Humboldt Universität zu Berlin WS 2006/07

Institut für Informatik
Informatik in Bildung und Gesellschaft
Seminar: Geschichte der Verschlüsselung
Tutorin: Constanze Kurz

Die Enigma

Dominik Oepen (503591) Sebastian Höfer (505008)

20. April 2007

Inhaltsverzeichnis

1 Einleitung

Die Enigma ist wahrscheinlich eine der bekanntesten Chiffriermaschinen der Geschichte. Ihre Erfindung, Verwendung sowie schließlich ihre Entschlüsselung hatten weitreichende Auswirkungen auf den Verlauf des Zweiten Weltkrieges, auf die nachfolgende Kryptographie, sowie auf die Art der Kriegsführung der folgenden Kriege des 20. und 21. Jahrhunderts. Informationsaustausch durch gesicherte und schnelle Kommunikation zwischen den einzelnen Truppenteilen gewannen im Zweiten Weltkrieg stärker an Bedeutung, und die Enigma ermöglichte den Nationalsozialisten – zumindest vor Ihrer Entschlüsselung – einen sicheren Nachrichtenverkehr, welcher koordinierte Überraschungsangriffe und nicht zuletzt die deutsche Blitzkriegtaktik erst ermöglichten.

Diese Arbeit setzt sich aus folgenden Teilen zusammen: Zunächst wird es einen kleinen Abriss über die Geschichte der Enigma geben. Darauf folgen Abschnitte über ihren Aufbau und ihre Funktionsweise sowie ein Abschnitt darüber, wie die Deutschen die Enigma während des Krieges verwendet haben. Wir gehen dabei vor allem auf die am weitesten verbreitete „Enigma I“ ein und sprechen an den entsprechenden Stellen Modifikationen bei anderen Versionen der Enigma an. Als nächstes werden die Arbeiten zur Entschlüsselung der Enigma in Polen und Großbritannien näher beleuchtet. Die Arbeit schließt mit einigen Überlegungen zu den historischen Auswirkungen der Enigma. Zum einen wird erörtert, inwiefern die Enigma den Deutschen einen entscheidenden Vorteil verschaffte, und wie diese Überlegenheit mit der erfolgreichen Entschlüsselung sich zugunsten der Alliierten wandte. Und schließlich stellen wir uns die Frage: Was wäre, wenn die Enigma nicht entschlüsselt worden wäre?

2 Die Geschichte

Nachdem es während des Ersten Weltkrieges v. a. auf deutscher Seite ein regelrechtes kryptographisches Debakel gab, schien der Ruf nach einer automatischen Chiffriermaschine, der ein sichereres Verschlüsselungsverfahren zugrunde liegt, groß. So setzten sich ab 1917 unabhängig voneinander dokumentiert vier Entwickler mit der Idee auseinander, eine so genannte Rotorchiffriermaschine (siehe 3) zu konstruieren, darunter der Holländer Alexander Koch, der Schwede Arvid Damm, der Amerikaner Edward Hebner sowie auch der Deutsche Arthur Scherbius; dieser reichte am 23. Februar 1918 in Deutschland das Patent DRP 416 219 für eine „Verschlüsselungsmaschine nach dem Rotorprinzip“ ein – die Enigma. Scherbius versuchte diese sowohl auf dem freien Markt als auch ans Militär zu verkaufen, doch der kommerzielle Erfolg blieb – wie auch bei den anderen Erfindern – zunächst aus. Für Firmen und Privatleute war das Gerät schlicht zu teuer[1], das deutsche Militär winkte dankend ab, da dieses zu diesem Zeitpunkt noch davon ausging, dass eine solche Verschlüsselungsmaschine nicht nötig wäre.

Abbildung 2.1: Arthur Scherbius

Tatsächlich hatten die Briten während des Ersten Weltkrieges eine brisante Nachricht des deutschen Staatssekretärs im Auswärtigen Amt Arthur Zimmermann an den deutschen Gesandten in Mexiko abgefangen und entschlüsselt, das so genannte *Zimmermann-Telegramm*. In diesem Telegramm hatten die Deutschen Mexiko ein Bündnis gegen die Vereinigten Staaten vorgeschlagen, sollten die USA in den Ersten Weltkrieg eintreten. Der Schuss ging nach hinten los – die Briten veröffentlichten 1917 das Telegramm, die USA traten in den Krieg ein und der Krieg war verloren. Jedoch hielten die Briten bis 1923, als Winston Churchill den ersten Band von „The World Crisis“ veröffentlichte, zurück, dass sie durch die Entschlüsselung der Nachricht an deren Inhalt gekommen waren. Die offizielle Version war bis 1923, dass der Inhalt des Zimmermann-Telegramms durch eine Unachtsamkeit in der deutschen Botschaft in fremde Hände gelangt war.

Doch auch der Schock, den das Wissen um die Entschlüsselung des Zimmermann-Telegramms bei der deutschen Obrigkeit hervorgerufen haben muss, verhalf der Enigma nicht unmittelbar zum kommerziellen Erfolg. Im Jahr 1926 fügte Willi Korn, ein Mitarbeiter von Scherbius, der Enigma einige Erweiterungen hinzu, darunter die Umkehrwalze (siehe 3). Erst in diesem Jahr konnten einige Maschinen an die deutsche Marine, 1928 an die Armee und 1935 an die Luftwaffe abgesetzt werden. Arthur Scherbius selbst aber konnte den Siegeszug der Enigma nicht miterleben: 1929 starb er bei einem Unfall mit seiner Kutsche. Im Jahr 1934 erwarben Rudolf Heimsoeth und Elsbeth Rinke die ehemalige Firma Scherbius, welche unter dem Firmennamen „Heimsoeth & Rinke“ in Berlin die Fertigung der Enigma fortsetzte.

[1] Nach [1] bot Scherbius die Enigma für 600 Reichsmark an, was nach [4] etwa 4200 Euro entspräche

3 Der Aufbau

Eine Enigma ist im Prinzip folgendermaßen aufgebaut: Über eine schreibmaschinenähnliche *Tastatur* wird der zu verschlüsselnde Text eingegeben. Jedes Mal, wenn ein Buchstabe eingegeben wird, leuchtet, solange die Taste gedrückt ist, der entsprechende verschlüsselte Buchstabe auf dem *Lampenfeld* auf. Die Komponenten, welche für die Verschlüsselung zuständig sind, sind das *Steckbrett* sowie die *Rotorwalzen*.

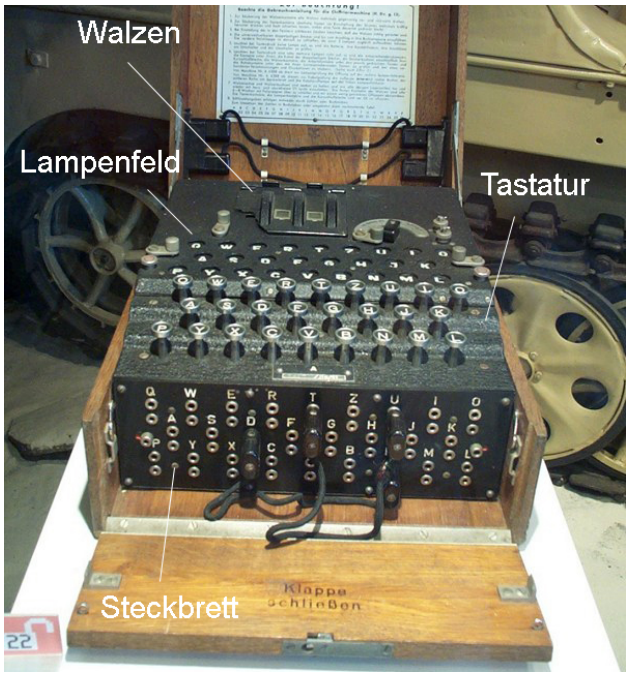

Abbildung 3.1: Die Enigma

3.1 Das Steckbrett

Die Tasten der Tastatur sind mit dem Steckbrett über elektrische Leitungen verbunden, so dass nach der Betätigung einer Taste der Strom zunächst durch das Steckbrett fließt. Mit Hilfe des Steckbrett können nun die Buchstaben miteinander vertauscht werden, d. h. wenn z. B. die Buchstaben „A“ und „X“ miteinander mit einem Kabel auf dem Steckbrett verbunden werden, so werden vor der weiteren Verschlüsselung durch die Rotorwalzen diese beiden Buchstaben vertauscht. Somit ist klar, dass durch das Steckbrett eine monoalphabetische Verschlüsselung realisiert wird, deren Stärke von der Anzahl der verwendeten Steckerkabel und somit der vertauschten Buchstabenpaare abhängt.

Bis 1939 wurden 6 Steckerkabel verwendet, so dass insgesamt 12 Buchstaben jeweils paarweise vertauscht wurden. Später wurde die Anzahl der Steckerkabel auf 8 erhöht.

3.2 Die Rotorwalzen

Monoalphabetische Verschlüsselungssysteme vergrößern zwar den Schlüsselraum ungemein, können aber durch Häufigkeitsanalysen meistens einfach geknackt werden, so dass die stärkste Verschlüsselungskomponente sicherlich bei den Rotorwalzen liegt. Die erste Walze, die *Eintrittswalze*, ist mit dem Steckbrett verbunden. Die Eintrittswalze ist dann mit der nachfolgenden Walze verbunden, und diese wieder mit noch einer etc. Da aus dem Steckbrett 26 Leitungen, für jeden Buchstaben eine, herausführen, haben auch die Walzen jeweils 26 Ein- und Ausgänge. Wie auf Abbildung 3.2 zu sehen, verfügt jede Walze dabei über eine interne Verdrahtung, welche zur Folge hat, dass die Eingänge auf möglichst unvorhersehbare Weise mit den Ausgängen verbunden sind. Somit findet eine weitere Vertauschung der Buchstaben in jeder Walze statt.

Die besondere kryptographische Stärke der Enigma liegt darin, dass jede Walze nach einer bestimmten Anzahl von eingegebenen Zeichen rotiert, und sich das Signal einen anderen Weg zurück zum Lampenfeld bahnt. Somit wird eine polyalphabetische Verschlüsselung erreicht, da sich die Permutationsfunktion mit jedem Anschlag ändert. Dabei rotiert die Eintrittswalze nach jedem Anschlag (deswegen wurde sie auch „schneller Rotor“ genannt), die nächste nach 26^1 (also einer kompletten Umdrehung der Eintrittswalze), die nächste nach 26^2 Anschlägen, usw. Werden also z. B. drei Walzen verwendet, ist die Ausgangskonfiguration der Walzen erst nach 26^3 Anschlägen wiederhergestellt.

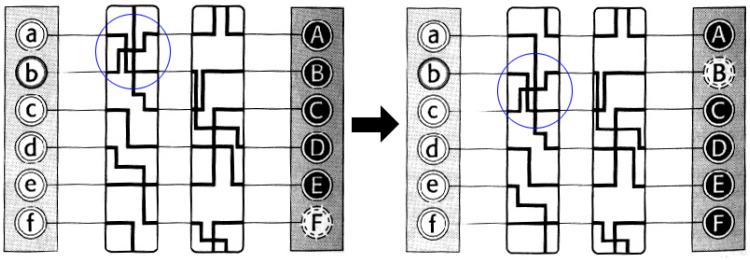

Abbildung 3.2: Die Konfiguration der Rotorwalzen einer fiktiven Enigma vor und nach Betätigung der „B“-Taste. Die erste Walze rotiert um einen Schritt, so dass bei erneuter Eingabe von „b“, dieses nicht wie beim ersten Mal in „F“, sondern in „B“ verschlüsselt wird.

Damit nun die Enigma auch zur Dechiffrierung eines Textes benutzt werden konnte, führte Willi Korn als vierte Walze die *Umkehrwalze*, auch *Reflektor* genannt, ein. Das Signal fließt nun aus der letzten Rotationswalze nicht direkt in das Lampenfeld, sondern in die Umkehrwalze. Diese hat nur auf einer Seite 26 Kontakte, so dass diese spezielle Walze das Signal wieder zurück durch die Rotationswalzen und ein weiteres Mal durch das Steckbrett leitet, bis es dann beim Lampenfeld ankommt und der verschlüsselte Buchstabe angezeigt wird. Die Umkehrwalze bewirkt also, dass wenn ein Buchstabe X bei einer bestimmten Ausgangskonfiguration durch den Buchstaben Y verschlüsselt wird, bei der gleichen Konfiguration auch Y durch X verschlüsselt wird. Zum einen versprachen sich die Entwickler der Enigma dadurch, dass das Signal nun zweimal die Walzen passierte, eine stärkere Verschlüsselung. Zum anderen hatte die Einführung der Umkehrwalze den großen Vorteil, dass nun eine verschlüsselte Nachricht bei identischer Ausgangskonfiguration der Walzen und denselben Steckbrettschaltungen in die Enigma eingegeben werden kann, und man den Klartext erhält. Das vereinfachte die Bedienung, sparte Kosten und war vor allem an der Front und ganz besonders in U-Booten, in welchen notorischer Platzmangel herrschte, äußerst praktisch. Diese Eigenschaft nennt man *Invultorik* - sie sollte sich bei aller Benutzerfreundlichkeit als verhängnisvolle kryptographische Schwäche der Enigma herausstellen (siehe 5).

In der gebräuchlichsten Version der Enigma waren drei Walzen gleichzeitig im Betrieb, bei den Modellen der Marine später vier, im ursprünglichen Modell waren sogar acht verschiedene Walzen in Reihe geschaltet. Allerdings kamen auch bei den Enigmavarianten, bei welchen weniger Walzen gleichzeitig in Betrieb waren, mehrere Walzentypen zum Einsatz. So standen ab 1939 fünf verschiedene Walzentypen zur Verfügung, welche mit römischen Zahlen I bis V durchnummeriert waren. Ebenso wurde eine weitere Umkehrwalze eingeführt; die zwei zu dieser Zeit gebräuchlichen Umkehrwalzen wurden mit A und B bezeichnet.

4 Die Verwendung

Die Deutschen hatten sehr genaue Vorschriften zur Verwendung der Enigma und zur Übermittlung der verschlüsselten Botschaften. Zunächst einmal musste die Enigma korrekt eingestellt werden. Während des Zweiten Weltkriegs wurden die Verwendungsvorschriften für die Enigma mehrmals verschärft. Wir beschreiben hier die gängigste Vorgehensweise.
Zunächst mussten die Walzen in die korrekte Ausgangsstellung gebracht werden. Die Ausgangskonfiguration der Enigma, der so genannte *Tagesschlüssel*, war in Codebüchern festgelegt und allen Kommunikationspartnern bekannt. Der Tagesschlüssel bestimmte die Ausgangskonfiguration der Enigma. Er legte fest welche Buchstaben durch das Steckerbrett vertauscht wurden, welche Walzen verwendet wurden und in welcher Reihenfolge sie eingesetzt wurden. Außerdem bestimmte er die Grundstellung der Walzen, also welcher Buchstabe bei jeder Walze in der Ausgangsstellung nach oben gedreht wurde.
Das kryptologische Problem der Verwendung von Tagesschlüsseln bestand darin, dass vor allem während des Krieges täglich eine riesige Masse an Nachrichten versandt und verschlüsselt werden musste. Grundsätzlich lässt sich sagen, dass ein Kryptoanalytiker, der eine Nachricht dekodieren und den verwendeten Schlüssel extrahieren möchte, leichteres Spiel hat, wenn er eine Fülle an Material hat, dass er analysieren kann. Die Nationalsozialisten mussten davon ausgehen, dass ihre Kommunikation abgehört wurde. Daher war die Sorge groß, dass der Feind den jeweiligen Tagesschlüssel herausfinden könnte, wenn alle Nachrichten eines Tages nur mit diesem verschlüsselt wurden.

Diesem Problem begegneten die Deutschen, indem sie zusätzlich so genannte *Spruchschlüssel* einführten. Dieser Schlüssel sollte von jedem Funker für jede zu versendende Nachricht individuell gewählt werden. Dazu suchte sich der Funker zunächst eine individuelle Grundstellung der Walzen aus. Die 3 Buchstaben, die diese Grundstellung kennzeichneten, verschlüsselte er mit dem Tagesschlüssel. Den Rest der Nachricht verschlüsselte er mit dem von ihm gewählten Spruchschlüssel. Der Empfänger der Nachricht entschlüsselte die ersten Buchstaben der Nachricht mit dem Tagesschlüssel, stellte seine Enigma auf den so gewonnenen Spruchschlüssel ein und konnte dann den Rest der Nachricht dechiffrieren. Durch dieses Verfahren wurde erreicht, dass möglichst wenig Nachrichtenmaterial mit dem Tagesschlüssel verschlüsselt wurde. Die Kryptoanalytiker hatten es daher mit einer Vielzahl an Nachrichten zu tun, die mit unterschiedlichen Schlüsseln codiert waren. Um Übertragungsfehler zu vermeiden, wurde der Spruchschlüssel zweimal hintereinander am Anfang einer Nachricht gesendet. Entschlüsselte der Empfänger die erhaltene Nachricht, und die beiden Buchstabentripel am Anfang der Nachricht stimmten nicht überein, so wusste er, dass bei der Nachrichtenübertragung ein Fehler unterlaufen war. Wie wir in Abschnitt 5.1 sehen werden, sollte sich die *Spruchschlüsselverdoppelung* als eine kryptographische Schwäche und als Angriffspunkt für die polnischen Kryptoanalytiker herausstellen.

5 Die Entschlüsselung

Die Geschichte der Entschlüsselung der Enigma lässt sich in zwei Phasen aufteilen. Vor dem Krieg sind vor allem die Leistungen der Polen hervorzuheben. Nach der Besetzung Polens durch die Deutschen wurde die Arbeit der polnischen Kryptoanalytiker von den Briten fortgesetzt.

5.1 Vor dem Krieg

Die weitaus größten Erfolge bei der Entschlüsselung der Enigma vor dem Krieg wurden in Polen erzielt. Die Polen unternahmen große Anstrengungen, um die Nachrichten der Deutschen zu entschlüsseln. Zuständig für die Entschlüsselung war das Biuro Szyfrów unter Hauptmann Maximilian Ciezki. Das Biuro Szyfrów war während des Angriffs der Russen gegründet worden, um die Nachrichten der Russen zu entschlüsseln und die Invasion durch die dadurch gewonnenen Informationen zu unterbinden. Nachdem der Angriff der Russen abgewehrt war, begannen die polnischen Kryptoanalytiker damit, auch den deutschen Nachrichtenverkehr zu entschlüsseln. Dies geschah, da sich Polen von Deutschland bedroht fühlte. Im Rahmen des Versailler Vertrages hatte Deutschland große Landstriche an Polen übergeben müssen, und die polnische Regierung befürchtete, dass Deutschland eines Tages versuchen würde diese zurück zu erobern. Einige Jahre lang entschlüsselten die polnischen Kryptoanalytiker den deutschen Nachrichtenverkehr erfolgreich. Doch als die Deutschen 1926 die Enigma einführten, gelang ihnen das nicht mehr. Maximilian Ciezki war deswegen sehr aufgebracht, da er um den strategischen Wert der durch die Entschlüsselung gewonnenen Informationen wusste. Er setzte alles daran, das neue Verschlüsselungsverfahren der Deutschen zu brechen, beauftragte sogar einen Hellseher damit, Codes vorherzusagen. Bald wurde ihm klar, dass er das neue Verschlüsselungsverfahren nicht mit klassischen Verfahrensweisen der Kryptoanalyse, wie z. B. der Häufigkeitsanalyse, würde brechen können. Er suchte nach einem neuen Ansatz und beschloss sich der Mathematik zu bedienen. Um geeignete Kryptoanalytiker mit mathematischer Ausbildung zu finden, veranstaltete er an der Universität Posen einen Kryptographiewettbewerb, bei welchem er drei Mathematiker für die Arbeit im Biuro Szyfrów auswählte. Tatsächlich wählte Ciezki die Universität Posen aus, da diese vor dem ersten Weltkrieg noch in deutscher Hand gewesen war, und somit die meisten Studenten und Lehrenden der Universität fließend Deutsch sprachen.

Der begabteste der drei ausgewählten Mathematiker war Marian Rejewski.

Dieser wurde sogleich mit der Entschlüsselung der Enigma beauftragt. Hierfür standen ihm zunächst nur eine kommerzielle Variante der Enigma und die bisher abgefangenen verschlüsselten Nachrichten der Deutschen zur Verfügung. Die kommerzielle Variante der Enigma unterschied sich jedoch signifikant von der militärischen Variante, da sie zum einen nicht über ein Steckbrett verfügte und zum anderen ihre Walzen anders verdrahtet waren. Rejewski versuchte zunächst die interne Walzenverdrahtung der militärischen Enigma zu ergründen. Es gelang ihm eine Gleichung aufzustellen, aus welcher die Walzenverdrahtung berechnet werden konnte. Allerdings enthielt diese Gleichung noch zu viele Unbekannte, um sie zu lösen. Zu diesem Zeitpunkt kam Rejewski das Schicksal zu Hilfe. Bereits 1931 hatten die Franzosen von dem Deutschen Hans-Thilo Schmidt,

welcher im deutschen Chiffrierwesen tätig war, die „Gebrauchsanweisung für die Chiffriermaschine Enigma“ und die „Schlüsselanleitung für die Chiffriermaschine Enigma“ erworben. Schmidt hatte zu der Zeit nicht viel für das deutsche Militär übrig, da ihm seit geraumer Zeit eine Beförderung verwehrt blieb, so dass ihm jede Möglichkeit recht war, dem deutschen Militär zu schaden. Die französischen Kryptoanalytiker hielten die Entschlüsselung der Enigma jedoch auch mit diesem Material für unmöglich und unternahmen daher keinerlei Bestrebungen, sich mit einer möglichen Entschlüsselung der Enigma zu beschäftigen. Im Rahmen eines 10 Jahre alten Abkommens zum Informationsaustausch zwischen Polen und Frankreich gaben die Franzosen die von Hans-Thilo Schmidt gewonnen Informationen an Polen weiter. Dank der Gebrauchsanweisung für die Enigma gelang es Rejewski einige der Unbekannten in seiner Gleichung zu eliminieren und schließlich die interne Walzenverdrahtung der militärischen Enigma zu ergründen. Mit diesen Informationen konnten nun Nachbauten der zu knackenden Enigma hergestellt werden.

Abbildung 5.1: Marian Rejewski

Zwar war nun das Verschlüsselungsverfahren bekannt, doch ohne Kenntnis der Schlüssel konnte es immer noch nicht gebrochen werden. Rejewski stand nun vor dem Problem die Tagesschlüssel der Deutschen rekonstruieren zu müssen. Er wusste, dass jede Nachricht mit einem individuellen Spruchschlüssel verschlüsselt wurde (siehe 4), und war sich darüber im Klaren, dass er nur über relativ wenig Nachrichtenmaterial, das mit demselben Schlüssel verschlüsselt worden war, verfügte. Allerdings gelang es ihm, einen Verfahrensfehler der Deutschen auszunutzen: Die Spruchschlüsselverdoppelung. Da der 3 Zeichen lange Spruchschlüssel am Anfang der Nachricht zweimal hintereinander übermittelt wurde, wusste Rejewski, dass der erste und vierte Buchstabe der verschlüsselten Nachricht für denselben Klartextbuchstaben standen. Dasselbe galt für den zweiten und fünften, beziehungsweise den dritten und sechsten Buchstaben. Da alle Spruchschlüssel mit dem selben Tagesschlüssel verschlüsselt waren, konnte Rejewski mit ausreichend Material im Laufe eines Tages eine Tabelle aufstellen, welche jeden Buchstaben des Alphabets mit einem anderen Buchstaben in Relation setzte.
Auf der Grundlage dieser Tabellen konnte Rejewski nun Rückschlüsse auf die zu Grunde liegende Walzenstellung ziehen. Hierbei ging er wie folgt vor: Er wählte einen Buchstaben und suchte aus seiner Relationstabelle den zugehörigen Partnerbuchstaben. Zu diesem Partnerbuchstaben suchte er wiederum den in Relation stehenden Buchstaben und schrieb diese Buchstaben hintereinander auf, solange bis er auf den zu Anfang gewählten Ausgangsbuchstaben stieß. Er hatte somit eine Kette gebildet, welche einen Buchstaben wieder in sich selbst überführte. Er bildete nun so lange weitere Ketten, bis alle Buchstaben des Alphabets Teil einer Kette waren. Das besondere an diesen Ketten war, dass sie charakteristisch für genau eine Walzenstellung waren. Anhand der Anzahl und der Länge der Ketten war genau eine Ausgangsstellung der Walzen der Enigma spezifiziert. Das Steckbrett hatte zwar einen Einfluss auf die Stellung der Buchstaben innerhalb dieser Ketten, jedoch nicht auf die Länge und Anzahl der Ketten. Rejewski war es also gelungen, die Entschlüsselung der Walzenstellung und des Steckbretts von einander zu trennen. Der Schlüsselraum für die Walzenstellung war signifikant kleiner als der gesamte Schlüsselraum der Enigma, insgesamt

waren „nur“ 17 576 Walzenstellungen möglich (siehe 3). Innerhalb eines Jahres stellten Rejewskis Assistenten einen Katalog mit den charakteristischen Ketten für alle möglichen Walzenstellungen zusammen. Übrig blieb noch der Einfluss des Steckbretts. Die Steckerverbindungen waren jedoch relativ einfach zu rekonstruieren, da bis 1939 nur sechs Stecker verwendet wurden, also nur sechs Buchstabenpaare vertauscht wurden. Es blieben somit 14 Buchstaben ungesteckert, die mit der ermittelten Walzenstellung auch ohne die Steckverbindungen korrekt in Klartext übersetzt wurden. Somit konnten bereits ohne Kenntnis der Steckerverbindungen große Teile des Klartexts gelesen werden, mit welchen sich die durch Stecker vertauschten Buchstaben recht leicht rekonstruieren ließen.

Somit war die Enigma gebrochen. Der Alltag der polnischen Kryptoanalytiker sah nun folgendermaßen aus: Zunächst mussten genügend Spruchschlüssel gesammelt werden, um die charakteristischen Ketten der Walzenstellung zu bilden. Waren die Ketten gefunden, konnte man aus dem Katalog die Walzenstellung heraussuchen und anschließend die Steckerverbindungen ergründen. Dieses Verfahren war sehr arbeitsintensiv, so dass zwei Geräte zu Automatisierung erfunden wurden: die Bomba und das Zyklometer. Beide basierten auf Walzensätzen der Enigma.

1939 führten die Deutschen zwei neue Walzen ein. Rejewski gelang es zwar die Verdrahtung der neuen Walzen IV und V zu erschließen, jedoch stieg die Anzahl der möglichen Walzenpositionen nun von 6 auf 60 ($\binom{5}{3}$, statt 3! Möglichkeiten). Um diese neue Variante der Enigma zu entschlüsseln, wären somit 60 statt 6 Bombas notwendig gewesen. Den Polen fehlten das Material und die Zeit um die Enigma ein weiteres Mal zu entschlüsseln. Als klar wurde, dass es bald zu einer deutschen Invasion in Polen kommen würde, beschlossen die Polen ihre Forschungsergebnisse an die Alliierten weiterzugeben.

5.2 Während des Krieges

Die Engländer setzten die Entschlüsselungsarbeiten der Polen im 70 km nordwestlich von London gelegenen Bletchley Park fort. Dorthin war die Government Code and Cipher School aus Platzgründen umgezogen. Und dieser Platz sollte auch benötigt werden. Bis zu 10000 Menschen waren zu Hochzeiten in Bletchley Park mit der Entschlüsselung der Nachrichten der Achsenmächte beschäftigt. Zunächst lief die Entschlüsselung über das Ausnutzen schwacher Spruchschlüssel ab. Die Deutschen verwendeten nämlich sehr oft schwache Spruchschlüssel (4) wie z.B. auf der Tastatur nebeneinander liegende Buchstaben. Diese schwachen Spruchschlüssel wurden auch *cillies* genannt, da angeblich ein deutscher Funker seine Nachrichten immer mit den ersten drei Buchstaben des Namens seiner Freundin Cilly verschlüsselte.

Doch auch komplexere Verfahren zum Entschlüsseln der Enigma wurden in Bletchley Park entwickelt. Hier müssen vor allem dir Arbeiten des wohl berühmtesten Codeknackers in Bletchley Park genannt werden: Alan Turing. Turing entwickelte die Arbeiten Rejewskis weiter. Allerdings wollte er sich nicht auf die Spruchschlüsselverdoppelung verlassen, da er damit rechnete, dass die Deutschen diese irgendwann als kryptographische Schwäche erkennen und fallen lassen würden. Statt dessen entwickelte er Rejewskis Ansatz der maschinellen Entschlüsselung weiter, in dem er das Konzept der Bomba ausarbeitete und die so genannte Turing Bombe konstruierte. Die Turing Bomben enthielten für jede der 60 möglichen Walzenlagen einen Satz von 12 Enigma Walzen, welche jeweils um eine Position versetzt liefen. Die Walzen waren so miteinander verschaltet, dass eine Lampe aufleuchtete, sobald die richtige Position gefunden war. Um den riesigen Schlüsselraum der Enigma nicht komplett durchsuchen zu müssen, behalf sich Turing mit wahrscheinlichen Wörtern

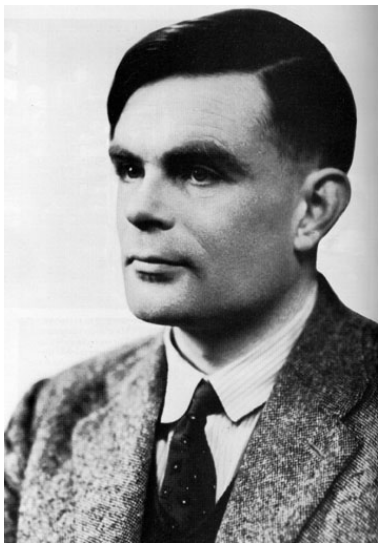

Abbildung 5.2: Alan Turing

im Klartext. Diese Wörter wurden von den Engländern “Cribs“ genannt. Da die Funknachrichten der Deutschen sehr stereotyp aufgebaut waren, enthielten sie eine Vielzahl an Cribs. Zum Beispiel waren in einer Großzahl der Funksprüche des deutschen Heeres die Worte „OBERKOMMANDODERWEHRMACHT“ zu finden. Auch konnten Regelmäßigkeiten im deutschen Funkverkehr ausgenutzt werden. So wurde vom deutschen Wetterdienst jeden Tag pünktlich um 5 Minuten nach 6 ein Wetterbericht geschickt. Dieser Bericht enthielt mit an Sicherheit grenzender Wahrscheinlichkeit das Wort Wetter.
Kannte man einen Crib so musste man noch herausfinden an welcher Position im Text er sich befand. Hierzu konnte eine konzeptuelle Schwäche der Enigma ausgenutzt werden, und zwar die *Invultorik* (3). Ein Effekt der Invultorik ist nämlich, dass kein Buchstabe in sich selbst verschlüsselt wird. Aus dem Klartextbuchstaben „A“ kann also nie der chiffrierte Buchstabe „A“ werden. Vermutet man nun, dass ein bestimmtes Wort im Klartext der Nachricht vorkommt kann man viele Positionen des Wortes ausschließen, indem man alle Positionen ausschließt, bei denen im chiffrierten und im Klartext der selbe Buchstabe an der selben Stelle auftaucht. Durch diese Methode gelang es Turing bei vielen Nachrichten den zu durchsuchenden Schlüsselraum drastisch zu reduzieren. Die Turing Bomben mussten somit nur noch einen Bruchteil des Schlüsselraums durchsuchen. Mit etwas Glück konnte der Tagesschlüssel dank dieses Verfahrens innerhalb von einer bis 5 Stunden gefunden werden

6 Fazit

Natürlich ist die Überlegung, wie der Krieg wohl verlaufen wäre, wenn die Enigma nicht gebrochen worden wäre, hochgradig spekulativ. Man kann jedoch feststellen, dass die Verluste der Alliierten, vor allem auf See, in den Phasen des Krieges, in welchen die Enigma auf Grund von Modifikationen nicht gebrochen werden konnten, ungleich höher waren, als zu den Zeitpunkten, in denen die Dechiffrierung gelang. Die meisten Autoren, die über dieses Thema geschrieben haben, sind sich einig, dass der Krieg wohl wesentlich länger gedauert hätte. Manche sind sogar der Ansicht, dass die Deutschen mit einer ungebrochenen Verschlüsselung England besiegen und den Krieg für sich hätten entscheiden können.
Eine erschreckende Überlegung hält die Website des deutschen Museums bereit [3]: Ursprünglich planten die USA die erste Atombombe über Deutschland und nicht über Hiroshima abzuwerfen. Nur auf Grund des frühzeitigen Kriegsendes wurde dieser Plan geändert. Wäre die Enigma also nicht entschlüsselt worden und hätte der Krieg daher länger gedauert, so wäre es unter Umständen zu einem Abwurf der Atombombe über Deutschland und somit wohl zu einer düsteren Zukunft für Deutschland gekommen.
Abschließend bleibt festzustellen, dass die Verschlüsselung des deutschen Funkverkehrs mittels der Enigma und dessen Entschlüsselung durch die Alliierten, immense Auswirkungen auf den Verlauf des Krieges hatten. Die Kryptologie spielte somit auch im Zweiten Weltkrieg eine große Rolle. Die für die Geschichte der Kryptologie bedeutendste Entwicklung des zweiten Weltkriegs ist wohl die massive Verwendung von maschinellen Verfahren sowohl zur Ver- als auch zur Entschlüsselung.

Literaturverzeichnis

[1] Atrops, Sascha: *Die Enigma.* Internet: http://www.sascha.atrops.com/pages/study/enigma.php [03.03.2007].

[2] Bauer, Friedrich: *Entschlüsselte Geheimnisse. Methoden und Maximen der Kryptologie.* 3. Auflage. Berlin: Springer, 2000.

[3] Deutsches Museum München: *Die Rotor-Chiffriermaschine Enigma der deutschen Wehrmacht* Internet: http://www.deutsches-museum.de/sammlungen/ausgewaehlte-objekte/meisterwerke-ii/enigma/ [03.03.2007].

[4] Matthaei, Rolf-Frederik: *Kaufkraft.* Internet: http://home.arcor.de/fredrik.matthaei/HVV/kaufkraft.htm [03.03.2007].

[5] Kahn, David: *The codebreakers. The story of secret writing.* 8. Auflage. New York: Scribner, 1996.

[6] Singh, Simon: *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.* München: Carl Hanser Verlag, 2000.

[7] Welchman, Gordon: *The hut six story. Breaking the Enigma codes.* New York: Penguin Books, 1984.

[8] Wikipedia: *Enigma (Maschine).* Internet: http://de.wikipedia.org/wiki/Enigma_%28Maschine%29 [03.03.2007].