.mlb.co.jp/linux/science/genigma/enigma-referat/node6.html>
- <http://www.ostfalia.de/cms/de/pws/seutter/kryptologie/enigma/Geschichte/Geschichte/geschichte4.html>
- <http://www.chessbase.de/nachrichten.asp?newsid=3245>