Kryptoanalyse mit der Maschine

1 Rotormaschinen

Das bei den im zweiten Weltkrieg eingesetzten Schlüsselmaschinen benutzte *Rotorprinzip* geht auf Edward Hugh Hebern zurück, der 1917 mit der "Electric code machine" (Patentanmeldung 1921) eine rotierende Vorrichtung zur "polyalphabetischen Substitution mit unabhängigen Alphabeten" erfand. Diese Erfindung stiess zunächst auf nur spärliches Interesse. Doch bereits ein Jahr später wurde das Rotorprinzip (Abb. 2-14) von Arthur Scherbius zum Patent angemeldet und mit dem Bau der "Enigma" (griech. Rätsel) in die Tat umgesetzt. Das staatliche Interesse hielt sich zunächst in Grenzen und nahm erst mit Deutschlands Aufstieg zur Weltmacht zu. Später war die Enigma die meistverwendete (aber nicht die einzige) Chiffriermaschine deutscher Nachrichtenübermittlungsstellen.

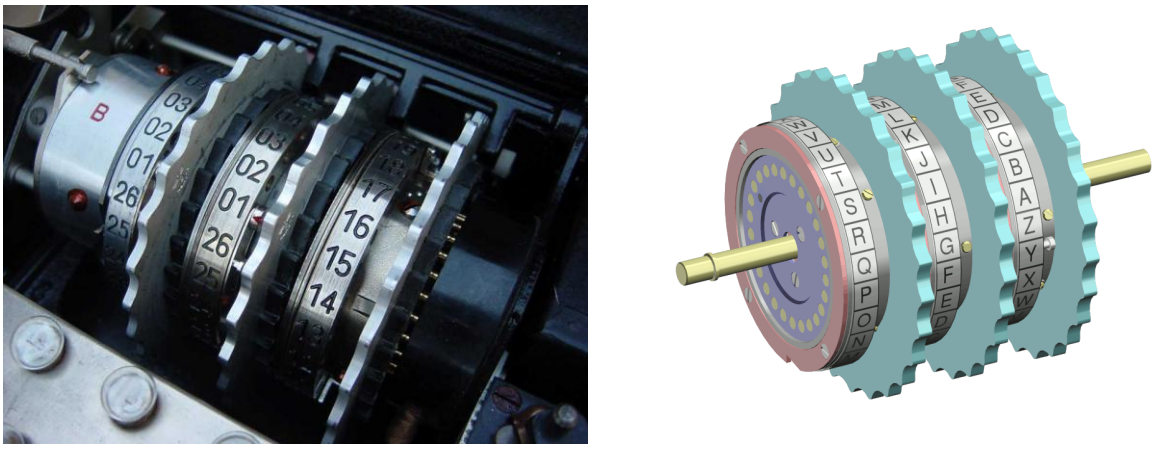

Abb. 2-14
ENIGMA-Walzen[1]

Anm.: Die **Rotoren** (auch als Walzen bezeichnet) sind drehbar angeordnet und ihre Stellung zueinander ändert sich dauernd während des Schlüsselvorgangs. An ihren Außenflächen besitzen sie mehrere Kontakte (meist 26 für die Großbuchstaben des lateinischen Alphabets), die im Innern durch isolierte Drähte gekreuzt miteinander verbunden sind. Durch die Drehung der Rotoren wird für jeden Buchstaben des Textes eine unterschiedliche (polyalphabethische) Substitution erzielt. Die Sicherheit der Verschlüsselung hängt wesentlich von der Anzahl der verwendeten Rotoren ab, da die Menge der möglichen Substitutionen im Schlüsselraum multiplikativ mit der Anzahl der eingesetzten Rotoren ansteigt.[2]

Unabhängig von den Genannten wurde das Rotorprinzip 1919 auch in den Niederlanden von Hugo Koch (Urheberschaft umstritten) und in Schweden von Arvid G. Damm entwickelt. Die Hebern-Rotormaschine wurde später durch die von William F. Friedman entwickelte SIGABA[3] ersetzt, die für den Nachrichtenverkehr der US-amerikanischen Streitkräfte von entscheidender Bedeutung war.

[1] http://de.wikipedia.org/wiki/Enigma-Walzen
[2] http://de.wikipedia.org/wiki/Rotor-Chiffriermaschine
[3] http://de.wikipedia.org/wiki/SIGABA

Mit der **ENIGMA** (Abb. 2-15) besass das deutsche Oberkommando der Wehrmacht ein unverzichtbares Schlüsselgerät. Als die Enigma patentiert wurde, galt sie zu recht als "unknackbar". Später jedoch wurde der Code von den Polen und danach von den Briten entziffert. Seit 1933 wurde der Apparat beim Heer, der Marine und im diplomatischen Dienst eingesetzt. Das Gerät unterlag einer permanenten Weiterentwicklung. Der Hersteller hatte das Rotorprinzip bereits 1928 durch ein Steckbrett ergänzt, wodurch der Verschlüsselungsgrad erheblich gesteigert wurde. Der Schlüsselraum der in der Wehrmacht benutzten Drei-Rotoren-Enigma betrug +2e23 (entsprechend einer Schlüssellänge von 77 Bit). Die aus Gründen der Sicherheit in der Marine eingesetzte Vier-Rotoren-Enigma besass eine noch grössere Verschlüsselungstiefe. Die Abwehr benutzte eine Sonderform ohne Steckerbrett. Übermittelte Nachrichten konnten nur entschlüsselt werden, wenn der Empfänger sämtliche Einstellungen der Sendestation kannte. Dazu bedurfte es eines Tagesschlüssels, um die Walzen und deren Lage sowie die Rotorstellung zu kennen. Später kam zusätzlich ein zu übermittelnder Spruchschlüssels hinzu. Unter dieser Voraussetzung konnte mit der empfangenden Enigma die Botschaft dechiffriert und im Klartext ausgelesen werden. Eine für die britischen Codebrecher nicht geringe Problematik, an der sie zunächst verzweifelten.

Abb. 2-15
Rotor-Schlüsselmaschine ENIGMA mit Steckerbrett[4]

2 Enigma entziffert

Lange galt die Enigma als unknackbar. Einige Jahre vor dem zweiten Weltkrieg übergab der Spion Hans-Thilo Schmid geheime Schlüsseltafeln und Bedienungsanleitungen an die Franzosen. Zu jener Zeit waren drei Walzen im Einsatz. Deren Lage wurde in vierteljährlichen Intervallen gewechselt. Bereits 1932 gelang es dem Mathematiker Marian Rejewski aus dem polnischen Chiffrierbüro BS4, hinter das Geheimnis der Enigma zu kommen. Infolge eines verfahrenstechnischen Vorganges der deutschen Übermittler gelang es Rejewski, den bisher unüberwindbaren Schlüsselraum auf lediglich 105'456 Möglichkeiten zu reduzieren. Mittels eines als *Zyklometer* bezeichneten Gerätes gelang es ihm ferner, die zugehörigen Permutationen zu finden. Die so ermittelten Charakteristika wurden in einem Katalog erfasst. Damit wurden bereits vor dem zweiten Weltkrieg die Voraussetzungen geschaffen, um die

[4] http://de.wikipedia.org/wiki/Enigma_(Maschine)

deutschen Botschaften zu entschlüsseln. Weil später diverse Modifikationen an der Enigma vorgenommen wurden, erwiesen sich Katalog und Zyklometer schliesslich als nutzlos. Dies führte zur Erfindung der Lochkarten-Methode (Zygalski) und schliesslich zur Konstruktion der *Bomba*.[5] Mittels dieses elektromechanischen Dechiffriergerätes gelang es den Polen, die gesuchten Permutationen innert weniger Stunden zu finden und so den Tagesschlüssel von Heer und Luftwaffe zu ermitteln. Später erhöhten die Deutschen die Walzenzahl. Lagenwechsel erfolgten nun täglich. Im Sommer 1939 übergaben die Polen ihr Wissen mitsamt den Konstruktionsplänen der "Bomba" den britischen Abhörspezialisten in Bletchley Park, nördlich von London (Domizil der "Government Code and Cypher School", die aus dem "Room 40" hervorgegangen war). Gegen Kriegsende waren in der "Station X" über 9'000 Mitarbeiter tätig. Der britische Premierminister bezeichnete diese dem MI6 zugehörige Institution als "Gans die goldene Eier legt und nie gackert".

3 Turing-Bomben

Die Entzifferung der Enigma-Sprüche erhielt den Decknamen "Ultra". Nachhaltigen Erfolg beim Dechiffrieren erzielten die Briten mit der *Turing-Bombe*[6], einer elektromechanischen Codebreaker-Maschine, die vom genialen Kryptoanalytiker und Mathematiker Alan Turing[7] ersonnen wurde. Verbessert wurde diese Maschine von Gordon Welchmann durch die Einführung des "Diagonal board". Bis Kriegsende wurden über 210 Exemplare der Turing-Bombe allein in England in Betrieb genommen.

Anm.: Turing zählte zu den besten Analytikern seiner Zeit. Bekannt ist die von ihm erdachte *Turingmaschine*[8] (1936) und das damit assoziierte Halteproblem. Aufgrund seiner homosexuellen Neigung geriet Turing nach dem Krieg mit dem Gesetz in Konflikt und musste sich anschliessend einer Hormonkur unterziehen. Dadurch gedemütigt kam es 1954 zum Suizid, wozu Turing in einen mit Zyankali präparierten Apfel biss. So wenigstens lautet die offizielle Version.

Sämtliche Bomben wurden nach dem Krieg zerstört. Weil Churchill ein absolutes Stillschweigen über die in Bletchley Park getätigten Vorgänge verhängte, blieben Turings kryptoanalytische Verdienste der Öffentlichkeit bis in die siebziger Jahre verborgen. Diese exzessive Geheimhaltung erscheint aus heutiger Sicht unverständlich. Der Bann wurde erst 1974 aufgehoben, als Frederick W. Winterbotham sein brisantes Buch "Operation Ultra" veröffentlichen konnte. Bis dahin hatte kein einziger der involvierten Mitarbeiter auch nur ein Sterbenswörtchen preisgegeben.

Dieses Beispiel zeigt exemplarisch auf, dass eine auf höchster Ebene verordnete Geheimhaltung über Jahrzehnte hinweg möglich ist. Ähnliches ist im Umfeld von Area 51 (Dreamland) zu finden, wo futuristische Flugmaschinen getestet werden.

[5] http://de.wikipedia.org/wiki/Bomba
[6] http://de.wikipedia.org/wiki/Turing-Bombe
[7] http://de.wikipedia.org/wiki/Alan_Turing
[8] http://de.wikipedia.org/wiki/Turingmaschine

4 Colossus

Bei den auf oberster Führungsebene üblichen Fish-Chiffren (verschlüsselter Fernschreibcode) wurden von deutscher Seite Schlüsselmaschinen von Lorenz als auch von Siemens & Halske eingesetzt.

a) Ab Februar 1944 vermochten die Briten mit ihrem *Colossus* (Abb. 2-16) sämtliche mit der Lorenz-Schlüsselmaschine[10] verfassten Nachrichten zu entziffern. Der Lorenzschreiber war bei den Codebrechern als "Tunny" (Thunfisch) bekannt. Infolge der Unachtsamkeit eines Übermittlers gelang den britischen Kryptoanalytikern schliesslich die Entzifferung der Lorenz-Chiffre. Weil das Knacken des Codes von Hand zu lange dauerte, wurden daraufhin zehn Colossus-Maschinen eingesetzt.

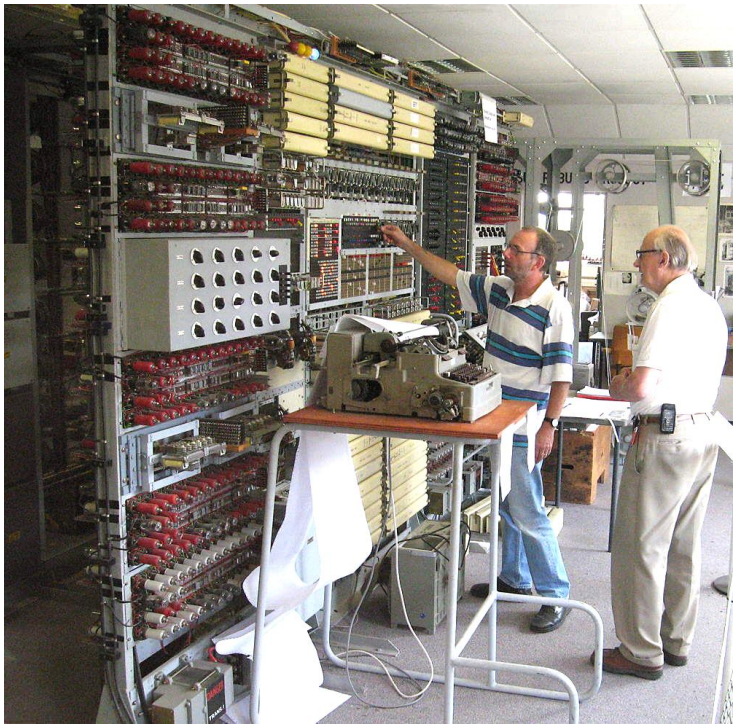

Abb. 2-16
Colossus (Rebuild)[9] in Bletchley Park.

In den 1990er Jahren entstand nach jahrelangen Vorarbeiten ein Nachbau des legendären Colossus. Treibende Kraft hinter dem "Rebuild Project" war der Nachrichtendienstler Tony Sale.

Die anfängliche Idee für diese geniale Lösung stammte von Max Newman. Die entscheidende Verbesserung und Realisierung kam von Tommy Flowers, einem versierten Elektroingenieur. Innert weniger Monate baute dieser im Forschungszentrum der Britischen Post in Dollis Hill einen aus 1'500 Elektronenröhren bestehenden Computer zusammen. Um die Lebensdauer der Röhren zu erhöhen, wurden sie mit Unterspannung betrieben. Zum Glück für die britische Abwehr besass Flowers bereits einschlägige Erfahrung aus dem Bau von elektronischen Telefonzentralen.

b) Der von Siemens & Halske gebaute Geheimschreiber T52 war bei den Briten als "Sturgeon" bekannt. Der G-Schreiber chiffrierte die aus dem Fernschreiber kommenden 5-Bit-Zeichen (Beaudot-Code), indem er diese mit den aus einem (Quasi)-Zufallsgenerator kommenden Streams nach einer XOR-Logik verknüpfte. Anschliessend erfolgte eine Permutation.

Anm.: Die Schweden lasen ab 1941 die deutschen Geheimbotschaften routinemässig mit. So war ihnen "Unternehmen Barbarossa" (Hitlers Angriff auf die Sowjetunion) frühzeitig bekannt. Der schwedische Mathematiker Arne Beuerling vom "Zimmer 100" entzifferte den Geheimschreiber-

[9] http://de.wikipedia.org/wiki/Colossus
[10] http://de.wikipedia.org/wiki/Lorenz-Schl%C3%BCsselmaschine

Code innert nur zweier Wochen. Die Entzifferung dieser Chiffre zählt zu den Meisterleistungen in der Geschichte der Kryptologie.

5 PURPLE

Auch die Japaner verschlüsselten vor und während dem zweiten Weltkrieg ihre Nachrichten. Die abgesetzten Funkmeldungen blieben den Abhördiensten ebensowenig verborgen wie die Schiffsbewegungen der japanischen Kriegsmarine auf hoher See. Die hervorragende Physikingenieurin und Kryptologin Agnes Meyer Driscoll[11] knackte den 5-Num-Code (JN-25) der kaiserlichen Marine. Nach dem Krieg war Driscoll als Kryptoanalytikerin bei der ins Leben gerufenen NSA[12] tätig.

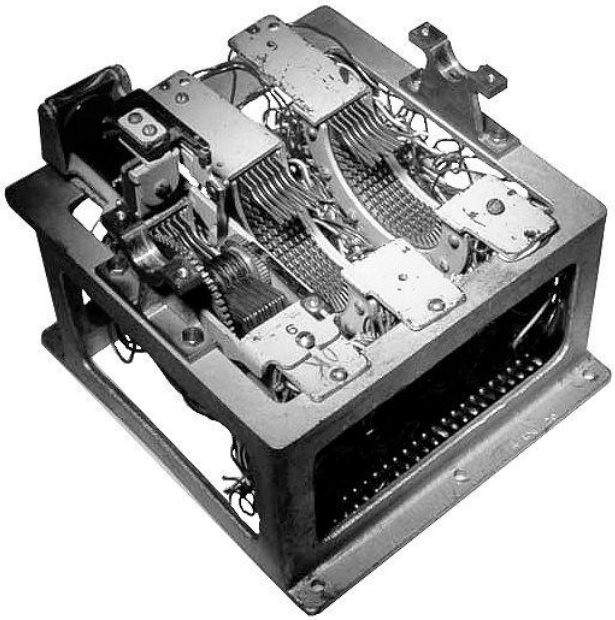

Abb. 2-17
PURPLE Chriffriermaschine

Die im diplomatischen Dienst benutzte und als *PurpleE*[13] bezeichnete Schlüsselmaschine (Abb. 2-17) besass anstelle der sonst üblichen Walzen mehrere elektromechanische Wählschalter und galt als besonders sicher. Die technischen Verbesserungen stammten von Risaburo Ito, einem Officer der kaiserlichen Marine.

Zunächst erwies sich der von PURPLE generierte Magic-Code als äusserst widerstandsfähig. Einem Team des US-Army “Signals Intelligence Service” (SIS) unter der Leitung von William Friedman gelang schliesslich diese als unmöglich geltende Aufgabe. Eine nicht geringere Leistung als das Friedman-Team erbrachte Leo Rosen mit dem Nachbau der PURPLE.

Literatur

Rudolf Kippenhahn: Verschlüsselte Botschaften (Rowohlt)

Klaus Schmeh: Codeknacker gegen Codemacher (w3l)

Albrecht Beutelsbacher: Geheimsprachen (C.H. Beck)

Simon Singh: Codes (Deutscher Taschenbuch Verlag)

Friedrich L. Bauer: Entzifferte Geheimnisse (Springer)

Stephen Harper: Kampf um Enigma. Die Jagd auf U 559 (Ullstein)

Joachim Beckh: Blitz und Anker, 2 Bände (BoD)

Bengt Beckmann: Arne Beurling und Hitlers Geheimschreiber (Springer)

[11] http://de.wikipedia.org/wiki/Agnes_Meyer_Driscoll
[12] NSA = **N**ational **S**ecurity **A**gency
[13] http://de.wikipedia.org/wiki/PURPLE