Technische Details der Enigma

In diesem Papier werden die technischen Details der unterschiedlichen Enigma-Varianten vorgestellt, wie sie in der Wehrmacht, der Luftwaffe und der Kriegsmarine geläufig waren.

Inhalt

Prinzipschaltung 1
Die Walzen 2
Die Umkehrwalze 3
Verdrahtung der Walzen 4
Der Verschlüsselungsprozess der Walzen 5
Schrittmechanismus der Walzen 7
Wichtiger Hinweis zum Walzenfortschritt 8
Das Steckerbrett 8
Zubehör 9
Mathematische Sicherheit 10

Prinzipschaltung

Die Enigma ist ein elektromechanisches Verschlüsselungsgerät. Sie besteht aus einer Tastatur im deutschem QWERTZ-Layout, einem Lampenfeld (engl.: lamp panel) zur Darstellung des Alphabets, sowie drei oder vier Walzen (engl.: rotors). Hinzu kommt je nach Modell ein Steckerbrett mit Steckern (engl.: plugboard, plugs). Ein oder mehrere Walzen bewegen sich bei jedem Tastendruck. Walzen und Stecker verschlüsseln die gedrückte Taste, indem eine entsprechende Lampe im Lampenfeld eingeschaltet wird. Manche Modelle haben Platz für eine eingebaute 4V-Batterie, manche haben einen Schalter, um zwischen einer internen und externen Batterie umzuschalten. Wieder andere verfügen über einen Transformator zum Anschloss an das Stromnetz.

Abbildung 1: Enigma mit Beschriftung der Hauptkomponenten (Quelle: Wikipedia, gemeinfrei)

Abbildung 2: Enigma mit offener Abdeckung (Quelle: Bob Lord, www.ilord.com, Creative Commons License)

Abbildung 2 zeigt eine Wehrmachts-Enigma mit offener Abdeckung. Von links nach rechts: Umkehrwalze, drei Walzen, Eingangs Stator sowie das Batteriefach. An der linken Seite der zweiten Lampenreihe eine Reservelampe, das Loch rechts dient

zum Testen der Lampen.

Das Schaltbild in Abbildung 3 verdeutlicht die Prinzipschaltung. Um das Beispiel einfach zu halten, sind nur vier Komponenten gezeigt. Normalerweise sind 26 Lampen, Tasten, Stecker, Drähte usw. vorhanden. Der elektrische Strom fließt von der Batterie (1) durch den gedrückten Tastenkontakt A (2) zum Steckerbrett (3). Das Steckerbrett erlaubt es, die Verbindungen zwischen den Tasten und dem Eingangsfeld zu verändern. Danach fließt der elektrische Strom durch den – ungenutzten, daher geschlossenen – Stecker A (3) über die Eingangswalze (4) durch die Verdrahtung der drei (bzw. vier) Walzen (5) bis zur Umkehrwalze (6). Die Umkehrwalze schickt den elektrischen Strom über einen anderen Pfad zurück durch die Walzen (5) und Eingangswalze (4), er durchläuft nochmals die Stecker (3) – im Beispiel durch den mit Kabel (8) verbundenen Stecker S zu D – und von dort über die nicht gedrückte Taste D (9) zur entsprechenden Lampe D. Die Tasten (2) und (9) sind als bidirektionale Schalter ausgelegt; sie leiten in gedrücktem Zustand den Strom zum Steckerbrett, ansonsten zum Lampenfeld.

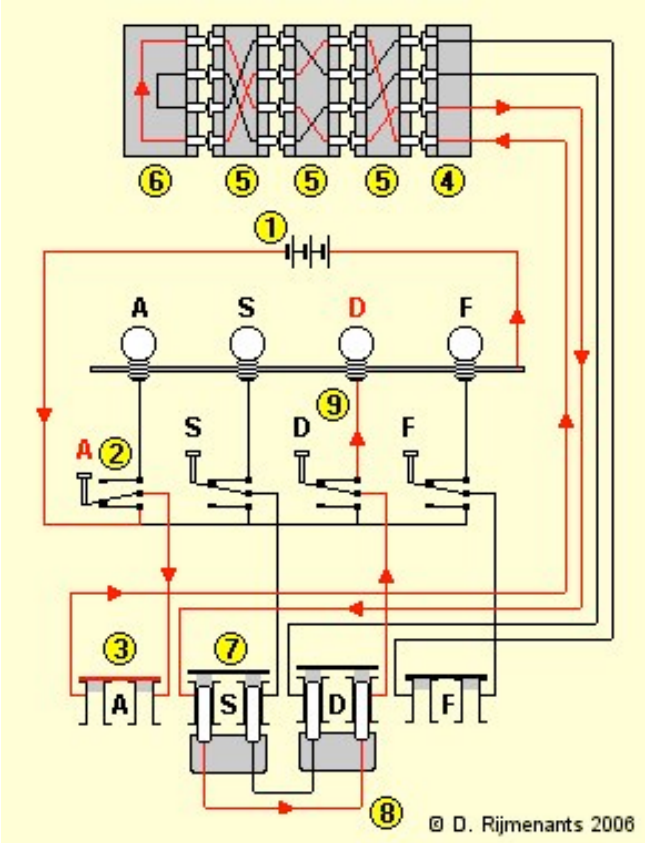

Abbildung 3: Prinzipschaltung der Enigma (Quelle: D. Rijmenants, mit Erlaubnis)

Anmerkung: Durch das Drücken einer Taste werden zuerst die Walzen gedreht, dann erst durchläuft der elektrische Strom die Verdrahtung zu den Lampen. Wird die Taste losgelassen, erlöscht die Lampe. Daher ist bei losgelassener Taste die Walzen-Grundstellung des soeben verschlüsselten Buchstaben sichtbar.

Die Walzen

Die Walzen sind das wichtigste Element der Enigma. Sie wurden aus Metall und Bakelit gefertigt, sind rund und haben einen Durchmesser von ca. 10 cm. Sie bestehen (vgl. Abbildung 4) auf ihrer rechten Seite aus 26 gefederten Kontakten (6); Drähte (5) verbinden die Kontakte mit 26 flachen Kontaktstellen auf ihrer linken Seite (4). In der Mitte ist eine Bohrung für eine Achse (8). Außen auf der Walze ist ein

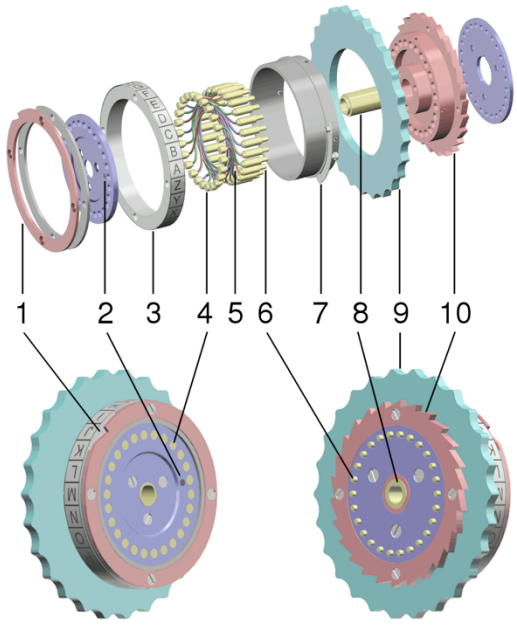

Abbildung 4: Aufbau einer Walze (Quelle: wikipedia, Crative Commons License)

beweglicher Ring (3) mit 26 Nummern oder Buchstaben und einer (oder zwei) Aussparungen (1). Der Ring ist drehbar auf der Walze angebracht und bei der Wehrmacht durch einen gefederten Stift (7) oder bei der Kriegsmarine durch zwei gefederte Bögen in einer der 26 möglichen Positionen fixiert. Wird die sog. Ringstellung verändert, so verändert sich die Position der Aussparung und des angezeigten äußeren Buchstabens relativ zur inneren Verdrahtung. Die Ringstellung wird über einen roten Punkt (2) gewählt. Jede Walze hat auf ihrer linken Seite eine Aussparung (1) und auf der rechten Seite eine Art Zahnrad (10). Diese werden von dem Mechanismus verwendet, der für das Weiterdrehen der Walzen verantwortlich ist. Die innere Verdrahtung der Walzen ist jeweils unterschiedlich. Für sich genommen stellt jede Walze eine einfache Substitutionschiffre dar. Die Kombination mehrerer Walzen, für jeden weiteren Buchstaben in anderer relativer Anordnung, macht die Komplexität der Gesamtverschlüsselung aus.

Abbildung 5: Walzen IV und V (Quelle: Bob Lord, www.ilord.com, Creative Commons License)

Zunächst wurde die Enigma mit drei Walzen ausgeliefert, ab 1939 mit fünf, bezeichnet mit römischen Ziffern I, II, III, IV, und V. Alle Walzen hatten eine Aussparung an jeweils anderer Stelle. Die Kriegsmarine erweiterte dies um drei weitere Walzen VI, VII und VIII, jede mit zwei Aussparungen. 1942 erweiterte die Kriegsmarine die Enigma um eine vierte Walze (M4). Damit sie mechanisch paßte, wurden die alten Umkehrwalzen (B und C) durch neue, dünnere Umkehrwalzen (b und c) ersetzt. Die Walzen für die vierte Position waren von besonderer Konstruktion, mit gefederten Kontakten auf beiden Seiten, und in zwei Ausprägungen (Beta und Gamma) vorhanden. Damit waren sie inkompatibel mit den anderen Walzen und konnten ausschließlich in der vierten Position benutzt werden.

Die Umkehrwalze

Die Umkehrwalze oder UKW ist eine typische Eigenschaft der Enigma. In jeder anderen Walze konnten alle 26 Buchstaben beliebig miteinander verbunden werden, d.h. A konnte mit F, F seinerseits mit K verbunden werden. In der Umkehrwalze wurden die Buchstaben nur paarweise vertauscht, d.h. wenn A mit F verbunden war, so war umgekehrt zwingend F mit A verbunden. Damit wurde die Verschlüsselung umkehrbar, d.h. die Entschlüsselung des verschlüsselten Textes wurde mit genau der gleichen Einstellung gemacht wie die ursprüngliche Verschlüsselung. Der Vorteil für die Bedienungsmannschaften ist klar, jedoch konnte dadurch niemals ein Buchstabe auf sich selbst abgebildet werden. Dies ist eine wesentliche Schwäche der Enigma, die durch die allierten Codeknacker regelmäßig ausgenutzt wurde.

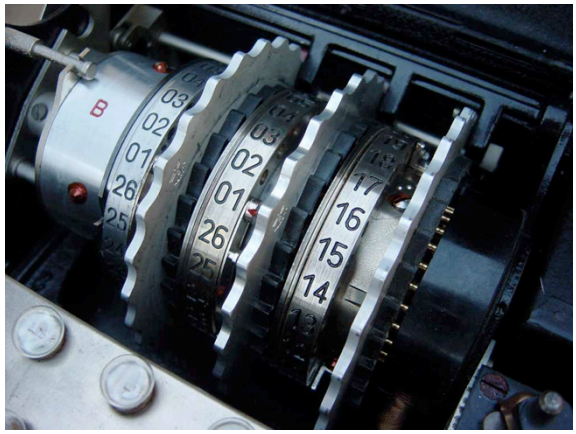

Abbildung 6: Umkehrwalze (B) und drei Rotoren eingesetzt (Quelle: Bob Lord, www.ilord.com, Creative Commons License)

Im zweiten Weltkrieg wurden zwei Umkehrwalzen eingesetzt. Sie hatten an ihrer linken Seite je 26 gefederte Kontakte. Die Enigma M4 der Kriegsmarine verwendete spezielle, dünnere Umkehrwalzen, die ebenfalls B und C benannt waren, jedoch eine andere Verdrahtung als die Wehrmachtsvarianten hatten. Allerdings war die Konstruktion so gewählt, dass die dünne Umkehrwalze B zusammen mit der Beta-Walze mit Ringstellung A und in Grundstellung A genau der Verdrahtung der Wehrmachts-Umkehrwalze B entsprach. Somit war die M4 in dieser speziellen Einstellung kompatibel zur Wehrmachts-Enigma. Gleiches gilt für die dünne Umkehrwalze C / Walze Gamma im Vergleich zur Wehrmachts-Umkehrwalze C.

Spät im Krieg wurde eine neue Umkehrwalze D eingeführt, die eine veränderliche innere Verdrahtung besaß.

Verdrahtung der Walzen

Die innere Verdrahtung der Walzen führte die eigentliche Verschlüsselung aus. In der Tabelle der Standard-Walzen ist zu sehen, dass beispielsweise Walze I den Buchstaben A nach E, B nach K, C nach M überführt. Die Buchstaben A bis Z repräsentieren die Kontakte auf jeder Seite der Walze. Allerdings stehen die Buchstaben der Tabelle in keiner Weise in Zusammenhang mit der tatsächlichen Taste A der Enigma. Das A-Signal, aus dem Steckerbrett kommend, kann sehr wohl an Position X in die Walze eingehen – dies hängt nur von der relativen Position (der Verdrehung bzw. der Grundstellung) der Walze in der Maschine ab sowie von deren Ringstellung.

Standard-Walzen der Wehrmacht und der Kriegsmarine

```
Eingang   = ABCDEFGHIJKLMNOPQRSTUVWXYZ (rechte Seite)
            ||||||||||||||||||||||||||
I         = EKMFLGDQVZNTOWYHXUSPAIBRCJ
II        = AJDKSIRUXBLHWTMCQGZNPYFVOE
III       = BDFHJLCPRTXVZNYEIWGAKMUSQO
IV        = ESOVPZJAYQUIRHXLNFTGKDCMWB
V         = VZBRGITYUPSDNHLXAWMJQOFECK
```

Zusätzliche Walzen der Kriegsmarine (M3 und M4)

```
Eingang   = ABCDEFGHIJKLMNOPQRSTUVWXYZ (rechte Seite)
            ||||||||||||||||||||||||||
VI        = JPGVOUMFYQBENHZRDKASXLICTW
VII       = NZJHGRCXMYSWBOUFAIVLPEKQDT
VIII      = FKQHTLXOCBJSPDZRAMEWNIUYGV
```

Spezialwalzen der Kriegsmarine M4, genannt Zusatz- oder Griechenwalzen

```
Eingang   = ABCDEFGHIJKLMNOPQRSTUVWXYZ (rechte Seite)
            ||||||||||||||||||||||||||
Beta      = LEYJVCNIXWPBQMDRTAKZGFUHOS
Gamma     = FSOKANUERHMBTIYCWLQPZXVGJD
```

Die Umkehrwalze oder UKW spiegelt die Eingänge wieder auf der gleichen Seite zurück in die Rotoren (technisch ist es nur ein sog. Halbrotor). Alle Verbindungen werden paarweise gemacht: im Falle der Umkehrwalze B wird A auf Y abgebildet, woraus folgt, dass Y seinerseits auf A abgebildet ist. Der Vorteil dieser Anordnung ist, das Ver- wie Entschlüsselung reziprok sind, d.h. mit den gleichen Einstellungen erfolgen. Nachteilig ist hingegen, dass niemals ein Buchstabe auf sich selbst abgebildet werden kann, womit die Analyse der Maschine erheblich erleichtert wurde.

Standard-Umkehrwalzen der Wehrmacht und Luftwaffe

```
Kontakte  = ABCDEFGHIJKLMNOPQRSTUVWXYZ
            ||||||||||||||||||||||||||
B         = YRUHQSLDPXNGOKMIEBFZCWVJAT
C         = FVPJIAOYEDRZXWGCTKUQSBNMHL
```

Dünne Umkehrwalzen (nur Kriegsmarine M4)

```
 Kontakte  = ABCDEFGHIJKLMNOPQRSTUVWXYZ
             ||||||||||||||||||||||||||
B „dünn"   = ENKQAUYWJICOPBLMDXZVFTHRGS
C „dünn"   = RDOBJNTKVEHMLFCWZAXGYIPSUQ
```

Die hier angegebenen Verdrahtungen sind nur für die Wehrmacht (Heer und Luftwaffe) sowie die Kriegsmarine gültig. Andere Varianten der Enigma hatten andere Walzen.

Der Verschlüsselungsprozess der Walzen

Die Walze besteht aus zwei wesentlichen Teilen. Zunächst ist da der bewegliche äußere Ring mit dem aufgeprägten Alphabet (oder den Zahlen 01 – 26), die in den Sichtfenstern oben auf der Enigma angezeigt werden. Der Ring ist mit seiner Aussparung wesentlich für die Fortschaltung beim Drehen der Walzen verantwortlich. Des weiteren ist da der Walzenkern mit der internen Verdrahtung für die eigentliche Verschlüsselung und den 2 mal 26 Kontakten. Dieser Kern ist fest mit einer Rändelplatte als Daumenring verbunden, mit der die Grundstellung durch ein manuelles Verdrehen der Walzen eingestellt wird.

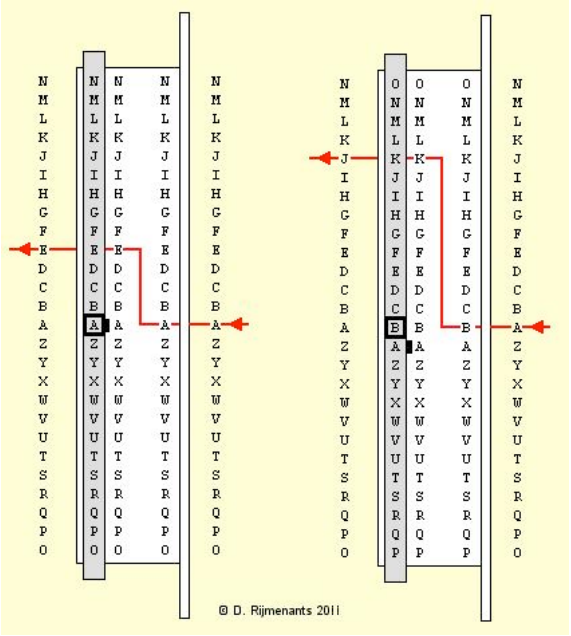

Abbildung 7: Verschlüsselung durch eine Walze
(Quelle: D. Rijmenants, mit Erlaubnis)

Verändert man die Position des äußeren Rings in Relation zum Kern, so spricht man vom Einstellen der Ringstellung.

In Abbildung 7 ist exemplarisch die Walze I dargestellt. Der äußere Ring ist durch die graue Spalte angedeutet. Weiß ist der Walzenkern sowie der fest damit verbundene Daumenring dargestellt. Die Buchstaben im weißen Feld dienen nur der Verdeutlichung;

auf der Walze sind tatsächlich keine Buchstaben angebracht. Die Grundstellung der Walze ist durch das kleine schwarze Fenster dargestellt. Das kleine schwarze Rechteck symbolisiert den Sperrstift für den äußeren Ring und zeigt somit die Ringstellung an.

Das Beispiel zeigt, wie Walze I (mit Ringstellung A-01) in der Abfolge zwei Buchstaben verschlüsselt. Links ist die Walze in Grundstellung A . Das Signal, das von der gedrückten Taste A kommt, erreicht die Walze hier in der A-Position, tritt am A-Kontakt ein und verlässt die Walze am E-Kontakt an der E-Position.

Rechts hat sich der Rotor in die B-Position weitergedreht. Wieder erreicht das Signal der gedrückten Taste A die A-Position, tritt dort aber in den B-Kontakt der (gedrehten) Walze ein und tritt an Kontakt K wieder aus. Da die Walze aber gegenüber dem linken Beispiel insgesamt um eine Position weitergedreht ist, wird der K-Kontakt auf der Ausgangsseite an der Position J zur nächsten Walze abgeführt.

Die Ringstellung wird auf den Walzen durch den Sperrstift (Wehrmacht) oder einen roten Punkt (Kriegsmarine) markiert. Diese Markierung identifiziert die Position des ersten Kontakts (A oder 01) des Walzenkerns. Ringstellung F oder 06 bedeutet also, dass der auf dem äußeren Ring aufgeprägte Buchstabe F an der Position A des Walzenkerns liegt. Die Veränderung der Ringstellung um eine Position verschiebt die Verschlüsselung um eine Position. Da die Aussparung fest mit dem äußeren Ring verbunden ist, ist die Schaltposition jedoch immer noch beim gleichen Buchstaben verblieben. Die Ringstellung darf nicht mit der Grundstellung verwechselt werden, die dem sichtbaren Buchstaben in dem kleinen Fenster der Enigma-Abdeckung entspricht.

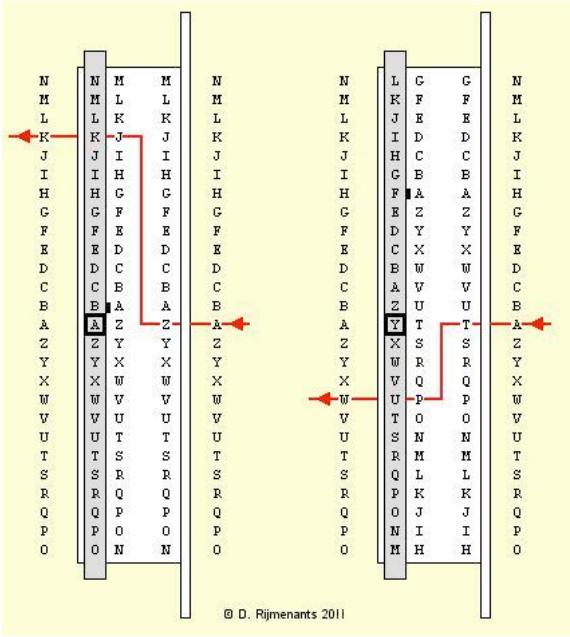

Abbildung 8: Verschlüsselung mit veränderter Ringstellung (Quelle: D. Rijmenants, mit Erlaubnis)

Abbildung 8 erläutert die Wirkung der Ringstellung. Im linken Bild ist Walze I mit Ringstellung B (oder 02, Markierung auf B) versehen, die Walzen befindet sich in Grundstellung A, d.h. A ist im Fenster der Enigma sichtbar. Das Signal erreicht die Walze an der A-Position, geht aber am Z-Kontakt hindurch und verlässt die Walze am Kontakt J. Aufgrund der Ringstellung ist der Walzenkern um eine Position verschoben, also auch die Ausgangskontakte. Daher befindet sich der Kontakt J an der Position K und erreicht somit an dieser Position die nächste Walze.

Im rechten Bild ist die gleiche Walze I, jetzt aber mit Ringstellung F (oder 06) dargestellt. Das an Position A ankommende Signal erreicht am T-Kontakt die Walze und verlässt sie am P-Kontakt. Aufgrund der Ringstellung ist der Walzenkern nun um sieben Plätze verdreht, daher liegt der P-Kontakt an Position W und das Signal erreicht dort die nächste Stufe.

Zur Erinnerung: wenn eine Taste niedergedrückt wird, schaltet die Mechanik die Walzen zunächst einen Schritt vorwärts. Daher muss, um den Signalfluss der Walze in Grundstellung A zu verfolgen, diese zuvor auf Z eingestellt sein. Dies gilt sinngemäß für alle Walzen, die durch den Tastendruck fortgeschaltet werden. Die obigen Beispiele sind

ohne jeden Stecker, d.h. alle Signale laufen direkt von der A-Taste zur Eingangswalze an Position A.

Der oben beschriebene Signalfluss geht von rechts nach links: das Signal, vom Steckerbrett kommend, erreicht die Walze am weitesten rechts, geht dann sukzessive durch die mittleren Walzen in die am weitesten links befindliche, von dort zur Umkehrwalze, zurück – diesmal von links nach rechts – über einen anderen Pfad durch die Walzen. Es liegt auf der Hand, dass damit eine sehr komplexe Verschlüsselung über mehrere Stufen vorgenommen wird. Ein Fortschritt der Walzen erzeugt für jeden weiteren Buchstaben eine vollständig andere Verschlüsselung.

Schrittmechanismus der Walzen

Jedesmal, wenn eine Taste gedrückt wird, ändert sich die Position der Walzen zueinander. Dadurch kommt jedesmal eine andere Substitutionschiffre zum Tragen. Die rechte, schnelle Walze schaltet jedesmal um eine Position weiter. Die mittlere Walze schaltet einmal alle 26 Schritte der rechten Walze, die linke, langsame Walze wiederum alle 26 Schritte der mittleren Walze.

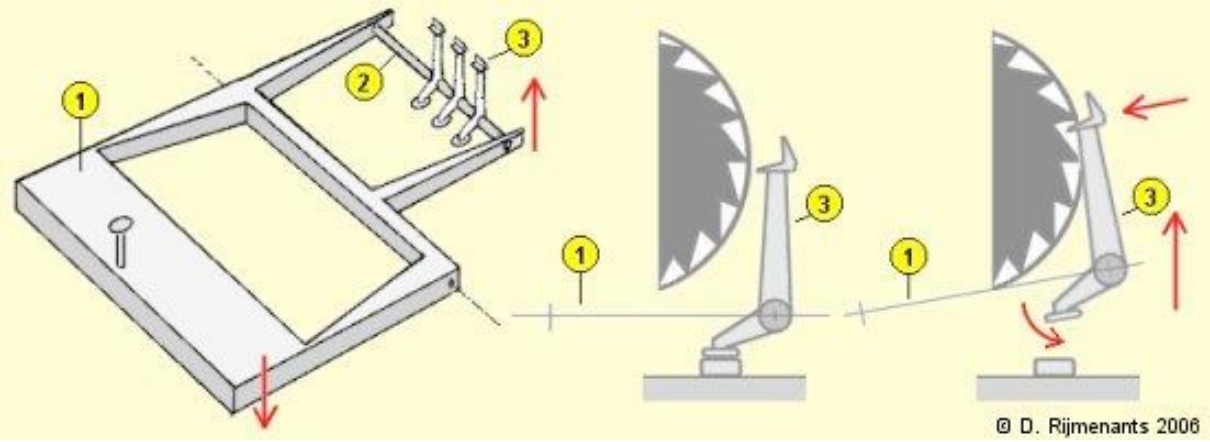

Abbildung 9: Der Schrittmechanismus der Walzen (Quelle: D. Rijmenants, mit Erlaubnis)

Durch das Drücken einer Taste wird die Schrittstange [1] nach unten gedrückt. Damit werden über die Klinkenachse [2] die gefederten Klinken [3] nach oben und vorne gedrückt. Jede Klinke drückt sich zwischen zwei benachbarte Walzen, sowohl gegen den Ring an der rechten als auch in den Zahnradmechanismus an der linken der beiden Walzen. Ist nun die Walze in der Schrittposition, so greift die Klinke sowohl in die Aussparung am Ring (rechts) als auch in einen Zahn der Walze links. Damit wird die linke Walze um einen Schritt weitergedreht. Ist die Walze nicht in der Schrittposition, so gleitet die Klinke über den Ring und erreicht das Zahnrad der linken Walze nicht, so dass sie nicht weitergedreht wird, da die Zahnräder nicht erreicht werden. Da auf der rechten Seite der ersten Walze keine Walze ist, kann die Klinke immer in das Zahnrad greifen, wodurch die erste Walze jedesmal weitergedreht wird.

Wird keine Taste gedrückt, so werden die Klinken [3] über die Achse [2] gegen Auflagen am Boden gedrückt, wodurch die Klinken von den Walzen abrücken. Dadurch können die Walzen in Ruhestellung durch den Bediener frei gedreht werden.

Jede Walze hat verschieden positionierte Aussparungen. Der nachfolgenden Tabelle kann entnommen werden, dass Walze I eine Aussparung am Buchstaben Y hat. Wenn also Y vor der Klinke steht, ist der Buchstabe Q im Fenster oben auf der Enigma sichtbar. Deshalb bewegt sich die Walze links davon, wenn sich Walze I von Q nach R dreht. Die Position der Schrittpositionen haben sich die Kryptoanalysten von Bletchley Park über

den Reim ROYAL FLAGS WAVE KINGS ABOVE gemerkt. Es ist bemerkenswert, dass die Kriegsmarine-Walzen VI, VII und VIII zwei Aussparungen haben. Damit drehen sich die Walzen doppelt so oft.

Rotor	Notch	Window	next left rotor steps when rotor steps from/to
I	Y	Q	Q -> R
II	M	E	E -> F
III	D	V	V -> W
IV	R	J	J -> K
V	H	Z	Z -> A
VI VII VIII	H + U	Z + M	Z -> A und M -> N

Wichtiger Hinweis zum Walzenfortschritt

Grundsätzlich scheinen sich die Walzen wie bei einem Kilometerzähler weiterzudrehen, die rechte Walze bei jedem Tastendruck, die anderen Walzen nach einer vollen Umdrehung der vorherigen Walze. Es gibt allerdings wegen der Klinken und Aussparungen einen wichtigen Unterschied. Die mittlere Walze schaltet ein zweites Mal weiter, wenn sich die erste Walze dreht und sich die mittlere Walze selbst in der Schrittposition befindet. Dies wird Doppelschritt (double step) genannt. Nachfolgend ein Beispiel der Schaltfolge, wenn die Walzen III – II – I benutzt werden:

KDO, KDP, KDQ, KER, LFS, LFT, LFU…

Wie man sehen kann, der Schritt Q nach R nimmt die mittlere Walze mit, die damit in die eigene Schrittposition kommt und beim nächsten Schritt die dritte Walze mitnimmt. Ursächlich dafür ist die Konstruktion der Klinken. Alle drei Klinken werden jedesmal gegen alle Walzen gedrückt. Jede Klinke bedeckt zur Hälfte den Ring mit der Aussparung an der rechten der beiden Walzen und das Zahnrad an der Walze zur linken. Der Ring verhindert, dass die Klinke ohne vorhandene Aussparung das Zahnrad zur linken erreicht und somit die höhere Walze mitnimmt. Ist eine Aussparung vor der Klinke, so wird die höhere Walze durch die Klinke mitgenommen, da sie in einen der 26 Zähne des Zahnrads greifen kann. Die Klinke greift aber auch in die Aussparung an der auslösenden Walze, die damit durch den festgesteckten Ring ebenfalls mitgenommen wird.

Eine Walze mit zwei Aussparungen löst auch zwei Doppelschritte pro Umdrehung aus.

Dieser Schrittmechanismus wird so bei der Wehrmacht und der Kriegsmarine verwendet. Die Vier-Walzen-Maschine M4 der Kriegsmarine ist direkt von der Wehrmachtsvariante abgeleitet worden, ohne den Schrittmechanismus zu verändern oder eine vierte Klinke hinzuzufügen. Daher dreht sich die vierte Walze nie. Andere Enigma-Varianten, wie die Enigma-G der Abwehr, haben einen völlig anderen Schrittmechanismus, eine mitdrehende Umkehrwalze und drei Walzen mit je mehreren Aussparungen. Die Weiterschaltung wurde über ein Getriebe gesteuert.

Das Steckerbrett

Im Jahr 1930 wurde das sogenannte Steckerbrett eingeführt. Das Steckerbrett befindet sich an der Vorderseite der Enigma. Ohne Stecker fließt der Strom von den Schaltern, die durch die Tasten angesteuert werden, direkt in die Eingangswalze. Wird ein Kabel

eingesteckt, so werden die beiden betreffenden Buchstaben vertauscht. Jede Enigma hatte standardmäßig 10 Kabel. Das Steckerbrett ist eine wichtige Verstärkung der kryptologischen Sicherheit.

An jeder Buchstabenposition am Steckerbrett befinden sich zwei Kontakte. Wird ein Stecker gesteckt, so wird die Verbindung zwischen dem oberen Kontakt, der zur Taste führt, und dem unteren Kontakt, der mit der Eingangswalze verbunden ist, unterbrochen. Das Kabel stellt dann eine Kreuzverbindung zum einem anderen Kontaktpaar her. Damit werden die Buchstaben effektiv vertauscht – die erste Taste führt über das Kabel zur Eingangswalze des anderen Steckers und umgekehrt. Das Steckerbrett wird – genau wie die Walzen – vom elektrischen Strom zweimal durchlaufen: einmal auf dem Weg von der Taste zu den Walzen, und erneut auf dem Rückweg von den Walzen zu den Lampen.

Zubehör

Eine praktische Einrichtung der Kriegsmarine-Enigma war der Schreibmax. Es handelt sich dabei um einen kleinen Drucker, der das Alphabet auf einem schmalen Papierstreifen drucken konnte. Damit konnte auf einen zweiten Funker verzichtet werden, der ansonsten die aufleuchtenden Lampen ablesen und notieren musste. Der Schreibmax wurde oben auf der Kriegsmarine-Enigma montiert und war mit den Lampen elektrisch verbunden: alle Lampen und die Abdeckung mussten dafür entfernt werden.

Abbildung 10: Enigma Uhr (Quelle: wikipedia, Creative Commons Lizenz)

Eine andere Erweiterung war das abgesetzte Lampenfeld. Wenn die Enigma damit ausgerüstet war, war der Koffer entsprechend größer. Es gab auch ein abgesetztes Lampenfeld, das nachträglich mit der Enigma verbunden werden konnte. Dieses musste aber, genau wie beim Schreibmax, mit allen Lampen einzeln verbunden werden. Das abgesetzte Lampenfeld ermöglichte einer Person, den entschlüsselten Text zu lesen, ohne dass der eigentliche Bediener dies auch konnte.

Im Jahr 1944 führte die Luftwaffe einen Umschalter für das Steckerbrett ein, genannt Uhr. Die Uhr war eine kleine hölzerne Kiste, die einen Umschalter mit 40 Positionen enthielt. Die Uhr ersetzte die ursprünglichen Stecker. Nachdem die Uhr-Stecker gemäß Tagesschlüssel mit der Enigma verbunden wurden, stellte der Bediener durch einfaches Drehen der Uhr auf eine der 40 verschiedenen Positionen jeweils eine andere Kombination von Steckerkombinationen ein. Die meisten Verbindungen der Uhr waren keine paarweise Vertauschungen.

Mathematische Sicherheit

Ein Maß für die mathematische Sicherheit der Enigma ist die Mächtigkeit der Menge aller Schlüssel (Schlüsselraum). Hierfür müssen alle verschiedenen Einstellungsmöglichkeiten berechnet werden. Dazu sind folgende Eigenschaften der Enigma beachtlich: die Auswahl und Anordnung der Walzen, deren Verdrahtung, die Ringstellung auf jeder Walze, die Anfangsposition der Walzen am Nachrichtenbeginn, die Umkehrwalze und das Steckerbrett. Es gibt nun verschiedene Möglichkeiten, die Anzahl der Kombinationen zu berechnen. In dieser Veröffentlichung der NSA (pdf) wurden alle möglichen Verdrahtungsalternativen jeder Walze berücksichtigt. Dann kommt eine gigantische Anzahl von ca. 3×10^{114} Schlüsseln heraus. Allerdings repräsentiert diese irreführenden Zahl alle theoretisch denkbaren Varianten der Walzenverdrahtung.

Die allierten Kryptoanalysten kannten jedoch die Maschine, die Walzen und deren innere Verdrahtung. Daher mussten sie nur die tatsächlichen Möglichkeiten zur Einrichtung der Maschine berücksichtigen, die tatsächliche Schlüsselmenge. Diese praktische Schlüsselmenge ist beträchtlich kleiner als die theoretische. Die deutschen Kryptologen hatten pro Walze $4x10^{26}$ Möglichkeiten zur Verdrahtung zur Verfügung, wodurch die obigen astronomischen Zahlen entstehen. Die alliierten Kryptoanalysten, die die Verdrahtung der Walzen jedoch kannten, mussten aber nur die 26 unterschiedlichen Anfangspositionen pro Walze berücksichtigen. Dadurch verkleinert sich der Schlüsselraum entsprechend dramatisch. Dies hat schon Auguste Kerckhoff formuliert: die Sicherheit eines Kryptosystems darf nicht auf dessen Geheimhaltung, sondern nur auf der Sicherheit des Schlüssels beruhen.

In the interesting R.A. Ratcliff paper for Cryptologia you can read how dangerous it is to rely on theoritical security – paper is missing.

Betrachten wir nun die tatsächlich veränderbaren Elemente der Enigma-Schlüsseleinstellungen. Als Beispiel diene die 3-Walzen-Enigma der Wehrmacht mit der Standard-Umkehrwalze B und den fünf Walzen I – V. Weiter werden 10 Stecker, die Standardanzahl, berücksichtigt.

Um 3 Walzen aus 5 auszuwählen, sind 60 Kombinationen möglich (5 x 4 x 3). Jede Walze kann in einer von 26 Anfangspositionen eingesetzt sein. Daher gibt es 17,576 verschiedene Anfangspositionen (26 x 26 x 26). Die Ringstellung verändert den angezeigten Buchstaben (hier ohne Bedeutung) und die Schaltposition für das Weiterdrehen der Walzen. Jeder Ring kann in einer von 26 Positionen eingestellt sein. Da links von der dritten Walze keine Weiterschaltung stattfindet, werden nur die Weiterschaltung der beiden anderen Walzen wirksam: 676 Kombinationen aufgrund der Ringstellung (26 x 26). Die 10 Steckerpaare ermöglichen 150,738,274,937,250 verschiedene Vertauschungen.

Insgesamt ergibt das: 60 x 17,576 x 676 x 150,738,274,937,250 = 107,458,687,327,250,619,360,000 oder 1.07×10^{23} Kombinationen für den Schlüsselraum. In der Realität konnte die Wehrmacht-Enigma also auf ungefähr 1.07×10^{23} verschiedene Weisen eingestellt werden, was einer Schlüssellänge von ungefähr 77 Bit entspricht.

Die maximale Periode der Walzen, d.h. die Anzahl der Schritte, bis wieder die Ausgangslage erreicht wird, ist etwas geringer als 17,576. Dies ist so wegen des weiter oben erläuterten Doppelschritts. Die tatsächliche Periode hängt von der Art der Walzen ab: die Walzen mit zwei Schrittpositionen verkürzen die Periode noch weiter. Da die

maximale Periodenlänge jedoch nicht Teil der einstellbaren Variablen ist, wird die Schlüssellänge davon nicht beeinflusst.

Die Wehrmacht-Enigma konnte mit den Umkehrwalzen B oder C bestückt werden. Normalerweise benutzten Funknetze immer die gleiche Umkehrwalze, da der Einsatz mehrerer solcher logistische, prozedurale und praktische Probleme mit sich brachte. Berücksichtigt man diese Variabilität jedoch, wird der Schlüsselraum nur verdoppelt (ein Bit mehr).

Die Einführung der vierten Walze der Kriegsmarine M4 war eine einfache, aber weitgehend nutzlose Erweiterung. Da die vierte Walze sich nicht bewegte, wurde lediglich ein Faktor 26 zum Schlüsselraum hinzugefügt. Zusammen mit der dünnen Umkehrwalze konnte die vierte Walze als eine einstellbare Umkehrwalze mit 26 Positionen betrachtet werden, deren Verdrahtung die Alliierten nach 10 panikerfüllten Monaten ermittelten. Die Einführung der 8 Walzen der Kriegsmarine M3 und später der M4 war bedeutend besser. Damit wurden die Walzenkombinationen von 60 auf 336 erhöht, mit zusätzlicher Komplexität aufgrund der Ringe mit zwei Schaltpositionen auf den Walzen VI – VIII.

Daraus folgt für den Schlüsselraum der M4: Hier werden 3 normale Walzen aus einer Menge von 8 ausgewählt (davon drei mit zwei Aussparungen im Ring). Das ergibt 336 Kombinationen (8 x 7 x 6). Die M4 hat weiter zwei Spezialwalzen Beta und Gamma für die vierte Position, was zwei weitere Wahlmöglichkeiten ergibt. Diese sind inkompatibel mit den normalen Walzen, können also nur an der vierten (äußerst linken) Position benutzt werden. Die vier Walzen können in 456,976 Positionen zueinander (26 x 26 x 26 x 26) eingestellt werden. Die Umkehrwalze wird bei der Berechnung des Schlüsselraums nicht berücksichtigt, da sie normalerweise nie gewechselt wurde. Die M4 hatte ebenfalls 10 Kabel.

Insgesamt ergibt das: 336 x 2 x 456,976 x 676 x 150,738,274,937,250 = 31,291,969,749,695,380,357,632,000 oder 3.1×10^{25}, vergleichbar mit einem 84 Bit Schlüssel.

Das ist etwa 291 mal stärker als die Wehrmacht-Enigma. Dies kommt im wesentlichen von der erhöhten Anzahl der Walzen, die jedoch bereits vor dem Krieg in der Marine-Version M3 benutzt wurden, und den denkbaren Grundstellungen von vier statt drei Walzen. Die vierte Walze hat, obwohl sie den Schlüsselraum tatsächlich vergrößerte, die Komplexität der Verschlüsselung nicht verbessert, da sie sich während der Verschlüsselung selbst nicht drehte. Eine deutlich bessere Lösung wäre die Einführung völlig neu verdrahteter Walzen zu bestimmten Zeitpunkten gewesen. Eine einzige Walze mit variabler Verdrahtung hätte den Schlüsselraum um gigantische $4x10^{26}$ Möglichkeiten vergrößert, deutlich mehr als durch die einstellbare Umkehrwalze mit ihren 7.8×10^{12} Möglichkeiten. Eine einzige, täglich gewechselte neu verdrahtbare Walze wäre viel effektiver gewesen als die hoch überschätzten Stecker mit ihren lediglich 2×10^{14} Möglichkeiten (immer paarweise).

Ein Kryptoanalyst würde die 17,576 Ringstellungen verwerfen. Auch mit völlig falschen Ringstellungen würde zu Beginn korrekter Text entschlüsselt werden. Sobald der Text unleserlich wird, wird der Ring der rechten Walze angepasst (26 Möglichkeiten) und dann erfolgt mit etwas Glück die korrekte Entschlüsselung von bis zu 676 nächsten Buchstaben. Im schlimmsten Fall muss nach 26 Buchstaben auch der Ring der mittleren Walze angepasst werden. Dies konnte alles während der eigentlichen Entschlüsselung durch einfaches Ausprobieren gelöst werden.

Unglücklicherweise für die Deutschen konnte die Turing Bombe durch gespiegelte identische Walzen das Steckerbrett bei der Suche nach sog. Cribs (bekannte Paare von Klar-und Schlüsseltext) ausschalten, was den Schlüsselraum um den Faktor 2×10^{24} verkleinerte.

Nichtsdestoweniger war das Brechen der Enigma eine enorme Herausforderung im Zeitalter der elektromechanischen Geräte. Mit einem praktischen Schlüsselraum von 1.07×10^{23} war eine vollständige Suche damals unmöglich, und die vergleichbare Schlüssellänge von 77 Bit ist auch für heutige Computer noch groß. Um einen Vergleich zu wagen: 1.07×10^{23} Blätter Papier reichen für ungefähr 70 Millionen Papiertürme, von denen jeder bis zur Sonne reicht. Für damalige Verhältnisse war die Enigma theoretisch sicher. Denn tatsächlich ist das Brechen von Codes eben mehr als nur die Mächtigkeit des Schlüsselraums und anderer Zahlenspielereien.