

<b>Zeitschrift:</b>	Armee-Logistik : unabhängige Fachzeitschrift für Logistiker = Organo indipendente per logistica = Organ independenta per logistichers = Organ indépendent pour les logisticiens
<b>Herausgeber:</b>	Schweizerischer Fourierverband
<b>Band:</b>	93 (2020)
<b>Heft:</b>	4
<b>Rubrik:</b>	Kryptografie

### Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 22.02.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

# Kryptografie

**Kryptografie** altgriechisch *kryptós*, deutsch «verborgen», «geheim» und *gráphein*, deutsch «schreiben» ist ursprünglich die Wissenschaft der Verschlüsselung von Informationen. Sie bezeichnet die Verschlüsselung von Nachrichten oder Daten zum Zwecke der Geheimhaltung.

Heute befasst sie sich auch allgemein mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind.

## Allgemein

Der Begriff Kryptografie bedeutet Geheimschrift; sie befasste sich historisch mit der Erzeugung, Betrachtung und Beschreibung von Verfahren, um «geheim zu schreiben», also mit Verschlüsselungsverfahren. Seit Ende des 20. Jahrhunderts werden sie zur sicheren Kommunikation und für sichere Berechnungen eingesetzt.

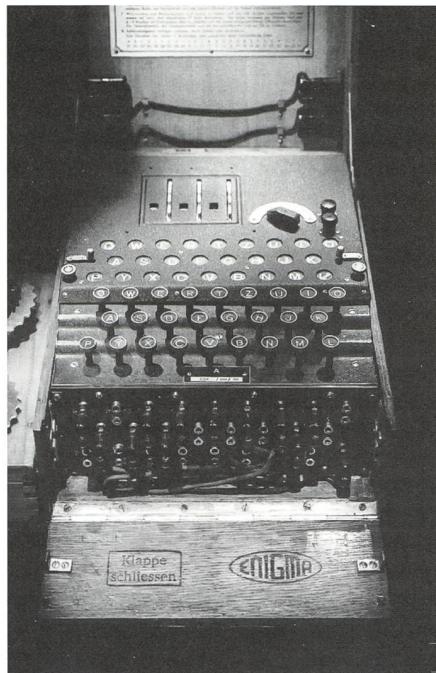
Die moderne Kryptografie hat vier Hauptziele zum Schutz von Datenbeständen, Nachrichten und/oder Übertragungskanälen:

1. Vertraulichkeit/Zugriffsschutz: Nur dazu berechtigte Personen sollen in der Lage sein, die Daten oder die Nachricht zu lesen oder Informationen über ihren Inhalt zu erlangen.
2. Integrität/Änderungsschutz: Die Daten müssen nachweislich vollständig und unverändert sein.
3. Authentizität/Fälschungsschutz: Der Urheber der Daten oder der Absender der Nachricht soll eindeutig identifizierbar sein, und seine Urheberschaft sollte nachprüfbar sein.
4. Verbindlichkeit/Nichtabstreichbarkeit: Der Urheber der Daten oder Absender einer Nachricht soll nicht in der Lage sein, seine Urheberschaft zu bestreiten, d.h., sie sollte sich gegenüber Dritten nachweisen lassen.

Kryptografische Verfahren und Systeme dienen nicht notwendigerweise gleichzeitig allen der hier aufgelisteten Zielen.

## Geschichte

Die Geschichte der Kryptografie kann in drei Epochen aufgeteilt werden. In der ersten wurde per Hand (z.B. mit Papier und Bleistift oder mit mechanischen Scheiben) verschlüsselt, in der zweiten (ca. 1920–1970) wurden spezielle Maschinen verwendet, in der dritten (ca. seit 1970) übernahmen Computer eine zentrale Rolle. Die Kryptoanalyse bildet das ergänzende Ge-



Enigma Quelle Bletchley Park

genstück zur Kryptografie. Dabei werden Methoden erforscht, um kryptografische Verfahren zu analysieren und möglichst zu brechen (Entzifferung). Kryptografie und Kryptoanalyse sind Teilgebiete der Kryptologie.

## Epoche der Verschlüsselung von Hand

Bei den alten Ägyptern im 3. Jahrtausend vor Christus finden sich die frühesten Hinweise auf verschlüsselte Texte. Es handelte sich um religiöse oder magische Texte, nur für eingeweihte Personen lesbar. Der Text – Klartext – wurde unlesbar gemacht und wurde zum Geheimtext. Nur wer den Schlüssel kannte, konnte ihn entziffern.

Bei der altgriechischen Skytale aus dem 5. Jahrhundert vor Christus fand dieser Prinzip ebenfalls Anwendung. Ein Papyrusband wurde um einen Stab gewickelt und beschrieben. Die Botschaft war vom Stab gerollt unlesbar. Das Band musste auf einen gleich dicken Stab gerollt werden, damit es gelesen werden konnte. Um den Text zu decodieren war der Stab der Schlüssel. Der Verschlüsselungsstab beruhte auf dem Prinzip der Transposition.

Eine Verschlüsselungstechnik benützte auch der römische Feldherr Julius Cäsar. In seinen Nachrichten ersetze er jeden Buchstaben durch jenen der im Alphabet z.B. drei Stellen danach kommt. Das Cäsar-Chiffre verschob jeden Buchstaben im Alphabet um einen festge-

legten Wert. Es konnten viele Geheimschriften erzeugt werden, aber das einfache Verfahren bot keine Sicherheit.

Zwischen 500 und 1400 gab es vor allem in der arabischen Welt bedeutende Beiträge zur Kryptografie, wie erst viel später bekannt wurden; z.B. sind statistische Methoden zur Kryptoanalyse beschrieben worden.

In Italien wurde das System im 15. Jahrhundert durch das System der Chiffrierscheibe verbessert, die 1466 von Leon Battista Alberti beschrieben wurde. Diese bestand aus zwei beweglichen Ringen; auf der äußeren Scheibe mit dem Klartext-Alphabet und auf der inneren Scheibe mit dem Geheimtextalphabet. Die Scheiben bzw. Buchstaben konnten beliebig verschoben werden und die Buchstaben-Verschiebung wurde nicht starr gehandhabt, womit verschiedene Geheimalphabete entstanden. Der Empfänger des Geheimtextes benötigte zur Entzifferung zusätzlich zur Chiffrierscheibe nur noch die Reihenfolge der Einstellungen zu wissen.

Italien wurde dadurch zur führenden Kryptografie-Nation der damaligen Zeit.

Blaise de Vignière veröffentlichte 1508 die Tabula recta, welche lange als unknackbar galt und erst nach fast 300 Jahren systematisch entziffert werden konnte.

Im amerikanischen Sezessionskrieg 1861–1865 wurde bereits Telegrafie benutzt, doch die Bedeutung der Datenverschlüsselung und der Dechiffrierung wurden unterschätzt. Beide Seiten des Konflikts koordinierten den Bereich der Kryptografie nicht, auch nicht qualifizierte Experten. Es lag im Ermessen des jeweiligen Befehlshabers, welches Verfahren für welchen Zweck eingesetzt wurde. Trotz geringem Aufwand gelangen zahlreiche Entzifferungen.

Wenn man das benutzte Verfahren kannte, waren viele Verschlüsselungen leicht zu knacken; die Verfahren konnten nicht geheim gehalten werden. Auguste Kerckhoffs formulierte 1833 den Grundsatz der Kryptografie (Kerckhoffs' Prinzip), wonach die Sicherheit eines kryptografischen Verfahrens nur von der Geheimhaltung des Schlüssels und seinem Besitz abhängen soll und bei Bekanntwerden des Verschlüsselungsverfahrens (Algorithmus) nicht gefährdet sein darf.

Dieses Prinzip gilt auch noch heute und ist ein wichtiger Grundsatz der Kryptografie, der auch bei der Verschlüsselung im Internet eingehalten wird. Moderne Verschlüsselungsalgorith-

# Kryptografie

men sind keine Geheimnisse mehr und nur die für die Dechiffrierung nötigen Schlüssel sind geheim.

Im Ersten Weltkrieg wurden für taktische Zwecke vergleichsweise simple Verfahren eingesetzt; sie konnten per Hand mit Papier und Bleistift ausgeführt werden. Das bekannteste mit Namen ADFGX konnte im April 1918 geknackt werden. Der Erste Weltkrieg gilt als der erste Krieg, in welchem die Möglichkeiten der Kryptoanalyse systematisch genutzt wurden. Einige Staaten betrieben zu Kriegsbeginn noch gar keine Entzifferungseinheiten. Der Aufwand zur Entzifferung gegnerischer Funksprüche stieg im Verlauf des Krieges deutlich. Neue Verschlüsselungsverfahren konnten mit der Entwicklung nicht Schritt halten; dies führte dazu, dass alle im Ersten Weltkrieg verwendeten Methoden mit wenig Aufwand geknackt wurden. Auf höherer Ebene wurden im Ersten Weltkrieg vor allem Codebücher verwendet; mit denen konnte jedes Wort eines Textes in ein unverständliches anderes Wort oder eine Zahl umgewandelt werden. Ein deutsches verschlüsseltes Telegramm (Zimmermann-Depesche) konnte vom britischen Geheimdienst abgefangen und dechiffriert werden.

**Epoche der Verschlüsselung mit Maschinen**  
Als Vorläufer erfand Gottfried Wilhelm Leibniz 1688 mit der *Machina deciphatoria* eine Chiffriermaschine. Er nahm damit rund 200 Jahre früher das Prinzip der Rotor-Schlüsselmaschine von Arvid Damm vorweg, nach dem die erste Generation der mechanischen Chiffriermaschinen ab 1918 funktionierte.

Die deutschen Militärs wollten eine Wiederholung der kryptografischen Katastrophe des Ersten Weltkrieges unbedingt vermeiden und suchten einen Ersatz für die inzwischen veralteten, umständlichen und unsicheren manuellen Verschlüsselungsverfahren. Als sicherste Lösung erkannten sie die neue Art der maschinellen Verschlüsselung, weil sie eine einfachere Handhabung und eine verbesserte kryptografische Sicherheit versprachen.

Während des Ersten Weltkrieges und in den Jahren danach wurden erste Maschinen zur Verschlüsselung entwickelt. Diese boten eine deutlich höhere Sicherheit als die bis dahin üblichen manuellen Methoden. Die zahlreichen Verschlüsselungsmaschinen läuteten eine neue Epoche in der Kryptografie-Geschichte ein.

Mit der Einführung der elektrischen Schreibmaschine und des Fernschreibers zu Beginn des 20. Jahrhunderts kamen zum Teil unabhängig voneinander und nahezu gleichzeitig mehrere



M-209, Haglin

Quelle: Wikipedia

Erfinder auf die Idee des Rotor-Prinzips zur Verschlüsselung von Texten.

1917 entdeckt und entwickelt der Amerikaner Gilbert S. Vernam das One-Time-Pad, das einzig nachweisbar sichere Kryptosystem. Es fällt in die Zeit der ersten Maschinenentwicklungen. Bei diesem Verfahren wird der Text zeichenweise gemeinsam mit einer zufälligen Zeichenfolge verschlüsselt, die nur einmal verwendet wird. Handelt es sich wirklich um eine Zufallsfolge, ist jedes Verschlüsselungsergebnis gleich wahrscheinlich und das Verfahren ist mathematisch sicher. Der Amerikaner Joseph O. Mauborgne setzte diese Idee um und prägte den Begriff One-Time-Pad (deutsch: Eimal-Block). Der One-Time-Pad wurde schnell populär, da sich das Verfahren sowohl per Maschine als auch von Hand nutzen liess.

Der Amerikaner Edward Hugh Hebern 1917, der Deutsche Arthur Scherbius 1918 und der Niederländer Hugo Alexander Koch und der Schwede Arvid Gerhard Damm 1919 meldeten alle ihre Ideen zu Rotor-Chiffriermaschinen zum Patent an.

## Enigma

Die Enigma wurde vom deutschen Ingenieur Arthur Scherbius erfunden, dessen erstes Patent für diese Chiffriermaschine vom 23. Februar 1918 stammt. Der Name «Enigma» stammt aus dem Griechischen und bedeutet wörtlich übersetzt «Rätsel».

Am 15. April 1918 bot Scherbius seine neue Erfindung der Kaiserlichen Marine an, die aber den Einsatz einer maschinellen Verschlüsselung für nicht erforderlich erachtete und ablehnte. So beschoss er die Maschine nach dem Krieg

für zivile Anwendungen zu vermarkten. Dazu wurde zur Fertigung am 9. Juli 1923 die Chiffriermaschinen-Aktiengesellschaft (ChiMaAG) in Berlin gegründet.

Ursprünglich sollte die Enigma nur für zivile Prozesse verwendet werden und wurde deshalb auch erstmals auf Messen kommerziell angeboten. Das erste Modell der Enigma, Die Schreibende Enigma genannt, wurde auf Messen zum Kauf angeboten, 1923 in Leipzig und Bern und 1924 auf dem internationalen Postkongress des Weltpostvereins in Stockholm.

Durch Publikationen über alliierte Entzifferungserfolge von deutschen Marinefunksprüchen und Handschlüsselmethoden des Kaiserlichen Heeres im Ersten Weltkrieg wurde das Interesse des deutschen Militärs in den Folgejahren geweckt.

1926 wurde die Enigma zunächst von der Reichsmarine unter dem Namen Funkschlüssel C und zwei Jahre später auch vom Heer versuchsweise eingesetzt; sie verschwand daraufhin vom zivilen Markt.

Kurz nach Beginn der Serienfertigung verunglückte Scherbius 1929 tödlich. 1934 übernahmen Rudolf Heinsoeth und Elsbeth Rinke die ChiMaAG und setzten die Entwicklung und Produktion der Maschine in der neuen Firma Heimsoeth & Rinke in Berlin fort.

In der Zeit des Nationalsozialismus und im Zuge der Aufrüstung der Wehrmacht ab 1933 wurde ein zuverlässiges Verschlüsselungssystem benötigt; dem Erfolg der Enigma stand damit nichts mehr im Wege. Man schätzt, dass etwas mehr als 40'000 Maschinen hergestellt wurden. Die Enigma wurde in mehreren Varianten und in unterschiedlichen Modellen hergestellt und diese kamen noch nach Kriegsende 1945 zum Einsatz. Die meistgenutzte Maschine war die Enigma I (Enigma eins), die ab 1930 von der Reichswehr und später von der Wehrmacht eingesetzt wurde und während des Zweiten Weltkriegs das auf deutscher Seite am häufigsten benutzte Maschinenschlüsselverfahren verkörperte.

Die Enigma I besteht im Wesentlichen aus der Tastatur zur Buchstabeneingabe, einem Walzensatz von drei austauschbaren Walzen und einem Glühlampenfeld zur Anzeige.

Wichtigste Funktionsgruppen der Enigma I: Tastatur, Walzensatz, Lampenfeld und Steckerbrett.

Der Walzensatz ist das Herzstück der Verschlüsselung. Die drei Walzen sind nebeneinander, unabhängig, drehbar angeordnet. Jede von ihnen weist auf beiden Seiten 26 elektrische Kontakte auf. Jeder Kontakt ist einem der 26 Grossbuchstaben des lateinischen Alphabets

zugeordnet. Drückt man eine Buchstaben-taste, so fliesst elektrischer Strom von einer in der Enigma befindlichen 4.5-Volt-Batterie über die gedrückte Taste durch den Walzensatz und lässt eine Anzeigelampe aufleuchten. Der aufleuchtende Buchstabe entspricht der Ver-schlüsselung des gedrückten Buchstabens. Da sich bei jedem Tastendruck die Walzen ähnlich einem mechanischen Kilometerzähler weiter-drehen, ändert sich das geheime Schlüssel-alphabet nach jedem Buchstaben.

### B, C und M Maschinen

Emanuel Nobel finanzierte dem Schweden Bo-  
ris Hagelin ein Büro und versorgte ihn mit Auf-trägen. Die wichtigste Aufgabe war die Aufsicht  
über die 1915 gegründete AB Cryptograph. Das  
Unternehmen hatte Arvid Damm gegründet  
unter Beteiligung von privaten Geldgebern. Am  
10. Oktober 1919 meldete Damm seine Rotor-  
Chiffriermaschine in Deutschland zum Patent  
an, drei Tage nach Hugo Alexander Koch. Dem  
Unternehmen ging 1921 das Kapital aus; in der  
Folge beteiligten sich Nobel und der Vater von  
Hagelin finanziell, da sie überzeugt waren, dass  
Chiffriermaschinen im Schriftverkehr heikler  
Angelegenheiten eine Rolle spielen könnten.  
Damm konnte das Interesse grosser Radioge-  
sellschaften für seine Maschine wecken, die auf  
drahtlose Telegrafie ausgelegt war. Die Proto-  
typen sollten in Paris gebaut werden. Hagelin  
übernahm auch die technische Leitung des  
Unternehmens, in welchen bereits der Kon-  
strukteur C. A. Lindmark arbeitete, der später  
beim Aufbau der ersten C-Maschinen bedeut-  
same Beiträge leistete.

1925 erhielt der schwedische Generalstab eine  
Enigma-Maschine von einem Deutschen Unter-  
nehmen für Versuchszwecke. Es gelang Hagelin  
den zuständigen Offizier davon zu überzeugen,  
dass sein Unternehmen bereits eine zehnjähri-  
ge Erfahrung auf dem Gebiet von Chiffriermas-  
chinen besitzt und sie deshalb eine bessere  
Maschine bauen könne. Hagelin erhielt den  
Auftrag eine Mustermaschine innerhalb von  
sechs Monaten zu bauen. Die Annahme des  
Auftrags war ein Vabanque-Spiel, aber es gelang  
einen Prototyp innerhalb der gesetzten  
Frist zu bauen, mit Namen B-211, der äusserlich  
der Enigma ähnlich sah. Hagelin reichte seinen  
Patentantrag sowohl in Schweden als auch in  
den USA ein.  
1927 übernahm Hagelin die Firma AB Crypto-  
graph, reorganisierte sie und änderte den Na-  
men in AB Cryptoteknik.

Ab 1932 reiste Hagelin durch Europa, um Käu-  
fer zu finden. Die französische Armee zeigte  
Interesse, verlangte jedoch Modifikationen,  
insbesondere zwei Bedingungen: Die Maschi-



General Guderian wartet auf eine Entschlüsselung  
eines Funkspruchs (1940) Quelle: Bundesarchiv (D)

ne sollte Text drucken können und dennoch  
tragbar sein. In der Privatwirtschaft konnte  
für den Büroeinsatz eine elektrische Schreib-  
maschine angekoppelt werden. Die Maschine wurde  
in Frankreich hergestellt bei L.M. Ericsson, eine Tochtergesellschaft der Telefon-AB,  
in Colombes bei Paris.

Die französische Armee fragte Hagelin 1934,  
ob er nicht einen druckenden Taschenapparat  
konstruieren könne. An der Entwicklung der C-  
Maschine, die weltweit die erfolgreichste wer-  
den sollte, war sein Mitarbeiter C. A. Landmark  
unentbehrlich geworden. So entstand 1935  
die unter der Bezeichnung C-35 vorgestellte  
Chiffriermaschine. Eine erhebliche Verbesse-  
rung der C-35 konnte durch die Mitarbeit des  
schwedischen Kryptologen Yves Gyldén erzielt  
werden. Dieses Modell C-36 hatte die Grösse  
einer Brotdose und wurde als epochale Erfin-  
dung bezeichnet. Bis Kriegsausbruch wurden  
ca. 500 Maschinen B-211 ausgeliefert, nach  
dem Krieg nochmals 100 Stück.

Das Unternehmen wurde am Jahreswechsel  
1939/1940 in AB Ingenieursfirma Cryptoteknik  
umbenannt.

Zwischen 1937 und 1940 fuhr Hagelin dreimal  
in die USA, um einen Prototyp der BC-Maschi-  
ne vorzustellen. 1940 erhielt er einen Probe-  
auftrag von 50 Maschinen der tragbaren und  
verbesserten C-38 Version. Nach ausführlichen  
kryptologischen Tests wurde die Maschine für  
den taktischen Einsatz unterhalb der Divisions-  
ebene akzeptiert. In dieser Zeit scheint er auch  
in Amerika den weltbekannten Kryptologen  
William F. Friedman kennengelernt zu haben,

der von 1922 bis 1947 Cryptanalyst im War De-  
partment war. Mit ihm stand Hagelin bis zu des-  
sen Tod 1969 in ständigem Kontakt und erhielt  
Anregungen der verschiedensten Art.

In Amerika wurde Hagelins Maschine als M-209  
beim Corona-Werk des Schreibmaschinenher-  
stellers L. C. Smith in Lizenz-Produktion herge-  
stellt, mit einem Tagesausstoss von bis zu 500  
Maschinen. Die US-Marine bezeichnete sie als  
CSP-1500. Hagelin hatte während des Krieges  
für die Wartung und Einweisung zu sorgen, des-  
halb blieb er bis 1944 in den USA. Bis zu seiner  
Rückreise waren 50'000 Maschinen produziert  
worden, bei Kriegsende waren es über 140'000  
Stück.

Das Unternehmen hatte auch in Stockholm,  
während Hagelins vierjähriger Abwesenheit,  
unter der Leitung von Store Nyberg Aufträge  
aus verschiedenen Ländern erhalten. Ab ca.  
Anfang 1941 benutzte z.B. die italienische Ma-  
rine die Hagelin C-38m, eine Version der M-209.

### Zweiter Weltkrieg

Im Zweiten Weltkrieg nutzten die Deutschen  
mindestens sieben unterschiedliche Verschlüs-  
selungsmaschinen: Enigma, Lorenz-Schlüssel-  
maschine, T52, T43, Schlüsselgerät 39 und 41,  
Hellschreiber.

Die zu Zehntausenden im Einsatz stehende  
Enigma galt auf deutscher Seite irrtümlicher-  
weise als unbrechbar.

Nachdem polnische Abhörstationen bereits  
am 15. Juli 1928 zum ersten Mal einen mit der  
Enigma chiffrierten deutschen Funkspruch  
abgefangen hatten, und 1932 der polnische  
Kryptoanalytiker Marian Rejewski die innere  
Verdrahtung der Rotoren aufdecken konnte,  
gelang Biuro Szyfrów vom polnischen Chiffrier-  
dienst zur Jahreswende 1932/1933 die ersten  
Enigma-Entzifferungen. 1939 wurden die bri-  
tischen und französischen Verbündeten beim  
Treffen von Pyry von den Polen mit Aufzeich-  
nungen und Dokumentationen eingeweiht  
und ihnen polnische Nachbauten der Enigma  
übergeben.

In England erkannte man die Wichtigkeit,  
Nachrichten der Enigma zu entschlüsseln zu-  
nächst nicht. Die Einrichtung, die sich mit der  
Entschlüsselung von chiffrierten Nachrichten  
beschäftigte, befasste sich nur mit Codebü-  
chern. Diese Einrichtung, in der Nachrichten  
entschlüsselt wurden, war im Landsitz Blet-  
chley Park (B.P.) untergebracht dem Haupt-  
quartier der Government Cod and Cipher  
School (GCandCS). Als die Briten endlich die  
Bedeutung und die Wichtigkeit der Enigma er-  
kannten, war es fast schon zu spät.  
Den britischen Codebreakers um Alan Turing

gelang es während des Zweiten Weltkrieges äusserst erfolgreich, die mithilfe der Y-Stations abgefangenen deutschen Funksprüche zu entziffern. Turing war der erste, dem es gelang mathematische Berechnungen und Theorien aufzustellen, um in das System der Enigma einzubrechen. Er entwickelte die Turing-Bombe, die wie eine Maschine funktionierte und den Code der Enigma entschlüsselte. Die Bomben waren sehr gross und wurden in Hallen untergebracht und beaufsichtigt; es mussten nur die Rotoren an den Bomben eingestellt und informiert werden, falls eine der Bomben stoppen sollte. An Januar 1940 wurde der deutsche Enigma-Funkverkehr mit nur wenigen Ausnahmen kontinuierlich mitgelesen.

Die Amerikaner nutzten im Zweiten Weltkrieg die von Hagelin entwickelte M-209, eine vergleichsweise kleine und handliche Maschine, die in grossen Stückzahlen gebaut wurde. Den Deutschen gelang es, diese Maschine mit Hilfe eines speziellen Dechiffriergeräts zu knacken.

Für wichtigere Nachrichten kam die Rotor-Verschlüsselungsmaschine SIGABA zum Einsatz; ihre Funktionsweise ähnelte der Enigma, sie bot jedoch eine grössere Sicherheit. Nach heutigem Wissensstand wurde die SIGABA nie geknackt.

Eine wichtige Rolle spielte der Navajo-Code während des Pazifikkrieges der US gegen Japan ab 1942. Die Verschlüsselungsmethode beruhte darauf, Angehörige des nordamerikanischen Indianer-Stammes der Diné (Navajo) als Codesprecher zu benutzen. Diese übersetzten die militärischen Anweisungen jeweils in ihre Muttersprache Navajo, die mit keiner europäischen oder asiatischen Sprache verwandt ist; deshalb der undurchdringliche Navajo-Code.

Den US-amerikanischen Dechiffrieren gelangen im Zweiten Weltkrieg grosse Erfolge, insbesondere das Entziffern der japanischen PURPLE. Nach ersten Einbrüchen in japanische Code-Systeme ca. 1940 wurde PURPLE

nach und nach von einer Gruppe um den amerikanischen Mathematiker und Kryptologen William Friedman enträtselt. Später war man in der Lage die Maschine nachzubauen und Funksprüche im Rahmen der Aktion MAGIC zu entschlüsseln. Im Dezember 1941 wurde ein mit PURPLE verschlüsselter Funkspruch mitgehört und entschlüsselt. Der Text enthielt den Abbruch der diplomatischen Beziehungen und war letztendlich die Kriegserklärung vor dem Angriff auf Pearl Harbour. Verzögerungen bei der Auswertung und Weitergabe der Information verhinderten eine rechtzeitige Warnung, mittels regulärem zivilen Telegramm traf die Nachricht nach dem Angriff auf den Flottenstützpunkt ein.

Quellen: Wikipedia und diverse Publikationen

Roland Haudenschild

# Ausgesucht für die Schweizer Armee

Transgourmet Schweiz AG  
Lochackerweg 5  
3302 Moosseedorf  
Telefon 031 858 48 48  
**transgourmet.ch**



**TRANSGOURMET  
PRODEGA**