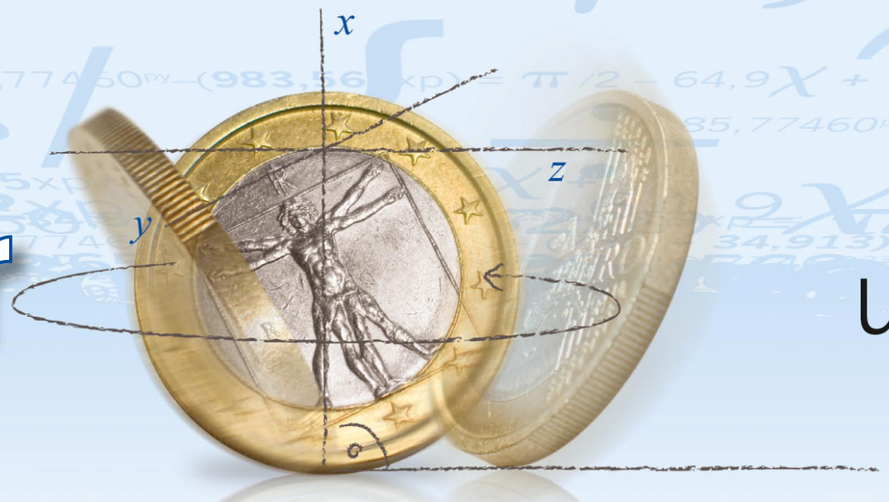
Kopf oder Zahl



universitätbonn

Bonn-Aachen International Center for Information Technology

computer Cosec security

Die ENIGMA (griech. Rätsel) ist eine Rotorschlüsselmaschine. Solche elektromechanischen Geräte verwenden mehrere Walzen, auch Rotoren genannt. Diese sind drehbar angeordnet und ihre Position ändert sich während des Schlüsselvorgangs, ähnlich einem Kilometerzähler. Außen haben die Walzen auf jeder Seite für jeden Buchstaben einen Kontakt. Diese sind im Inneren durch isolierte Drähte miteinander verbunden. Drehen sich die Walzen, so erhält man für jeden Buchstaben nach jedem Schritt eine unterschiedliche Ersetzung (Permutation).

1914

1918: *Arthur Scherbius,* Patentanmeldung der Enigma.

1923

1923: Kommerzielle Nutzung, Präsentation auf Messen.

1926: Patentierung der Umkehrwalze.

Beginnendes militärisches Interesse.

1928

1928: Polen bemerkt, dass Deutschland zur maschinellen Verschlüsselung übergegangen ist.

1930

1930: Nutzung der 3-Walzen-Enigma durch die Wehrmacht.

1932

1932: Die Entzifferung der Enigma beginnt.

1932: *Hans-Thilo Schmidt*, ein für Frankreich spionierender Deutscher, verrät hochgeheime Informationen über die Enigma an den französischen Geheimdienst. Dieser leitet die Unterlagen an britische und polnische Kollegen weiter.

1932: *Marian Rejewski,* polnischer Mathematiker, erschließt die Verdrahtung der von der deutschen Wehrmacht veränderten Walzen. Dazu verwendet er die Informationen von *Hans-Thilo Schmidt* und eine legal gekaufte kommerzielle Enigma.

1938: Die polnische Bomba bricht die Enigmaverschlüsselung unter Ausnutzung eines Verfahrens-fehlers der Deutschen.

1938

September 1938: Eine Änderung der Verfahrenstechnik behebt die kryptographische Schwäche, welche die Polen ausgenutzt haben. Damit ist die Enigma *zunächst* wieder sicher.

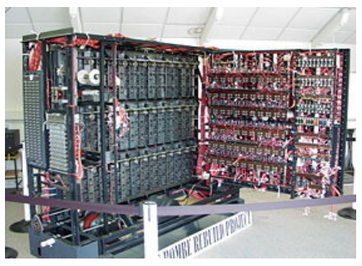
1939

Januar 1939: Einführung zweier neuer Walzen.

1939: Zwei Wochen vor dem deutschen Überfall übergeben die Polen im Wald bei Warschau ihre gesamten Kenntnisse an französische und britische Kryptographen.

1939-1945: Unter dem Decknamen „*Ultra*“ entschlüsseln die Briten in *Bletchley Park* täglich etwa 2500 Nachrichten der Luftwaffe und des Heeres.

1939-1941: *Alan Turing* und *Gordon Welchman*, britische Mathematiker, entwickeln auf Grundlage von *Rejewskis* Bomba die sogenannte Turing-Bombe.



1940

1941

Mai 1941: Mit *U110* wird eine M3-Enigma samt der dazugehörigen Code-Bücher erbeutet. Damit kann erstmals auch die Marine-Variante der Enigma geknackt werden.

1942

Februar 1942: „*Schüsselnetz Triton*“ (bei den Briten „*Shark*“): Die neue Marine Enigma M4 verwendet vier Walzen gleichzeitig.

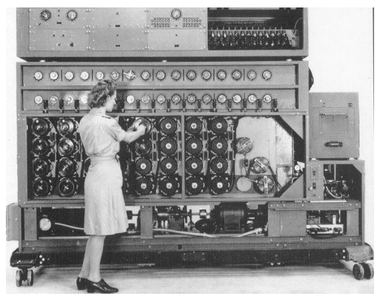
1943

Juni 1943: Immer mehr deutsche U-Boote werden durch die Alliierten versenkt.

Dezember 1942: In *Bletchley Park* kann „*Shark*“ mit Hilfe geborgener Schlüsselunterlagen aus *U559* kurzzeitig gelesen werden.

April 1943: Der Amerikaner *Joseph Desch* leitet in Dayton, Ohio, den Bau von 120 Turing-Bomben, die speziell gegen die M4-Enigma gerichtet sind.

Juni 1943: Ab jetzt kann der Funkverkehr der U-Boote wieder gelesen werden. Alliierte Konvois können deutschen U-Boot-Verbände ausweichen.



1945

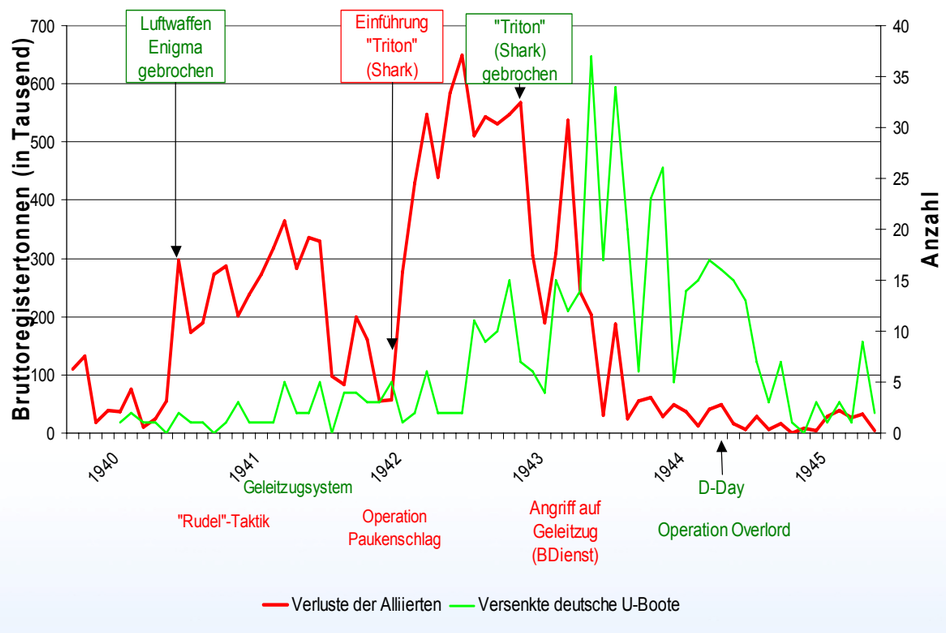
1950

1945-1950: Die Briten zerstören viele ihrer 210 Turing-Bomben, um das Geheimnis der Enigmaentschlüsselung zu wahren. Angeblich werden etwa 50 Bomben weiter verwendet.

1945-1975: Die Alliierten verkaufen erbeutete und nachgebaute Enigmas in den Nahen Osten und nach Afrika.

1974: Spätestens durch das Buch *The Ultra Secret* des Kriegsveteranen *F. W. Winterbotham* wird bekannt, dass die Enigma bereits während des Krieges geknackt wurde.

Verluste im Seekrieg



Sieglinde Brunhilde Tschaki tschaki@bit.uni-bonn.de
Michael Nüsken nuesken@bit.uni-bonn.de
b-it (Bonn-Aachen International Center for Information Technology)

Mit Unterstützung der Deutsche Telekom Stiftung

In Kooperation mit: :wissenschaftsregion bonn

Deutsches Museum Bonn

Wissenschaftsjahr 2008 Mathematik Alles, was zählt