1 Die Enigma

Lange sicherte die Verschlüsselungsmaschine Enigma der deutschen Wehrmacht nachrichtendienstliche Vorteile. Als es den Alliierten gelang die als unknackbar geltende Verschlüsselung zu dechiffrieren ging auch der 2. Weltkrieg bald seinem Ende entgegen. Der folgende Artikel zeichnet die Geschichte der ENIGMA und deren Enschlüsselung nach.

Die Entstehungsgeschichte der Enigma

Der deutsche Erfinder Arthur Scherbius und sein enger Freund Richard Ritter gründeten 1918 die Firma Scherbius & Ritter, ein innovatives Unternehmen, das vom Heizkissen bis zur Turbine alles Erdenkliche herstellte. Scherbius, ein findiger und umtriebiger Geist, war für Forschung und Entwicklung zuständig. Es war eines seiner Lieblingsvorhaben, die unzulänglichen Chiffriersysteme aus dem Ersten Weltkrieg durch neue zu ersetzen. Bleistift und Papier sollten der Vergangenheit angehören, das neue System sollte die technischen Möglichkeiten des 20. Jahrhunderts nutzen. Scherbius, der in Hannover und München Elektrotechnik studiert hatte, entwickelte eine kryptographische Maschine. Er Nannte sie Enigma, und sie sollte die gefürchtetste Chiffriermaschine der Geschichte werden.

Arthur Scherbius

Scherbius' Enigma enthält eine Reihe raffiniert ausgetüftelter Elemente, die er zu einer beeindruckend komplizierten Verschlüsselungsmaschine zusammenbaute. Wenn wir die Maschine jedoch wieder in ihre Bestandteile zerlegen, können wir nachvollziehen, wie sie arbeitet. Sie besteht in ihrer Grundausführung aus drei Hauptelementen die miteinander verdrahtet sind:

- eine Tastatur für die Eingabe der Klartextbuchstaben,
- eine Verschlüsselungseinheit, die jeden Klarbuchstaben in einen Geheimtextbuchstaben verwandelt, und
- einen Lampenfeld, das die Geheimbuchstaben anzeigt.

Abbildung 1 zeigt einen vereinfachten Bauplan einer solchen Maschine für ein Alphabet von sechs Buchstaben. Um eine Klarbotschaft zu verschlüsseln, tippt der Chiffreur den jeweiligen Klarbuchstaben in die Tastatur, die ein elektrisches Signal durch die zentrale Verschlüsselungseinheit bis auf die andere Seite schickt, wo der Strom die Lampe für den entsprechenden Geheimbuchstaben aufleuchten lässt.

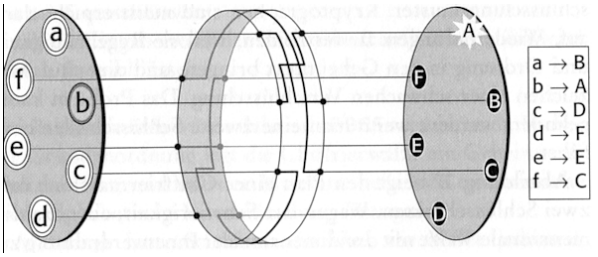


Abbildung 1

Der wichtigste Teil der Maschine ist die Walze (auch Rotor genannt), eine dicke Gummischeibe, die von Drähten durchzogen ist. Von der Tastatur ausgehend, führen die Drähte an sechs Punkten in die Walze hinein, in deren Innern sie kreuz und quer verlaufen, bis sie schliesslich an sechs Punkten auf der anderen Seite austreten. Die Verdrahtung im Innern der Walze bestimmt, wie die Klarbuchstaben verschlüsselt werden.

Die Botschaft `cafe` würde mit obiger Walze daher als DBCE verschlüsselt. In dieser Grundanordnung legt die Chiffrierwalze ein Geheimtextalphabet fest, und mit der Maschine liesse sich eine einfache monoalphabetische Verschlüsselung erzeugen.

Allerdings hatte Scherbius die Idee, die Walze jedes mal, wenn ein Buchstabe verschlüsselt war, weiterzudrehen, und zwar um ein Sechstel ihres Umlaufs (also um ein Sechsundzwanzigstel ihres Umlaufs bei einem vollständigen Alphabet von 26 Buchstaben). Abbildung 2 zeigt die gleiche Anordnung wie oben; wiederum wird durch die Eingabe des Buchstaben b das Lämpchen für A aufleuchten. Diesmal jedoch wird sich unmittelbar nach der Eingabe des Klarbuchstabens und

dem Aufleuchten des Geheimbuchstabens die Schlüsselwalze um ein Sechstel ihres Umlaufs weiterdrehen.

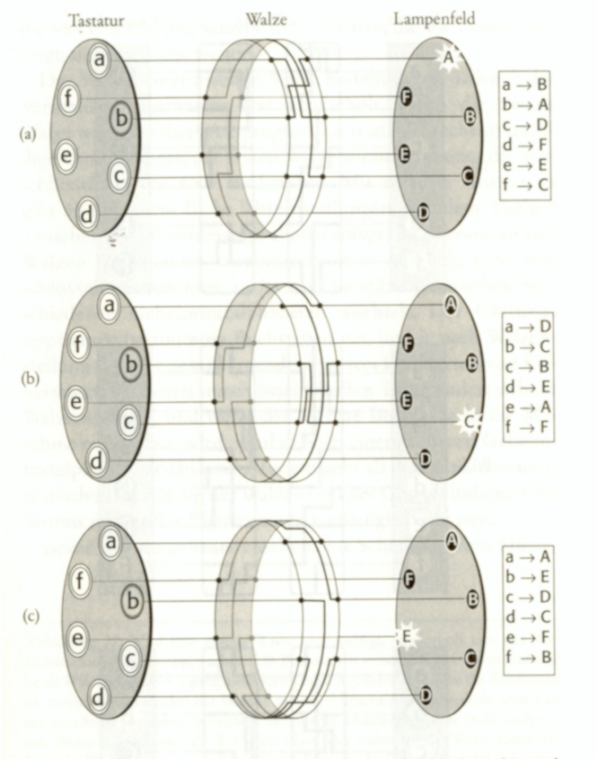


Abbildung 2

Wird jetzt noch einmal b eingegeben, dann leuchtet ein anderer Buchstabe auf, nämlich C. Wird sechsmal in Folge b eingetippt, erhält man den Geheimtext ACEBDC. Die Maschine, die mit dieser rotierenden Walze ausgestattet ist, bietet sechs Geheimtextalphabete und ist daher für eine polyalphabetische Verschlüsselung geeignet.

Die rotierende Walze ist das wichtigste Element des Grundmodells von Scherbius. Bislang hat die Maschine jedoch einen offensichtlichen Schwachpunkt. Wenn b sechsmal eingetippt wurde, kehrt die Walze in ihre ursprüngliche Position zurück, und wenn weiter b eingegeben wird, wiederholt sich das Verschlüsselungsmuster. Kryptographen sind meist erpicht darauf, Wiederholungen zu vermeiden, weil sie Regelmässigkeit und Ordnung in den Geheimtext bringen, und dies sind Anzeichen einer schwachen Verschlüsselung. Das Problem kann gelindert werden, wenn man eine zweite Schlüsselwalze einführt.

Abbildung 3 zeigt den Plan einer Chiffriermaschine mit zwei Schlüsselwalzen. Jedesmal, wenn ein Buchstabe verschlüsselt wird, dreht sich die erste Walze um eine Stelle. Dagegen bleibt die zweite Walze die meiste Zeit über in der gleichen Position. Sie dreht sich erst, wenn die erste Walze eine vollständige Umdrehung hinter sich hat. Die erste Walze ist mit einem Federzapfen ausgestattet, und erst wenn dieser einen bestimmten Punkt erreicht, schiebt er die zweite Walze um eine Stelle weiter.

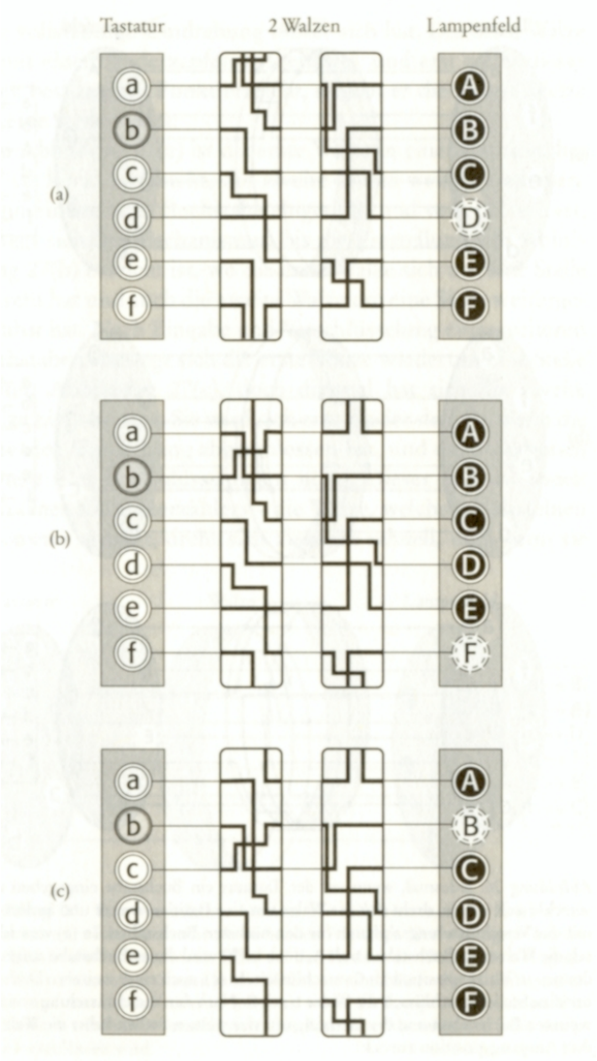


Abbildung 3

In der Abbildung 3 (a) ist die erste Walze in einer Position, bei der sie kurz davorsteht, die zweite Walze weiterzuschieben. Wenn ein weiterer Buchstabe eingetippt und verschlüsselt ist, bewegt sich der Mechanismus, bis die Einstellung von (b) erreicht ist, wo die erste Walze sich um eine Stelle gedreht hat und auch die zweite Walze um eine Stelle weitergeschubst hat. Nach Eingabe und Verschlüsselung eines weiteren Buchstabens bewegt sich die erste Walze wiederum eine Stelle weiter, (c), doch diesmal hat sich die zweite Walze nicht bewegt. Sie wird sich erst wieder drehen, wenn die erste eine Umdrehung abgeschlossen hat, und dazu sind noch weitere fünf Verschlüsselungen nötig.

Der Vorteil einer zweiten Walze besteht darin, dass sich das Verschlüsselungsmuster erst wiederholt, wenn die zweite Walze wieder in ihrer Ausgangsposition ist, was sechs vollständige Umdrehungen der ersten Walze voraussetzt oder die Verschlüsselung von 6 x 6

Buchstaben. Mit anderen Worten, es gibt 36 unterschiedliche Walzenstellungen, was dem Wechsel zwischen 36 Geheimtextalphabeten entspricht. Wenn man also Walzen miteinander kombiniert, ist es möglich, eine Verschlüsselungsmaschine zu bauen, die ständig zwischen verschiedenen Geheimtextalphabeten wechselt. Der Chiffreur tippt einen bestimmten Buchstaben ein, und je nach Walzenstellung kann er gemäss irgendeinem von Hunderten von Geheimtextalphabeten verschlüsselt werden. Dann ändert sich die Walzenstellung, und wenn der nächste Buchstabe in die Maschine eingegeben wird, wird er nach einem anderen Geheimtextalphabet verschlüsselt. Zudem geht all dies dank der automatischen Bewegung der Walzen und der Geschwindigkeit des Stroms mit grosser Effizienz und Genauigkeit vor sich.

Bevor wir uns genauer ansehen, wie Scherbius' Verschlüsselungsmaschine eingesetzt werden sollte, müssen wir zwei weitere Bauteile der Enigma kennenlernen, die Abbildung 4 zeigt.

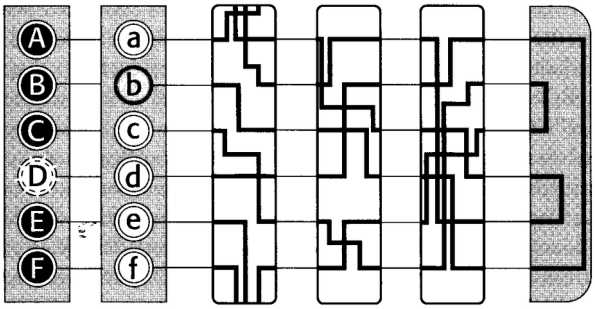


Abbildung 4

Zunächst baute man im Grundmodell der Enigma eine dritte Walze ein, die einen zusätzlichen Komplikationsgrad an Verschlüsselung erbrachte - bei einem vollständigen Alphabet ermöglichten diese Walzen 26 x 26 x 26 oder 17576 unterschiedliche Einstellungen. Zweitens fügte Scherbius einen Reflektor oder eine Umkehrwalze hinzu. Der Reflektor rotiert nicht, und die Leitungen treten auf derselben Seite wieder aus, auf der sie eintreten. Der Chiffreur tippt einen Buchstaben ein und schickt damit ein elektrisches Signal durch die drei Walzen und dann in den Reflektor. Der Reflektor schickt es durch die Walzen wieder zurück, doch auf einem anderen Weg. Bei der in Abbildung 4 gezeigten Stellung beispielsweise wird mit der Eingabe von b ein Signal durch die drei Walzen in den Reflektor geschickt, woraufhin es durch die Drähte zurückkehrt und den Buchstaben D aufleuchten lässt. Das Signal wird auf das Lampenfeld geleitet. Auf den ersten Blick erscheint der Reflektor vielleicht als ein sinnloser Zusatz zur Maschine, weil er unbeweglich ist und die Zahl der Geheimtextalphabete nicht erhöht. Sein Nutzen wird erst klar, wenn wir uns ansehen, wie die Maschine tatsächlich eingesetzt wurde, um eine Nachricht zu verschlüsseln und wieder zu entschlüsseln.

Ein Chiffreur will eine geheime Nachricht verschicken. Bevor er mit der Verschlüsselung beginnt, muss er die Walzen in eine bestimmte Ausgangslage drehen. Die Grundstellung entscheidet darüber, wie die Nachricht verschlüsselt wird. Wir können die Enigma als ein allgemeines Chiffriersystem betrachten, bei dem die Grundstellung die konkrete Verschlüsselung eines Textes bestimmt. Kurz, die Grundstellung ist der Schlüssel. Es war üblich, diese in einem Schlüsselbuch aufzulisten, das an alle Chiffreure im Funknetz verteilt wurde. Ein solches Schlüsselbuch zu verteilen kostet Zeit und Mühe (Schlüsseltauschprob-lem!), doch weil täglich nur ein Schlüssel gebraucht wird, konnte man ein Schlüsselbuch mit 28 Schlüsseln erstellen und damit vier Wochen lang über die Runden kommen.

Sobald die Walzen der Enigma nach dem jeweiligen Tagesschlüssel eingestellt sind, kann der Sender mit der Verschlüsselung beginnen. Er tippt den ersten Buchstaben der Nachricht ein, beobachtet, welcher Buchstabe auf dem Lampenfeld aufleuchtet, und notiert ihn als ersten Buchstaben des Geheimtextes. Die erste Walze hat sich inzwischen mechanisch um eine Stelle weitergedreht, der Chiffreur gibt nun den zweiten Buchstaben des Klartexts ein und so weiter. Hat er den vollständigen Geheimtext erzeugt, übergibt er ihn einem Funker, der ihn an den Empfänger sendet.

Um die Nachricht zu entschlüsseln, braucht der Empfänger ebenfalls eine Enigma und ein Exemplar des Schlüsselbuchs, das die Anfangseinstellung der Walzen für den jeweiligen Tag enthält. Nachdem er die Maschine vorschriftsgemäss eingestellt hat, tippt er den Geheimtext Buchstabe für Buchstabe ein, während auf dem Lampenfeld der jeweilige Klarbuchstabe aufleuchtet - Verschlüsselung und Entschlüsselung sind spiegelverkehrte Prozesse. Dass die Entschlüsselung so einfach ist, liegt am Reflektor.

Natürlich dürfen Schlüssel und Schlüsselbuch niemals in gegnerische Hände fallen. Es mag durchaus sein, dass der Gegner eine Enigma erbeutet, doch ohne die Anfangseinstellungen für die Verschlüsselung kann er eine abgefangene Botschaft nicht ohne weiteres entschlüsseln. Ohne das Schlüsselbuch muss der gegnerische Analytiker wieder einmal alle möglichen Schlüssel prüfen, also alle 17576 möglichen Walzeneinstellungen. Der verzweifelte Kryptoanalytiker würde die erbeutete Enigma in eine bestimmte Walzenstellung

bringen, ein kurzes Stück des Geheimtextes eingeben und prüfen, ob der ausgegebene Text Sinn macht. Wenn nicht, würde er eine andere Walzeneinstellung wählen und es erneut probieren. Wenn er pro Minute eine Walzeneinstellung prüfen und Tag und Nacht arbeiten könnte, würde er insgesamt fast zwei Wochen brauchen. Das wäre ein annehmbares Mass an Sicherheit, doch wenn der Gegner ein Dutzend Leute an die Aufgabe setzte, könnte er alle Einstellungen an einem einzigen Tag prüfen.

Scherbius entschloss sich daher, die Sicherheit seines Verfahrens noch einmal zu verstärken, und erhöhte die Zahl der Anfangseinstellungen und damit die Zahl der möglichen Schlüssel.

Er hätte die Sicherheit durch zusätzliche Walzen steigern können, doch damit wäre die Maschine unhandlicher geworden. Er entschloss sich zu zwei Veränderungen. Die Walzen konnten ab jetzt herausgenommen und vertauscht werden. Diese sogenannte Walzenlage beeinflusst auf entscheidende Weise die Verschlüsselung. Es gibt sechs verschiedene Möglichkeiten, die drei Walzen anzuordnen, so dass diese Änderung die Zahl der Schlüssel oder die Zahl der möglichen Anfangsstellungen um den Faktor sechs erhöht.

Die zweite Änderung war der Einbau eines Steckerbretts zwischen der Tastatur und der ersten Walze. Das Steckerbrett ermöglicht es dem Chiffreur, über Kabel die Buchstaben miteinander zu vertauschen, bevor ihr Signal in die Walzen eintritt. Wenn man beispielsweise die Buchsen a und b auf dem Steckerbrett mit einem Kabel verbindet, geht bei Eingabe von b das elektrische Signal den Weg, den zuvor das Signal für den Buchstaben a gegangen ist und umgekehrt. Der Chiffreur an der Enigma hatte sechs Kabel, er konnte also sechs Buchstabenpaare vertauschen, die anderen vierzehn blieben ohne Kabelverbindung und daher unvertauscht. Die Buchstaben, die durch das Steckerbrett vertauscht werden, gehören mit zur Grundeinstellung der Maschine und müssen daher im Schlüsselbuch aufgeführt sein. Abbildung 5 zeigt den Plan der Maschine mit zusätzlichem Steckerbrett. Weil der Zeichnung nur ein sechsbuchstabiges Alphabet zugrunde liegt, sind hier nur zwei Buchstaben, a und b, vertauscht.

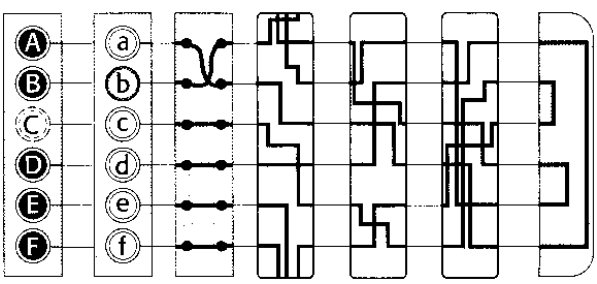


Abbildung 5

Wir haben jetzt die Hauptelemente von Scherbius' Enigma kennengelernt.

Wenn Sender und Empfänger sich auf den Schlüssel, d.h. die Steckerverbindungen am Steckerbrett, die Reihenfolge der Walzen und ihre jeweilige Einstellung geeinigt haben, können sie ohne weiteres Nachrichten verschlüsseln und wieder entschlüsseln. Ein gegnerischer Spion, der den Schlüssel nicht kennt, müsste jedoch jeden einzelnen der 10 000 000 000 000 000 möglichen Schlüssel überprüfen, um den Geheimtext zu knacken.

Scherbius erwarb 1918 sein erstes Patent. Seine Chiffriermaschine steckte in einer kleinen Kiste, die nur 34 x 28 x 15 Zentimeter mass, doch immerhin 12 Kilo wog. Abbildung 6 zeigt eine (geöffnete) Enigma in ihrer Kiste.

Abbildung 6

Zu erkennen ist die Tastatur, auf der die Klarbuchstaben eingegeben werden, und darüber die Lampentafel, die die entsprechenden Geheimbuchstaben anzeigt. Unter der Tastatur liegt das Steckerbrett. Zu hinterst erkennt man die drei Walzen.

Scherbius hielt seine Chiffriermaschine für unbezwingbar, und die deutsche Militärführung liess sich von Scherbius denn auch bald überzeugen, die Enigma anzuschaffen.

Scherbius begann 1925 mit der Serienfertigung der Maschine, und im Jahr darauf wurde sie in den militärischen Einsatz übernommen.

Während der nächsten zwanzig Jahre kaufte das Militär über 30 000 Enigmas. Scherbius' Erfindung verschaffte den Deutschen das sicherste Verschlüsselungssystem der Welt, und bei Ausbruch des Zweiten Weltkriegs war

der militärische Nachrichtenverkehr durch einen beispiellosen Grad der Verschlüsselung geschützt. Manchmal schien es so, als würde die Enigma ganz entscheidend zu einem Sieg der Nationalsozialisten beitragen, doch statt dessen spielte sie eine Rolle beim Ende des Hitlerregimes. Scherbius erlebte die Erfolge und Misserfolge seines Chiffriersystems nicht mehr. Im Jahr 1929 verlor er bei einem Ausritt die Kontrolle über seine Pferdekutsche und krachte gegen eine Mauer. Er starb am 13. Mai an seinen inneren Verletzungen.

Die Entschlüsselung der Enigma

Die Briten, die Amerikaner und auch die Franzosen versuchten die Enigma-Verschlüsselung in der Zeit nach dem Ersten Weltkrieg zu knacken, doch ihre Versuche scheiterten kläglich. Deutschland hatte jetzt das sicherste militärische Fernmeldesystem der Welt.

Nach dem Ersten Weltkrieg wurde Polen erneut ein souveräner Staat, doch die Polen sahen die neugewonnene Unabhängigkeit bald schon gefährdet. Im Osten lag die Sowjetunion, die darauf aus war, ihren Kommunismus zu verbreiten, und im Westen lag Deutschland, erpicht darauf, Gebiete, die es nach dem Krieg an Polen abtreten musste, wiederzugewinnen. Derart in die Zange genommen, waren die Polen dankbar für jede Information über die beiden Gegner und richteten deshalb einen neuen Dechiffrierdienst ein, das Biuro Szyfrów.

Verantwortlich für die Dechiffrierung des deutschen Funkverkehrs war Hauptmann Maximilian Ciezki. Aber Ciezki hatte keine militärische Version der Enigma zur Verfügung, und ohne die Verdrahtung des Militärgeräts zu kennen, hatte er keine Chance, die Meldungen des deutschen Heeres zu entschlüsseln. So blieb es einem von seinem Land enttäuschten Deutschen, Hans-Thilo Schmidt, vorbehalten, dem ersten Angriff auf die Enigma den Weg zu bereiten.

Hans-Thilo Schmidt wurde 1888 als zweiter Sohn eines angesehenen Professors und seiner adligen Frau geboren. Schmidt schlug eine Laufbahn im deutschen Heer ein und diente im Ersten Weltkrieg, doch nach den drastischen Kürzungen in der Folge des Versailler Vertrags hielt das Heer ihn für entbehrlich. Daraufhin versuchte er sein Glück als Geschäftsmann.

H.T. Schmidt

Nach dem Zusammenbruch seiner Firma sah sich HansThilo gezwungen, seinen Bruder um Hilfe zu bitten, und der besorgte ihm Arbeit in der Berliner Chiffrierstelle, dem für den verschlüsselten Nachrichtenverkehr verantwortlichen Dienst. Die Chiffrierstelle war die hochgeheime Schaltzentrale für die Enigma, in der streng geheime Informationen über die Tische gingen. Als Schmidt die neue Arbeit antrat, liess er seine Familie in Bayern zurück, wo die Lebenshaltungskosten noch erträglich waren. Er lebte allein im teuren Berlin, verarmt und ohne Freunde. Die Folge war unvermeidlich. Schmidt verdiente sich Geld, indem er geheime Informationen zur Enigma an fremde Mächte verkaufte, und damit konnte er zugleich Rache üben, die Sicherheit seines Landes untergraben.

Im November 1931 liess er gegen Bezahlung einen französischen Agenten zwei Dokumente fotografieren: die "Gebrauchsanweisung für die Chiffriermaschine Enigma" und die "Schlüsselanleitung für die Chiffriermaschine Enigma". Diese Unterlagen enthielten zwar keine genaue Beschreibung der Walzenverdrahtung, doch sie enthielten die nötigen Informationen, um sie zu erschliessen.

Dank Schmidts Verrat war es den Alliierten jetzt möglich, ein genaues Duplikat der deutschen Enigma zu bauen. Allerdings reichte dies nicht aus, um die mit der Enigma chiffrierten Meldungen zu entschlüsseln. Die Stärke der Verschlüsselung hängt nicht davon ab, ob die Maschine selbst geheim bleibt, sondern von der Geheimhaltung ihrer jeweiligen Grundstellung (d.h. des Schlüssels). Will ein Kryptoanalytiker eine abgefangene Nachricht entschlüsseln, dann muss er nicht nur ein Duplikat der Enigma besitzen, er muss auch herausfinden, welcher der unzähligen möglichen Schlüssel benutzt wurde, um die jeweilige Nachricht zu verschlüsseln.

Die französischen Kryptoanalytiker waren offenbar weder willens noch fähig, diese brandheissen Informationen auszuwerten. Nun fügte es sich, dass die Franzosen zehn Jahre zuvor ein militärisches Kooperationsabkommen mit den Polen unterzeichnet hatten. Die Polen hatten ihr Interesse an allem bekundet, was mit der Enigma zu tun hatte, und so händigten die Franzosen ihre Fotos von Schmidts Dokumenten ihren Verbündeten aus und überliessen dem Biuro Szyfrów die hoffnungslose Aufgabe, die Enigma zu knacken. Die Unterlagen waren nur eine Starthilfe, das wussten die Polen, doch im Gegensatz zu den Franzosen fürchteten sie eine Invasion und hatten damit Grund genug, am Ball zu bleiben. Die Polen verbissen sich in den Gedanken, es müsse eine Abkürzung geben, um den Schlüssel für eine Enigma-

chiffrierte Botschaft zu finden, und man müsse nur genug Mühe, Erfindungsgabe und Scharfsinn investieren, um diesen Weg zu finden.

Schmidts Dokumente enthüllten nicht nur die innere Verdrahtung der Walzen, auch die von den Deutschen benutzten Schlüsselbücher waren genau beschrieben. Jeden Monat erhielten die Enigma-Operatoren ein neues Schlüsselbuch, das für jeden Tag einen Schlüssel (Steckerverbindungen, Walzenlage und Grundstellung der Walzen) vorschrieb.

Eine Möglichkeit bestand nun darin, den gesamten Funkverkehr eines bestimmten Tages mit dem Tagesschlüssel zu chiffrieren. Dann stellten alle Enigma-Chiffreure einen ganzen Tag lang zu Beginn jeder Meldung ihre Maschinen auf den jeweiligen Tagesschlüssel ein. Jeder Funkspruch wurde zunächst in die Maschine getippt; der verschlüsselte Text wurde aufgezeichnet und dem Funker zum Senden übergeben.

Auf der Empfängerseite ging die Meldung zunächst beim Funker ein, der sie dem Bediener der Enigma übergab. Dieser wiederum tippte sie in seine Maschine, die er bereits auf den einheitlichen Tagesschlüssel eingestellt hatte. Die aufleuchtenden Buchstaben auf dem Lampenfeld ergaben dann den Klartext der Meldung.

Die Schwäche dieses Verfahrens besteht jedoch darin, dass der Tagesschlüssel immer wieder benutzt wird, um die vielleicht Hunderte von Meldungen zu senden, die täglich anfallen. Wird ein einziger Schlüssel benutzt, um eine enorme Menge von Nachrichten zu verschlüsseln, dann ist es für den Kryptoanalytiker im allgemeinen leichter, sie zu entschlüsseln. Eine grosse Menge Text, auf die gleiche Weise verschlüsselt, gewährt dem Kryptoanalytiker eine grössere Chance, den Schlüssel ausfindig zu machen.

Als zusätzliche Vorsichtsmassnahme gingen die Deutschen deshalb zu dem Verfahren über, den Tagesschlüssel einzusetzen, um für jede Meldung einen neuen Spruchschlüssel festzulegen. Bei diesem Verfahren werden die einzelnen Funksprüche zwar mit den im Tagesschlüssel festgelegten Steckerverbindungen und Walzenlagen chiffriert, doch mit anderen, selbstgewählten Walzenstellungen. Da die neuen Walzenstellungen nicht im Schlüsselbuch enthalten sind, müssen sie ebenfalls auf sichere Weise übermittelt werden. Dazu wird die Maschine zunächst auf den einheitlichen Tagesschlüssel eingestellt, der auch eine bestimmte Grundstellung der Walzen festlegt, beispielsweise QCW. Als nächstes wählt der Chiffreur aus freien Stücken eine neue Walzenstellung für den Spruchschlüssel, etwa PGH. Dann verschlüsselt er die Buchstabenfolge PGH mit dem Tagesschlüssel. Der Spruchschlüssel wird, um sicherzugehen, gleich zweimal in die Enigma getippt. Dann werden die Walzen auf PGH eingestellt, und die eigentliche Meldung wird mit dem Spruchschlüssel chiffriert.

Auch auf Empfängerseite ist die Maschine zunächst auf den Tagesschlüssel QCW eingestellt. Die ersten sechs Buchstaben der eingehenden Meldung werden eingetippt und ergeben pghpgh. So weiss der Empfänger, dass er seine Walzen auf den Spruchschlüssel PGH einstellen muss, und kann die eigentliche Meldung entschlüsseln.

Sender und Empfänger benutzen also denselben Hauptschlüssel, doch dann verwenden sie ihn nicht, um alle Meldungen zu verschlüsseln, sondern nur, um für jede Einzelmeldung einen neuen Schlüssel zu chiffrieren und dann die eigentliche Botschaft mit diesem neuen Schlüssel zu senden.

Auf den ersten Blick schien das System undurchdringlich, doch die polnischen Kryptoanalytiker liessen sich nicht entmutigen. Sie waren bereit, jede Möglichkeit auszuloten, um eine Schwäche in der Enigma und dem System der Tages- und Spruchschlüssel zu finden. Das Biuro Szyfrów organisierte einen Kryptographie-Lehrgang und lud dazu zwanzig Mathematiker ein. Drei von den zwanzig Kandidaten zeigten besonderes Talent für die Entschlüsselung von Geheimtexten, und das Biuro stellte sie ein. Der begabteste von ihnen war Marian Rejewski, ein schüchterner, bebrillter junger Mann von dreiundzwanzig Jahren, der Statistik studiert hatte und eigentlich in die Versicherungswirtschaft gehen wollte.

M. Rejewski

Rejewskis Angriffsstrategie gegen die Enigma stützte sich hauptsächlich auf die Tatsache, dass die Wiederholung der Feind der Geheimhaltung ist: Wieder-holungen ergeben bestimm-te Muster, und das sind die Lieblingskinder der Kryptoanalytiker. Die augenfälligsten Wiederholungen bei den Enigma-Sendungen waren die Spruchschlüssel, die zu Beginn jeder Meldung gesendet wurden. Die Deutschen schrieben diese Wiederholung vor, um Irrtümer durch Interferenzen oder Bedienungsfehler zu vermeiden. Dass sie damit die Sicherheit der Verschlüsselung gefährdeten, sahen sie nicht voraus.

Rejewski bekam täglich einen neuen Stapel abgehörter Meldungen auf den Schreibtisch. Sie alle begannen mit den sechs Buchstaben

des wiederholten dreibuchstabigen Spruchschlüssels, alle nach dem vereinbarten Tagesschlüssel chiffriert. So erhielt er beispielsweise vier Funksprüche, die mit den folgenden chiffrierten Spruchschlüsseln begannen:

1. Funkspruch	L	0	K	R	G	M
2. Funkspruch	M	V	T	X	Z	E
3. Funkspruch	J	K	T	M	P	E
4. Funkspruch	D	V	Y	P	Z	X

Die ersten und die vierten Buchstaben, soviel steht fest, sind Verschlüsselungen desselben Klarbuchstabens, nämlich des ersten Buchstabens des Spruchschlüssels. Auch die zweiten und fünften Buchstaben sind Verschlüsselungen desselben Buchstabens, nämlich des zweiten Buchstabens des Spruchschlüssels, und die dritten und sechsten Buchstaben sind Verschlüsselungen des dritten Buchstabens des Spruchschlüssels. Im ersten Funkspruch sind also L und R Verschlüsselungen desselben, nämlich des ersten Buchstabens des Spruchschlüssels. Der Grund, warum dieser Buchstabe unterschiedlich verschlüsselt wird, erst als L und dann als R, ist einfach der, dass sich die erste Walze inzwischen drei Schritte weitergedreht und damit den Verschlüsselungsweg verändert hat.

Der Tatsache, dass L und R Verschlüsselungen desselben Buchstabens sind, verdankte Rejewski einen winzigen Hinweis auf die ursprüngliche Einstellung der Maschine. Diese Grundstellung, die er nicht kannte, verschlüsselte den ersten Buchstaben des Spruchschlüssels, den er ebenfalls nicht kannte, mit L, und eine spätere Walzenstellung, ebenfalls unbekannt, aber drei Schritte von der Grundstellung entfernt, verschlüsselte denselben Buchstaben mit R.

Dieser Hinweis mag vage erscheinen, da noch zu viele Unbekannte eine Rolle spielen. Mit jeder neuen abgehörten Meldung aber können weitere Beziehungen zwischen den ersten und den vierten Buchstaben des wiederholten Spruchschlüssels aufgespürt werden. In all diesen Beziehungen spiegelt sich die Grundstellung der Enigma.

Rejewski stellte diese Beziehungen in einer Tabelle zusammen. Für die bisherigen vier Funksprüche spiegelt die Tabelle die Beziehungen zwischen (L,R), (M,X), (J,M) und (D,P) wider.

Wenn der Abhördienst Rejewski an einem Tag genug Funksprüche lieferte, konnte er das Alphabet dieser Beziehungen vervollständigen. Die folgende Tabelle zeigt ein solches vollständiges Beziehungsmuster:

erster Buchstabe
ABCDEFGHIJKLMNOPQRSTUVWXYZ
FQHPLWOGBMVRXUYCZITNJEASDK
vierter Buchstabe

Rejewski kannte den Tagesschlüssel nicht und hatte auch keine Ahnung, welche Spruchschlüssel gewählt worden waren, doch er wusste, dass sie, mit dem Tagesschlüssel chiffriert, diese Beziehungstabelle ergaben.

Wäre der Tagesschlüssel anders gewesen, dann hätte auch die Tabelle völlig anders ausgesehen. Die nächste Frage lautete, ob es anhand dieser Tabelle eine Möglichkeit gab, den Tagesschlüssel herauszufinden. Rejewski begann nach Mustern in der Tabelle zu suchen, Strukturen, die vielleicht auf den Tagesschlüssel hindeuteten. Schliesslich begann er ein bestimmtes Muster zu untersuchen, das sich aus Buchstabenketten ergab. In der obigen Tabelle beispielsweise ist das A in der oberen Zeile mit dem F in der unteren Zeile verknüpft, und Rejewski suchte nun wiederum das F in der oberen Zeile. Er stellte fest, dass F mit W verknüpft war, und suchte daraufhin das W in der oberen Zeile. Und dieses W schliesslich war wiederum mit dem A verknüpft, bei dem er angefangen hatte. Die Kette war geschlossen. Rejewski suchte auch bei den anderen Buchstaben im Alphabet nach diesen Verknüpfungen und konnte verschiedene Ketten zusammenstellen. Er listete sie auf und notierte die Zahl der Verknüpfungen in jeder Kette:

3 Verknüpfungen A->F->W->A
9 Verknüpfungen B->Q->Z->K->V->E->L->R->I->B
7 Verknüpfungen C->H->G->O->Y->D->P->C
7 Verknüpfungen J->M->X->S->T->N->U->J

Bislang haben wir nur die Beziehungen zwischen den ersten und vierten Buchstaben des sechsbuchstabigen, wiederholten Schlüssels betrachtet. Rejewski wandte sein Verfahren auch auf die Beziehungen zwischen den zweiten und fünften sowie den dritten und sechsten Buchstaben an und listete alle Ketten und die Zahl ihrer Verknüpfungen auf. Er stellte fest, dass sich die Ketten jeden Tag änderten. Mal ergaben sich viele kurze Ketten, ein andermal nur ein paar lange. Und natürlich änderten sich die Buchstaben in den Ketten. Die Eigenschaften der Ketten waren offenbar eine Folge des jeweiligen Tagesschlüssels.

An diesem Punkt gelangte Rejewski zu einer bemerkenswerten Einsicht. Zwar wirken sich Steckerbrett und Walzenkonfiguration gemeinsam auf die genaue Zusammensetzung der Ketten aus, doch ihre Beiträge lassen sich in gewissem Masse auseinanderdröseln. Insbesondere eine Eigenschaft der Ketten hängt ausschliesslich von Lage und Einstel-

lung der Walzen ab und hat mit den Steckerbrettverbindungen nichts zu tun: die Zahl der Verknüpfungen innerhalb der Ketten.

Durch das Anbringen der Steckerverbindungen verändern sich Ein paar Buchstaben in den Ketten, doch die Zahl der Verknüpfungen jeder Kette bleibt unverändert. Rejewski hatte eine Eigenschaft der Ketten entdeckt, in der sich allein die Walzenkonfiguration widerspiegelte.

Welche der 105'456 möglichen Walzenkonfigurationen steckte hinter der Zahl der Verknüpfungen innerhalb einer bestimmten Gruppe von Ketten? Diese Zahl ist immer noch gross, allerdings etwa hundert Milliarden mal kleiner als die Gesamtzahl der möglichen Tagesschlüssel. Kurz, die Aufgabe ist hundert Milliarden mal leichter geworden und damit in den Bereich menschlicher Möglichkeiten gerückt.

Rejewski ging wie folgt vor. Dem Spion Hans-Thilo Schmidt hatte er zu verdanken, dass er mit identischen Nachbauten von Enigma-Maschinen arbeiten konnte. Seine Leute setzten sich an die mühselige Aufgabe, jede einzelne der 105'456 Walzenkonfigurationen durchzuprüfen und die sich jeweils ergebenden Kettenlängen zu erfassen. Sie brauchten ein ganzes Jahr, um den Katalog zu erstellen, doch sobald das Biuro die Daten zusammengestellt hatte, konnte Rejewski endlich damit beginnen, die Enigma-Verschlüsselung zu brechen.

Jeden Tag sah er sich die chiffrierten Spruchschlüssel an, d.h. die ersten sechs Buchstaben aller abgehörten Nachrichten, und erstellte seine Beziehungstabellen. Hatte er diese zur Hand, konnte er die Buchstaben zu Ketten verbinden und für jede Kette die Zahl der Verknüpfungen feststellen. Beispielsweise ergab die Analyse der ersten und vierten Buchstaben vier Ketten mit 3, 9, 7 und 7 Verknüpfungen. Die zweiten und fünften Buchstaben ergaben vier Ketten mit 2, 3, 9 und 12 Verknüpfungen. Die dritten und sechsten Buchstaben schliesslich erbrachten 5 Ketten mit 5, 5, 5, 3 und 8 Verknüpfungen. Den Tagesschlüssel kannte Rejewski zwar immer noch nicht, doch er wusste, dass dieser Tagesschlüssel diese drei Gruppen von Ketten ergab.

Jetzt konnte Rejewski seinen Katalog zu Rate ziehen, der jede Walzenkonfiguration enthielt, geordnet nach den Merkmalen der jeweils sich ergebenden Ketten. Sobald er den Katalogeintrag mit der richtigen Kettenzahl und der richtigen Verknüpfungszahl gefunden hatte, kannte er die Walzenkonfiguration, die der jeweilige Tagesschlüssel vorsah. Die Ketten waren gleichsam Fingerabdrücke, die auf die Spur der Walzenkonfiguration führten.

Zwar hatte Rejewski jetzt den Walzenteil des Tagesschlüssels gefunden, doch die Steckerbrettverbindungen kannte er immer noch nicht. Obwohl es etwa hundert Milliarden Möglichkeiten für diese Verbindungen gibt, war dies eine verhältnismässig einfache Aufgabe. Rejewski stellte zunächst die Walzen seiner Enigma gemäss dem soeben ausfindig gemachten Walzenteil des Tagesschlüssels ein. Dann entfernte er alle Kabel am Steckerbrett, das deshalb keine Auswirkung auf die Verschlüsselung hatte.

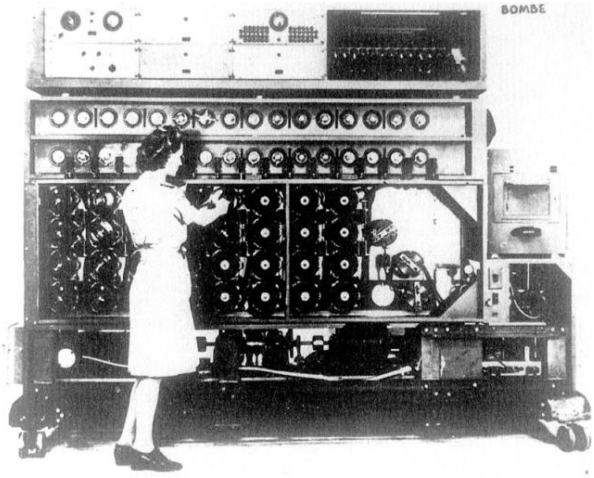
Das ergab weitgehend Unsinn, denn die Steckerbrettverkabelung fehlte und war auch nicht bekannt. Schliesslich nahm er einen abgehörten Geheimtext und tippte ihn in die Enigma. Allerdings tauchten doch hin und wieder einigermassen erkennbare Wortgebilde auf, etwa `alkulftilbernil` - vermutlich sollte dies `Ankunft in Berlin` lauten. Wenn diese Annahme zutraf, dann mussten die Buchstaben `R` und `L` miteinander verbunden, das heisst durch ein Kabel am Steckerbrett vertauscht sein, `A, K, U, F, T, I, B` und `E` dagegen nicht.

Durch die Analyse weiterer Buchstabenfolgen war es dann möglich, die anderen Buchstabenpaare, die am Steckerbrett vertauscht waren, ausfindig zu machen. Rejewski hatte nun die Verbindungen am Steckerbrett mitsamt der Walzenkonfiguration, also den vollständigen Tagesschlüssel in der Hand. Damit konnte er jede Meldung des Tages entschlüsseln.

Mit Rejewskis bahnbrechendem Erfolg war der deutsche Funkverkehr zu einem offenen Geheimnis geworden. Die Polen waren nicht im Krieg mit den Deutschen, sahen sich jedoch von einer Invasion bedroht und waren daher ausgesprochen erleichtert, die Enigma geknackt zu haben. Die Polen setzten Rejewskis Technik mehrere Jahre lang erfolgreich ein.

Selbst als die Deutschen ihr Verfahren der Nachrichtenübermittlung leicht modifizierten, konnte Rejewski zurückschlagen. Sein alter Katalog der Kettenlängen war jetzt nutzlos geworden, doch er schrieb ihn nicht um, sondern entwickelte eine mechanische Version des Katalogsystems, das automatisch nach den richtigen Walzenkonfigurationen suchte. Rejewskis Erfindung funktionierte ähnlich wie die Enigma selbst und konnte sehr schnell jede der 17'576 Walzenkonfigurationen durchprüfen, bis sie eine Übereinstimmung registrierte. Wegen der sechs möglichen Walzenlagen musste man sechs von Rejewskis Maschinen parallel arbeiten lassen, jede mit einer der möglichen Walzenlagen. Die ge-

samte Anlage konnte den Tagesschlüssel in etwa zwei Stunden finden. Sie wurde als Bombe bezeichnet.



Bombe

Die Bomben mechanisierten jedenfalls von Grund auf den Prozess der Entzifferung und waren die unvermeidliche Antwort auf die Mechanisierung der Verschlüsselung durch die Enigma.

Als die deutschen Kryptographen im Dezember 1938 die Enigma-Verschlüsselung eine Stufe komplizierter machten, war Rejewski mit seinem Latein am Ende. An alle Chiffreure wurden zwei neue Walzen ausgegeben, so dass die Walzenlage sich aus drei von fünf möglichen Walzen zusammensetzte. Zuvor hatte man nur drei Walzen eingesetzt (mit den Nummern 1, 2 und 3) und nur sechs Möglichkeiten gehabt, sie anzuordnen, doch nun gab es zwei weitere Walzen (mit den Nummern 4 und 5), und die Zahl der möglichen Walzenlagen stieg auf 60. Die erste Herausforderung für Rejewski bestand darin, die innere Verdrahtung der beiden neuen Walzen zu erschliessen. Mehr Sorgen bereitete ihm allerdings, dass er zehnmal so viele Bomben bauen musste, um jeden Walzenstand darzustellen. Die blossen Kosten für den Bau einer solchen Batterie von Bomben betrugen das Fünfzehnfache des gesamten Materialbudgets des Biuro. Im Monat darauf verschlimmerte sich die Lage, denn die Zahl der Steckerkabel stieg von sechs auf zehn. Nicht mehr zwölf Buchstaben wurden vertauscht, bevor die Signale in die Walzen eintraten, sondern zwanzig. Die Zahl der möglichen Schlüssel stieg auf 159 000 000 000 000 000 000.

Der polnische Abhör- und Entschlüsselungsdienst war 1938 auf dem Gipfel seiner Leistungsfähigkeit, doch Anfang 1939, als die neuen Walzen und die zusätzlichen Steckerkabel eingesetzt wurden, war die Ausbeute an Informationen schon dünner. Rejewski, der die Grenzen der Kryptoanalyse in den Jahren zuvor ständig erweitert hatte, war ratlos. Er hatte bewiesen, dass die Enigma-Verschlüsselung nicht unlösbar war, doch ohne die erforderlichen technischen Mittel, um jede Walzenkonfiguratioin prüfen zu können, war der Tagesschlüssel nicht zu finden und die Entschlüsselung unmöglich.

Die neuerliche Undurchdringlichkeit der Enigma war ein verheerender Schlag für Polen, denn die Enigma war nicht nur ein Mittel der Kommunikation, sie war das Herz von Hitlers Blitzkrieg. Blitzkrieg bedeutete gut abgestimmte, schnelle und schwere Angriffe mit grossen gepanzerten Verbänden, die mit der Infanterie und der Artillerie in ständiger Verbindung standen. Zudem wurden die Bodentruppen von Sturzkampfbombern unterstützt, die sich auf schnelle und sichere Nachrichtenverbindungen zwischen den Truppen an der Front und den Flugplätzen verlassen mussten. Der Grundgedanke des Blitz krieges lautete "schneller Angriff, schnelle Abstimmung der Kräfte".

Wenn die Polen die Enigma nicht knacken konnten, hatten sie keine Chance, den deutschen Überfall zu stoppen, der offenbar nur noch wenige Monate auf sich warten liess. Deutschland hatte bereits das Sudetenland besetzt, und am 27. April 1939 kündigte es den Nichtangriffspakt mit Polen.

Am 30. Juni 1939 lud Major Langer (Rejewskis Chef) seine französischen und britischen Kollegen telegrafisch nach Warschau ein, um einige dringliche Fragen im Umkreis der Enigma zu erörtern. Am 24. Juli betraten ranghohe französische und britische Kryptoanalytiker, unsicher, was sie erwarten würde, das Hauptquartier des Biuro. Langer führte sie in einen Raum, in dem ein mit schwarzem Tuch verhüllter Apparat stand. Mit theatralischer Geste zog er das Tuch weg und enthüllte eine von Rejewskis Bomben. Rejewski habe die Enigma schon vor Jahren geknackt, durfte das verdutzte Publikum erfahren. Die Polen waren allen andern auf der Welt um ein Jahrzehnt voraus. Besonders verblüfft waren die Franzosen, denn die polnische Arbeit beruhte auf den Erfolgen der französischen Spionage. Sie hatten die von Schmidt abgekauften Informationen an die Polen weitergegeben, in dem Glauben, sie seien wertlos, doch jetzt belehrten die Polen sie eines Besseren.

Als letzte Überraschung bot Langer den Engländern und Franzosen zwei entbehrliche Nachbauten der Enigma und die Baupläne der Bomben an, die daraufhin im Diplomatengepäck nach Paris gebracht wurden. Von dort ging eine der Enigmas am 16. August auf die Weiterreise nach London. Zwei Wochen später, am 1. September 1939, fielen Hitlers Ar-

meen in Polen ein – der Zweite Weltkrieg hatte begonnen.

Die Polen hatten bewiesen, dass die Enigma keine perfekte Verschlüsselung lieferte, und den Alliierten zudem gezeigt, wie wichtig es war, Mathematiker als Codebrecher zu beschäftigen. Bei den Engländern hatten die Linguisten und Altphilologen immer die erste Geige gespielt, doch nun bemühte man sich gemeinsam, auch Mathematiker und Naturwissenschaftler zu rekrutieren.

Die Neuen fuhren nach Bletchley Park in Buckinghamshire. Diese neugebildete Organisation war nun für die Dechiffrierung zuständig.

Bletchley Park

In der Mitte von Bletchley Park stand ein altes viktorianisches Herrenhaus im Stil der Tudor-Gotik, erbaut im 19. Jahrhundert. Das Haus mit seiner Bibliothek, dem Speisesaal und dem prachtvollen Ballsaal war die Herzkammer der gesamten Operation Bletchley. Doch die Aussicht wurde bald durch den Bau zahlreicher Baracken verdorben. Diese auf die Schnelle errichteten Holzgebäude beherbergten die verschiedenen Dechiffrier-Abteilungen. Anfangs arbeiteten nur 200 Menschen in Bletchley Park, doch fünf Jahre später beherbergten das Herrenhaus und die Baracken 7'000 Männer und Frauen.

Im Herbst 1939 studierten die Wissenschaftler und Mathematiker in Bletchley die komplizierte Wirkungsweise der Enigma und machten sich polnischen Techniken rasch zu eigen. Bletchley hatte mehr Personal und Mittel als das polnische Biuro Szyfrów und konnte daher auch mit der grösseren Walzenzahl zurechtkommen, die bedeutete, dass die Enigma jetzt zehnmal schwerer zu knacken war. Alle 24 Stunden arbeiteten die britischen Codebrecher dieselbe Routine ab. Um Mitternacht gingen die deutschen Enigma-Chiffreure zu einem neuen Tagesschlüssel über, und damit war alles, was Bletchley am Tag zuvor erarbeitet hatte, für die Entschlüsselung wertlos geworden.

Die Codebrecher mussten sich nun von neuem auf die Suche nach dem Tagesschlüssel machen. Das konnte mehrere Stunden dauern, doch sobald die Enigma-Einstellungen des jeweiligen Tages entdeckt waren, konnte man in Bletchley auch die deutschen Funkmeldungen entziffern, die sich bereits angesammelt hatten, und damit Informationen gewinnen, die für die Kriegführung von unschätzbarem Wert waren.

Das Überraschungsmoment ist für jeden Befehlshaber eine entscheidende Waffe. Wenn Bletchley Park die Enigma brechen konnte, waren die Vorhaben der Deutschen kein Geheimnis mehr, und die englische Seite konnte die Gedanken der deutschen Militärführung lesen. Wenn die Briten von einem unmittelbar drohenden Angriff erfuhren, konnten sie entweder Verstärkung schicken oder ein Ausweichmanöver veranlassen. Wenn die Alliierten verfolgen konnten, wie auf deutscher Seite über die eigenen Schwachpunkte gestritten wurde, dann konnten sie ihre Angriffe genau darauf ausrichten. Die Entschlüsselungen in Bletchley Park waren von höchstem Wert. Als die Deutschen im April 1940 in Dänemark und Norwegen einfielen, lieferte Bletchley ein detailliertes Bild der deutschen Operationen. Auch bei der Luftschlacht um England konnten die Kryptoanalytiker im Voraus vor Bombenangriffen warnen und sogar Zeiten und Ziele angeben.

Sobald die Kryptoanalytiker in Bletchley die polnischen Techniken beherrschten, machten sie sich auf die Suche nach eigenen Abkürzungen zu den Enigma-Schlüsseln. Zum Beispiel nutzten sie den Umstand, dass die deutschen Enigma Chiffreure hin und wieder simple Spruchschlüssel wählten. Der Chiffreur sollte für jede Meldung einen neuen Spruchschlüssel verwenden, drei willkürlich ausgewählte Buchstaben. Die überarbeiteten Männer strengten in der Hitze des Gefechts jedoch nicht immer ihre Phantasie an, sondern nahmen einfach drei nebeneinanderliegende Buchstaben von der Tastatur der Enigma, etwa `QWE` oder `BNM`. Diese voraussagbaren Spruchschlüssel taufte man in Bletchley cillies. Als cilly galt auch die wiederholte Verwendung desselben Spruchschlüssels, vielleicht der Initialen der Freundin des Chiffreurs. Bevor man die Enigma auf die harte Tour knackte, versuchten es die Kryptoanalytiker routinemässig mit den cillies, und ihre Eingebungen zahlten sich manchmal aus.

Da die Enigma-Maschine während des Krieges ständig verändert wurde, waren die Kryptoanalytiker andauernd gezwungen, sich etwas Neues einfallen zu lassen, ihre Bomben umzubauen und zu verfeinern und ganz neue Strategien zu entwickeln. Nicht zuletzt beruhte der Erfolg auf der eigentümlichen Melange

aus Mathematikern, Naturwissenschaftlern, Linguisten, Philologen, Schachgrossmeistern und Kreuzworträtselsüchtigen, die in den Baracken arbeiteten.

Ein vertracktes Problem ging von Hand zu Hand, bis es an jemanden geriet, der die richtigen geistigen Werkzeuge dafür besass. Wenn es dennoch eine Persönlichkeit verdient, besonders hervorgehoben zu werden, dann ist es der Mathematiker Alan Turing, der die grösste Schwäche der Enigma aufspürte und sie auf raffinierte Weise ausnutzte. Dank Turing wurde es möglich, die Enigma-Verschlüsselung auch unter den schwierigsten Umständen zu knacken.

Nach Kriegsausbruch verliess Turing seine Stelle an der Universität Cambridge und schloss sich den Codebrechern in Bletchley Park an. Viel Zeit verbrachte er im ehemaligen Obstlager von Sir Leon, wo nun der Think-tank, die Denkzentrale von Bletchley untergebracht war. Dort sassen die Kryptoanalytiker zusammen, redeten sich die Köpfe über die anstehenden Fragen heiss und überlegten vorsorglich, wie mit möglichen künftigen Schwierigkeiten umzugehen wäre.

Turing beschäftig-te vor allem die Frage, was ge-schehen würde, wenn das deutsche Militär sein System der Spruchverschlüs-selung ändern würde. Die An-fangserfolge in Bletchley beruhten auf Rejewskis Arbeit, der die Tatsache ausgenutzt hatte, dass die Enigma-Chiffreure jeden Spruchschlüssel zweimal chiffrierten. Diese Wiederholung sollte die Empfänger vor Fehlern schützen, doch zugleich war sie das Einfallstor für die Entschlüssler der Enigma. Die britischen Experten vermuteten, dass es nicht mehr lange dauern würde, bis die Deutschen bemerkten, dass die Wiederholung des Schlüssels die Sicherheit der Enigma gefährdete. Daraufhin würden die Chiffreure den Befehl erhalten, den Schlüssel nur noch einmal zu senden, und die bisherigen Entschlüsselungsverfahren von Bletchley wären wirkungslos gemacht. Turings Aufgabe war es nun, eine andere Angriffslinie gegen die Enigma aufzubauen, bei der man sich nicht auf die Wiederholung des Spruchschlüssels verlassen musste.

Im Laufe einiger Wochen sammelte sich in Bletchley eine gewaltige Bibliothek entschlüsselter Funksprüche an. Turing fiel auf, dass viele von ihnen eine strenge Ordnung aufwiesen. Er sah sich die alten dechiffrierten Meldungen näher an und stellte fest, dass er den Inhalt einiger unentschlüsselter Meldungen wenigstens zum Teil voraussagen konnte, vorausgesetzt, er wusste, wann sie gesendet worden waren und aus welcher Quelle sie stammten. Erfahrungsgemäss sendeten die Deutschen jeden Tag kurz nach sechs Uhr morgens einen verschlüsselten Wetterbericht. Eine verschlüsselte Meldung, die fünf Minuten nach sechs abgehört wurde, musste also fast sicher das Wort `wetter` enthalten. Die strengen Vorschriften, wie sie in allen militärischen Organisationen üblich sind, bedeuteten in diesem Fall, dass die Meldungen sprachlich stark geregelt waren, so dass Turing mit einiger Sicherheit die Position von `wetter` in dem verschlüsselten Bericht ausfindig machen konnte. Beispielsweise wusste er aus Erfahrung, dass die ersten sechs Buchstaben eines bestimmten Kryptogramms dem Klarwort `wetter` entsprachen. Wenn auf diese Weise ein Stück Klartext mit einem Stück Geheimtext verknüpft werden kann, ergibt sich ein sogenannter Crib, ein Anhaltspunkt.

Alan Turing

Turing konnte beweisen, dass der Crib eindeutige Rückschlüsse auf die Voreinstellung der Maschine erlaubte, mit der die Nachricht verschlüsselt worden war. Dies bedeutete, dass es tatsächlich möglich war, sich zum Spruchschlüssel und dann auch zum Tagesschlüssel voranzutasten, mit dessen Hilfe wiederum andere Meldungen vom selben Tag entschlüsselt werden konnten. Gleichwohl mussten immer noch Tausende Walzeneinstellungen der Enigma überprüft werden, um herauszufinden, welche die jeweiligen Forderungen erfüllte. Deshalb entwickelte Turing eine Maschine für diese Aufgabe, die ebenfalls als "Bombe" bezeichnet wurde, nach der polnischen Codebrechermaschine, der Bletchley Park seine erfolgreiche erste Attacke gegen die Enigma-Verschlüsselung verdankte.

Während Turing auf die Lieferung der ersten Bombe wartete, setzte er seine tägliche Arbeit in Bletchley fort. Die Kunde von seinem Erfolg verbreitete sich rasch unter den anderen führenden Kryptoanalytikern, die nun seine einzigartige Begabung als Codeknacker erkannten.

Alles, was in Bletchley Park vor sich ging, war natürlich top secret, und daher wusste kein Aussenstehender von Turings bemerkenswerten Leistungen. Beispielsweise ahnten seine Eltern nicht einmal, dass er als Codebrecher arbeitete.

Bis Ende 1941 waren fünfzehn Bomben in Betrieb, die Cribs ausnutzten, Walzenstellungen prüften und Schlüssel enthüllten, und jede Bombe klapperte wie eine Million Stricknadeln. Wenn alles gutging, fand eine Bombe innerhalb einer Stunde den Enigma-Schlüssel.

Sobald die Steckverbindungen und die Walzenkonfiguration (der Spruchschlüssel) feststanden, war es einfach, den Tagesschlüssel zu erschliessen. Alle anderen Meldungen dieses Tages konnten dann rasch dechiffriert werden.

Obwohl die Bomben einen entscheidenden Durchbruch der Kryptoanalyse markierten, war die Entschlüsselung noch keineswegs blosse Routine. Viele Hürden waren zu nehmen, bis die Bomben auch nur auf die Suche nach dem Schlüssel gehen konnten. Zum Beispiel brauchte man zuerst einen Crib. Die erfahrenen Codebrecher überreichten ihre Cribs den Fachleuten an den Bomben, doch es gab keine Garantie, dass die Codebrecher die richtige Bedeutung des Geheimtextes erraten hatten. Und selbst wenn sie den richtigen Crib hatten, lag er vielleicht an der falschen Stelle - die Kryptoanalytiker mochten wohl erraten haben, dass eine verschlüsselte Botschaft eine bestimmte Wortfolge enthielt, doch vielleicht hatten sie diese Folge über den falschen Abschnitt des Geheimtextes gelegt. Immerhin gab es einen guten Trick, um zu prüfen, ob der Crib in der richtigen Position war.

Ein Merkmal der Enigma war, dass sie wegen des Reflektors nicht in der Lage war, einen Buchstaben mit sich selbst zu verschlüsseln. Der Buchstabe a konnte nie als A verschlüsselt werden, b nie als B und so weiter. Um die korrekte Verknüpfung für den Crib zu finden, verschieben wir einfach Klartext und Geheimtext gegeneinander, bis kein Buchstabe mit sich selbst gepaart ist.

Die Informationen über das gegnerische Militär, die man nach dem Bruch der Enigma-Verschlüsselung sammeln konnte, gehörten zu einer umfassenderen Aufklärungsoperation mit dem Codenamen Ultra. Die Ultra-Akten, die auch entschlüsselte Meldungen der Italiener und Japaner enthielten, verliehen den Alliierten auf allen wichtigen Kriegsschauplätzen klare Vorteile. In Nordafrika trug Ultra dazu bei, die deutschen Nachschublinien zu zerstören und die Alliierten über den Kräftestand von Rommels Truppen aufzuklären, was es der britischen achten Armee ermöglichte, deren Angriffe abzuwehren. Ultra warnte auch vor der deutschen Invasion Griechenlands und erlaubte den britischen Truppen den Rückzug ohne schwere Verluste. Tatsächlich lieferte Ultra genaue Berichte über die Feindlage im gesamten Mittelmeerraum. Diese Informationen waren besonders wertvoll bei der Landung der Alliierten 1943 in Sizilien und auf dem italienischen Festland. Auch 1944, während der alliierten Invasion in Frankreich, spielte Ultra eine entscheidende Rolle. Beispielsweise ergab das entschlüsselte Material aus Bletchley in den Monaten vor D-Day ein genaues Bild der deutschen Truppenkonzentrationen entlang der französischen Küste.

Entscheidend war, dass die Informationen auf eine Weise genutzt wurden, die bei den deutschen Militärs keinen Verdacht erregte. Um das Ultra-Geheimnis zu wahren, trafen Churchills Kommandeure verschiedene Vorkehrungen. Zum Beispiel lieferten die Enigma-Entschlüsselungen die Positionen zahlreicher U-Boote, doch es wäre unklug gewesen, jedes einzelne sofort anzugreifen, weil eine plötzliche, unerklärliche Zunahme der britischen Erfolge die Deutschen misstrauisch gemacht hätte. Folgerichtig liessen die Alliierten einige U-Boote entkommen und griffen andere erst an, wenn ein Spähflugzeug ausgeflogen war, womit sich die Annäherung eines Zerstörers – ein paar Stunden später scheinbar erklären liess. Oder aber die Alliierten schickten fabrizierte Meldungen in den Äther, wonach U-Boote gesichtet worden seien, was ebenfalls ausreichte, um den darauf folgenden Angriff zu erklären.

Trotz dieser Strategie, Hinweise auf die Entschlüsselung der Enigma zu vermeiden, erregten die britischen Unternehmungen gelegentlich Verdacht bei der deutschen Abwehr. Bei einer Gelegenheit entzifferte Bletchley eine Enigma-Meldung mit der genauen Position einer Gruppe von neun deutschen Tank- und Versorgungsschiffen. Die Admiralität beschloss in diesem Fall, nicht alle diese Schiffe zu versenken, da ein so glatter Erfolg die Deutschen misstrauisch gemacht hätte. Deshalb gab man den eigenen Zerstörern die genauen Positionen von nur sieben Schiffen durch, die Gadania und die Gonzenheim sollten unbeschädigt entkommen. Die sieben zum Abschuss freigegebenen Schiffe wurden tatsächlich versenkt, doch die Zerstörer der Royal Navy begegneten zufällig auch den beiden Schiffen, die verschont werden sollten, und versenkten sie ebenfalls. Die Offiziere auf den Zerstörern wussten nichts von der Enigma und der Strategie der Verdachtvermeidung - sie waren einfach überzeugt, ihre Pflicht zu tun. In Berlin leitete Admiral Kurt Fricke eine Untersuchung dieses und ähnlicher Vorfälle ein, um der Möglichkeit nachzugehen, dass die Briten Enigma entschlüsselt hatten. Der Bericht kam zu dem Schluss,

dass die zahlreichen Verluste entweder schlichtes Pech waren oder Schuld eines englischen Spions, der sich in die Kriegsmarine eingeschleust hatte. Die Entschlüsselung der Enigma hielt man für unmöglich und undenkbar.

Einige, wenn auch umstrittene Stimmen behaupteten, die Leistungen von Bletchley Park seien entscheidend für den Sieg der Alliierten gewesen. Sicher ist jedenfalls, dass die Codebrecher von Bletchley den Krieg wesentlich verkürzten. Dies wird deutlich, wenn man noch einmal die Atlantikschlacht Revue passieren lässt und darüber nachdenkt, was ohne den Vorteil des Aufklärungswissens von Ultra geschehen wäre. Zunächst einmal hätte die deutsche U-Boot Flotte in ihrer Übermachtstellung sicher noch mehr alliierte Schiffe und Nachschub zerstört, die entscheidende Verbindung nach Amerika weiter geschwächt und die Alliierten gezwungen, noch mehr Arbeitskraft und Ressourcen in den Bau neuer Schiffe zu stecken. Historiker schätzen, dass sich die alliierten Unternehmungen in diesem Fall um mehrere Monate verzögert hätten, und das hiesse, D-Day wäre bis mindestens ins folgende Jahr verschoben worden. Dies hätte auf beiden Seiten viele Menschenleben gekostet.

Allerdings ist die Kryptoanalyse eine Arbeit, die sich dem öffentlichen Blick entziehen muss, und so blieben die Erfolge von Bletchley auch nach dem Krieg ein streng gehütetes Geheimnis. Grossbritannien, das während des Krieges den gegnerischen Nachrichtenverkehr so wirksam entschlüsselt hatte, wollte seine Strategie fortsetzen und war keineswegs geneigt, andere an seinen Möglichkeiten teilhaben zu lassen.

Nach drei Jahrzehnten des Schweigens wurde das Geheimnis von Bletchley Park Anfang der siebziger Jahre aufgedeckt. Captain E W. Winterbotham, der für die Verteilung des Ultra Materials verantwortlich gewesen war, begann die britische Regierung mit Eingaben zu bombardieren. Die Commonwealth-Länder, so argumentierte er, verwendeten die Enigma nicht mehr, und man könne nichts gewinnen, wenn man die Tatsache verberge, dass England sie geknackt hatte. Die Geheimdienste gaben widerstrebend nach und erlaubten ihm, ein Buch über die Arbeit von Bletchley Park zu schreiben. Winterbothams The Ultra Secret erschien im Sommer 1974 und war das Signal dafür, dass die Leute von Bletchley Park endlich die Anerkennung erhielten, die sie verdienten.

Für Alan Turing kam dies alles zu spät. Vor dem Krieg hatte er sich als mathematisches Genie erwiesen und Arbeiten veröffentlicht, in denen er die grundlegende Funktionsweise des Computers und der digitalen Informationsverarbeitung beschrieben hatte. In Bletchley Park wandte er sein Denken der Aufgabe zu, die Enigma zu knacken, deren Schwachstellen er mit der sicherlich bedeutendsten Einzelleistung aller Beteiligten aufzuspüren half. Nach dem Krieg jedoch bejubelte man ihn nicht als Helden, sondern verfolgte ihn wegen seiner Homosexualität. Als er 1952 einen Einbruch bei der Polizei anzeigte, äusserte er unbedacht, dass er eine homosexuelle Beziehung habe. Die Polizisten waren der Meinung, sie hätten keine andere Wahl, als ihn zu inhaftieren und anzuzeigen. Die Zeitungen berichteten von dem darauf folgenden Prozess und der Verurteilung. Turing wurde öffentlich gedemütigt.

Turings Geheimnis war enthüllt, seine Homosexualität war jetzt öffentliches Wissen. Die britische Regierung entzog ihm den Status eines Geheimnisträgers und verbot ihm jegliche Mitarbeit in Forschungsprojekten, die mit der Entwicklung des Computers zu tun hatten. Er wurde gezwungen, einen Psychiater aufzusuchen, und musste eine Hormonbehandlung über sich ergehen lassen, die ihn impotent und fettleibig werden liess. In den zwei Jahren darauf bekam er schwere Depressionen, und am 7. Juni 1954 ging er mit einem Glas Zyanidlösung und einem Apfel in sein Schlafzimmer. Er tauchte den Apfel in das Zyanid und ass einige Bissen davon. Im Alter von nur zweiundvierzig Jahren ging eines der wahren Genies der Kryptoanalyse in den Freitod.

2 Dokumentation

2.1 Get started

Willkommen bei deinem neuen Programm! Um dich schnell auf den Weg zu machen, hier ein kurzes Codebeispiel zur Bedienung des Programms. Du kannst direkt loslegen indem Du folgenden Code in deiner Konsole eingibst:

```
user@example:~$ python3 Enigma_<version>.py\
 -m „HELLOWORLD“ \
-rl „ROTOR_I,ROTOR_II,ROTOR_III“  \
-ro „W,X,C“ -pb „PLUGBOARD_A“ \
-ref „REFLECTOR_B“

Original message: RUSSIANSARECOMING
Crypted message: FHVNEOLKLCVNCKIEF
```

Du kannst den Code hier einfach kopieren und in eine Kommandozeile eingeben und Enter drücken.

Beachte aber:

Die hier ausgegebene Nachricht muss nicht unbedingt der tatsächlichen verschlüsselten Nachricht entsprechen. Die Nachricht dient lediglich der Anschauung.

Für Informationen und Details über die jeweiligen Argumente, guck bitte in den entsprechenden Abschnitt zu dem Argument. Diese sind im Inhaltsverzeichnis verlinkt/einfach anklickbar.

2.2 Argumente

Die erste Version stellt jeweils die Kurzform des jeweiligen Arguments dar. Die zweite Version stellt die Langversion da. Was von Beidem benutzt wird, spielt für die Funktionalität des Programms keine besonders große Rolle.

„-m ‚HELLO“ / „--message ‚HELLO‘“:

Quelle:

Simon Singh
CODES
Carl Hanser Verlag

Weiterführende Links: (30.10.03)

http://www.deutsches-museum.de/ausstell/meister/enigma.htm

http://www.informatik.hu-berlin.de/~huber/enigma/enigma.html

http://putsch.net/entwurf/?main=enigma

http://www.informatik.uni-kiel.de/inf/deRoever/SS03/SWP/main004.html

http://home.t-online.de/home/grey-wolf/uenigmaapplet/uenigmasimulation.htm