3.Ultra versus Enigma

3.1 Die Enigma, das System und seine Möglichkeiten

Die drahtlose Nachrichtenübermittlung erfolgt bei allen Streitkräften im Kriegsfall in der Regel in verschlüsselter Form, und die Wehrmacht machte da keine Ausnahme. Alle Wehrmachtsteile, darunter die Kriegsmarine und mit ihr die U-Boot-Waffe, setzten dabei bevorzugt auf das elektrisch-mechanische Schlüsselsystem Enigma. Da über diesen Komplex schon viel geschrieben wurde, beschränken wir uns hier auf eine kurze Darstellung der wichtigsten Grundzüge, soweit deren Kenntnis zum Verständnis der folgenden Ausführungen erforderlich erscheint.

Während die anderen Wehrmachtsteile und Behörden den ursprünglichen Handelsnamen "Enigma" verwendeten, sprach die Marine vom "Schlüssel M", wobei man unter Schlüssel M nicht allein die Enigma-Maschine zu verstehen hat, sondern im weiteren Sinn auch das zugehörige Schlüsselverfahren (die Programmierung der Maschine, wie man heute sagen würde).[1]

Die eigentliche Maschine ist mit einer Tastatur ausgerüstet und hat eine gewisse Ähnlichkeit mit einer Schreibmaschine. Der Klartext wird über die Tastatur eingegeben und der verschlüsselte Text auf einem Glühlampenfeld Buchstabe für Buchstabe abgelesen. (Bei der Entschlüsselung läuft derselbe Vorgang umgekehrt ab.) Die Verschlüsselung erfolgt auf elektro-mechanischem Weg über Tausch- oder Schlüsselwalzen, die ihrerseits mit verstellbaren Walzenringen ausgestattet sind. Bei jeder Eingabe eines Buchstabens, d.h. bei jedem Buchstabentausch, dreht sich die erste Walze um eine Position weiter, nach deren vollem Umlauf die zweite usw. Als zusätzliche Sicherung ist ein Steckerbrett mit 13 vertauschbaren Steckerverbindungen vorgesehen. Dadurch ergeben sich eine große Zahl von (Tausch-)Möglichkeiten.[2]

Zu jeder Maschine gehört ein Satz von 8 Walzen, die sich durch eine unterschiedliche innere Verdrahtung voneinander unterscheiden.[3] Von diesen wurden bei Betriebsbeginn jeweils 3 eingesetzt. Während die anderen Benutzer bei 3 Walzen blieben, ging die Kriegsmarine am 1. Februar 1942 aus Sicherheitsgründen auf eine 4-Walzen-Version über, Schlüssel M 4 genannt.

1 Hinter der Bezeichnung Schlüssel M verbergen sich drei unterschiedliche Modelle, die Schlüssel M 1, M 2 und M 3, die sich jedoch nur wenig voneinander unterscheiden.

2 Vgl. das Schaubild zur Funktionsweise der Enigma-Maschine in Anhang D.

3 davon drei besondere Walzen (VI bis VIII), die nur von der Kriegsmarine verwendet wurden

Bild 1 (Seite 42) zeigt die Walzen im Innern der geöffneten Maschine. Zum Schlüssel M 4 gehörte ein Satz von 12 Walzen, von denen 8 Tauschwalzen und 4 Umkehrwalzen waren. Der Übergang auf 4 Walzen war, wie wir noch sehen werden, von großer Tragweite.[4]

Vor Gebrauch des Schlüssels M wurde zunächst der gültige Tagesschlüssel eingestellt. Dazu wurden die Ringe an den Walzen gestellt (Ringstellung), dann die Walzen in der befohlenen Reihenfolge eingesetzt (Walzenlage), die Steckerverbindungen geschaltet und schließlich die Walzen in die Ausgangsposition (Grundstellung) gedreht.[5]

War der Tagessschlüssel eingestellt, wurde für jeden Spruch noch ein besonderer Spruchschlüssel verwendet, der mit Hilfe von sogenannten Kenngruppen gebildet wurde. Dieser wurde vor Spruchbeginn durch Verdrehen der Walzen eingestellt. Der Spruchschlüssel war Bestandteil des Funkspruchs und konnte von der Gegenstelle mit Hilfe der M.Dv. Nr.98 ("Kenngruppenbuch") ermittelt werden. Der Empfänger hatte damit die Startstellung der Walzen (Grundstellung) und konnte nun den Spruch entschlüsseln und im Klartext lesen.

Wie man sieht, ein sehr aufwendiges Chiffriersystem, das aufgrund seiner Konzeption und nicht zuletzt der großen Zahl von Tauschmöglichkeiten mit einigem Recht für einbruchssicher gehalten wurde. Daß es das dennoch nicht war, stellte sich im Lauf des Kriegs heraus. Aber die entsprechende Reaktion auf deutscher Seite blieb aus. Obwohl eine Fülle ernstzunehmender Verdachtsmomente, daß der Enigma-Schlüssel "geknackt" wurde, vorlag, wurde das Schlüsselverfahren nicht umgestellt. Die Folgerung, die Rohwer in [33] daraus zieht, spricht Bände.[6] Wie wir schon gesehen haben, wurde die Ursache für ein Versagen immer bei anderen gesucht. Es steht heute zweifelsfrei fest, welche fatalen Folgen das Beharren auf dem Enigma-Schlüssel für die Deutschen hatte.

Einer der Gründe für das offenbar unbegrenzte Vertrauen in die Einbruchssicherheit dieses Chiffriersystems war die Zahl von Tauschmöglichkeiten. Daß diese tatsächlich unvorstellbar groß war, geht aus einer Berechnung hervor, die der Elektronisch-Optische Betrieb der Königlich Niederländischen Marine (Marine Electronisch Optisch Bedrijf van de Koninklijke Nederlandse Marine/MEOB) in Oestgeest angestellt hat [47] und auf der die nachstehende Darstellung beruht.

4 Während Enigmas und Schlüssel-M-Geräte anfangs miteinander kommunizieren konnten, war das offenbar von einem gewissen Zeitpunkt an (1944?) nicht mehr oder nur mit Einschränkungen möglich. Vgl. dazu die einschlägigen Bestimmungen der M.Dv. Nr.32/1 ("Der Schlüssel M. Verfahren M Allgemein"), Ziffer 121 ff., in Anhang E.

5 Zu jedem Tagesschlüssel ("M Allgemein") gab es einen besonderen Schlüssel "M Offizier". Der nach dem Verfahren "M Allgemein" verschlüsselte Spruch wurde hier ein zweites Mal mit anderen Steckerverbindungen verschlüsselt.

6 Der Text ist in der Schlußbetrachtung im Wortlaut wiedergegeben.

Die Möglichkeiten der Enigma

angegeben ist die Zahl der Tauschmöglichkeiten (Buchstabentausch)

a. Das Steckerbrett

Zahl der Möglichkeiten mit n Steckerverbindungen
nach der Formel $26!/[n! \cdot (26-2n)! \cdot 2^n]$

Steckerverbindungen (n)	Tauschmöglichkeiten
0	1
1	325
2	44.850
3	3.453.450
4	164.038.875
5	5.019.589.575
6	100.391.791.500
7	1.305.093.290.000
8	10.767.019.640.000
9	53.835.098.190.000
10	150.738.274.900.000
11	205.552.193.100.000
12	102.776.096.500.000
13	7.905.853.580.550
0-13 Steckerverbindungen	532.985.208.200.000

b. Die drei Tausch- oder Schlüsselwalzen

Zahl der möglichen Reihenfolgen beim Einsetzen
- bei Auswahl aus einem Satz von 3 Walzen 6 Möglichkeiten
- bei Auswahl aus einem Satz von 5 Walzen 60 Möglichkeiten
- bei Auswahl aus einem Satz von 8 Walzen 336 Möglichkeiten

Zahl der Möglichkeiten beim Einstellen der Grundstellung
- bei einem Satz von 3 Walzen 17.576 Möglichkeiten

c. Die vierte Walze beim Marinemodell (=Schlüssel M 4, 1942-45)

Zahl der Möglichkeiten
- bei Auswahl aus einem Satz von 2 Walzen 2 Möglichkeiten
- beim Einstellen der Grundstellung 26 Möglichkeiten

*

Die Zahl der Tauschmöglichkeiten, mithin der Schlüssel, betrug danach für die Normalausführung der Enigma, wie sie von 1938 bis 1945 beim Heer Verwendung fand, mit einem Satz von 5 Walzen und Schaltung von 7 bis 11 Steckerverbindungen:

60 (Auswahl aus einem Satz von 5 Walzen) mal 17.576 (Einstellen der Grundstellung) mal 422.197.679.120.000 (Schaltung von 7 bis 11 Steckerverbindungen), also insgesamt 445.232.784.600.000.000.000 Möglichkeiten.

*

Die Zahl der Tauschmöglichkeiten, mithin der Schlüssel, für die Marineausführung der Enigma, die unter der Bezeichnung Schlüssel M 4 von 1942 bis 1945 Verwendung fand, betrug dagegen mit einem Satz von 8 Walzen, der zusätzlichen vierten Walze und Schaltung von 7 bis 11 Steckerverbindungen:

336 (Auswahl aus einem Satz von 8 Walzen) mal 17.576 (Einstellen der Grundstellung) mal 2 (Auswahl der vierten Walze aus einem Satz von 2) mal 26 (Einstellen der Grundstellung der vierten Walze) mal 422.197.679.120.000 (Schaltung von 7 bis 11 Steckerverbindungen), also insgesamt nicht weniger als 129.651.786.900.000.000.000.000 Möglichkeiten!

3.2 Die Enigma bei der Kriegsmarine

Bei der Kriegsmarine gab es anfangs nur eine beschränkte Anzahl von Schlüsselnetzen, also Funknetzen mit eigenem Tagesschlüssel, von denen die beiden wichtigsten Heimische Gewässer ("Hydra") und Außerheimische Gewässer ("Ägir") waren.[7] Das erste der beiden hatte eine Vielzahl von Nutzern: die Atlantik-U-Boote, die meisten Überwasserschiffe, die Küstenverteidigung und andere mehr. Dieser Zustand erschien der U-Boot-Führung aus Gründen der Geheimhaltung unbefriedigend. Auf ihr Drängen wurde am 5. Oktober 1941 ein besonderes Schlüsselnetz für die Atlantik-U-Boote eingeführt, Triton genannt (englischer Deckname "Shark" = Hai), und der U-Boot-Funkverkehr somit von anderen Funknetzen getrennt [49, S.235/236].

Im weiteren Kriegsverlauf ging man aus Sicherheitsgründen dann noch einen Schritt weiter und teilte jedem U-Boot einen individuellen Schlüssel zu. Im November 1944 fingen die Alliierten erstmals Funkverkehr auf, der sich solcher "Sonderschlüssel" bediente, und ab Februar 1945 wurde praktisch der gesamte operationelle Verkehr mit den Booten auf diese Weise abgewickelt. Wie wirkungsvoll diese (reichlich verspätete) Maßnahme vom deutschen Standpunkt aus war, wird daran deutlich, daß nur drei dieser Schlüssel "geknackt" werden konnten, und auch das nur für kurze Zeit [34, S.853].[8]

Vor dieser erst in der letzten Kriegsphase eingeführten Neuerung war der Tagesschlüssel für alle Boote, die sich zu einer gegebenen Zeit in einem bestimmten Seegebiet aufhielten, d.h demselben Schlüsselnetz angehörten, der gleiche. Dadurch war es möglich, den gesamten Funkverkehr nach Entschlüsselung im Klartext mitzulesen und sich aus den Meldungen der anderen Boote ein Bild von der Lage zu machen, was auch der Sinn dieser Betriebsordnung war. Das betraf allerdings nur den normalen Verkehr und nicht die mit "Offizier" gekennzeichneten Sprüche, die doppelt, d.h. ein zweites Mal, entschlüsselt werden mußten und deren Inhalt somit nur wenigen zur Kenntnis gelangte.[9]

Die Unterlagen für die zweite Entschlüsselung waren im Besitz des Kommandanten, vgl. die M.Dv. Nr.32/2 ("Der Schlüssel M. Verfahren M Offizier und M Stab"). Fritz Deters berichtete, daß er manchmal trotz dieser Vorsichtsmaßnahmen solche Sprüche mitlesen konnte, dann nämlich, wenn der Kommandant oder der als Funkoffizier eingeteilte Wachoffizier (I oder II WO) die Maschine nach der Dechiffrierung an den Funker zurückgab und dabei vergaß, die von ihm vorgenommene Einstellung rückgängig zu machen. Der Funker konnte jetzt, da er die Anzahl der Buchstaben oder Entschlüsselungs-"Schritte" des Spruchs kannte,

7 Zu diesem Thema vgl. u.a. [31, S.10], [48], [49]. 1939 scheint bereits ein eigenes Netz für die U-Boot-Ausbildung in der Ostsee ("Thetis") in Gebrauch gewesen zu sein.

8 Der Vollständigkeit halber sei angemerkt, daß für den 1. Mai 1945 noch eine Änderung geplant war, die den alliierten Kryptologen die Arbeit weiter erschwert hätte: die Einführung einer Mehrzahl von Enigma-Grundstellungen für jeden Tag anstelle einer einzigen [34, S.853], [50, S.121].

9 Für die alliierten Entschlüsselungsdienste stellten die Offizier-FTs ein großes Problem dar ("an excruciatingly difficult problem for much of the war" [51, S.502]).

die Maschine entsprechend zurückstellen und durch Eingabe des von ihm selbst ursprünglich entschlüsselten Texts den wirklichen Inhalt lesen.[10] Oftmals waren die übermittelten Informationen nicht von großer Wichtigkeit, wie etwa eine Beförderung oder ähnliches; es konnte aber auch vorkommen, daß ein neuer Einsatzbefehl erteilt wurde. Der Funker konnte dann aber sein Wissen nicht an seine Kameraden weitergeben, da er ja von solchen Meldungen keine Kenntnis haben durfte und eine Verbreitung des Inhalts seinen Verstoß gegen die Vorschriften offenbar gemacht hätte.

Nach den mir vorliegenden Auskünften wurde die innere Einstellung (Walzenlage und Ringstellung) jeweils um Mitternacht vorgenommen, die äußere Einstellung (Steckerverbindungen) um 12.00 h mittags. Ab 1.7.1942 erfolgte der Wechsel offenbar gleichzeitig um 12.00 h mittags. Deters teilte mir mit, daß die innere Einstellung zwar Offizierssache war, in der Praxis aber doch vom Funker, meistens einem Funkmaat oder Oberfunkmaat, vorgenommen wurde.[11] Die Durchführung dieser Anordnung hätte nämlich bedeutet, daß der zuständige Offizier seine jeweilige Tätigkeit als Wachoffizier um Mitternacht hätte unterbrechen bzw. hätte geweckt werden müssen, um die Maschine neu einzustellen. Im U-Boot-Betrieb galten sowieso eigene Regeln.[12]

Der Dienst der vier Funker an Bord war so geregelt, daß zwei von ihnen tagsüber jeweils 4 Stunden Wache und 4 Stunden wachfrei hatten, die zwei für nachts eingeteilten Funker lösten sich im 6-Stunden-Rhythmus ab. Man kann sich gut vorstellen, wie monoton der Alltag für die Funker bei einer 16wöchigen Feindfahrt war [54].

Es wird geschätzt, daß bei der Kriegsmarine etwa 20.000 Schlüssel-M-Geräte im Einsatz waren. Von diesen Schlüsselmaschinen dürfte es, einschließlich der bei den anderen Wehrmachtsteilen und Behörden verwendeten Enigmas, insgesamt an die 100.000 gegeben haben. Einige davon sind, wie auch die dazugehörigen Unterlagen, durch verschiedene Umstände bei Kriegsende der Vernichtung entgangen; man spricht von einigen Dutzend Enigma- und Schlüssel-M-4-Geräten, auch die Zahl von deutlich über hundert wird genannt. Viele dieser Maschinen sind in den vergangenen Jahren nach und nach zum Vorschein gekommen.

10 Daneben gab es offenbar noch andere Tricks, den Inhalt zu erfahren. Wolfgang Hirschfeld, ebenfalls ehemaliger U-Boot-Funker, schreibt: "Ich kann behaupten, daß uns Funkern auf U 109 in den zwei Jahren...kein M-Offizier unbekannt blieb" [52].

11 Er glaubt sich daran zu erinnern, daß sich zwei Schlüsselmaschinen an Bord befanden. War eine davon auf den bis Mitternacht gültigen, die andere auf den neuen Schlüssel eingestellt, so konnte man gegebenfalls fehlende FTs vom Vortag entschlüsseln, ohne die Maschine zurückzustellen.

12 Ein großes Problem bei der Wiedergabe historischer Sachverhalte ist, daß die persönlichen Erfahrungen der Beteiligten oft ganz unterschiedlich sind. Das wird auch in diesem Zusammenhang deutlich: Paul Tenholt [53] widerspricht Deters; daß beide auf unterschiedlichen Kriegsschauplätzen eingesetzt waren - Tenholt auf U 431 im Mittelmeer (1941-1944) und Deters auf U 313 und U 365 im Eismeer und im Atlantik - , könnte zur Erklärung dieser Diskrepanzen beitragen.

Das kann man von den Schlüsselunterlagen allerdings nur mit Einschränkungen sagen. Das ist auch verständlich, weil nach den damaligen Vorschriften der Tagesschlüssel nach Gebrauch zu vernichten war,[13] und ein Spruchschlüssel durfte nur ein einziges Mal benutzt werden. Darauf wurde im Schlüssel-M-Handbuch M.Dv. Nr.32/1 ausdrücklich hingewiesen.[14] Das erklärt auch die heute bestehende große Informationslücke, was die täglich vorzunehmenden Einstellungen des Schlüssels M angeht. Von Ausnahmen abgesehen, sind kaum Unterlagen über die Tagesschlüssel erhalten geblieben.[15]

Es war deswegen eine kleine Sensation, als durch einen glücklichen Zufall etwa 1980 in den Niederlanden einiges an deutschem Schlüsselmaterial aus der Kriegszeit auftauchte. Darunter befanden sich auch Kenngruppentafeln ("Doppelbuchstabentauschtafeln für Kenngruppen") zu M.Dv. Nr.98. Diese bestehen, wie bei den von der Kriegsmarine verwendeten Geheimpapieren mit eng begrenzter Gültigkeit üblich, aus Wasser aufsaugendem rosa Papier, das mit wasserlöslicher roter Tinte bedruckt ist. Aus den dort abgedruckten Tabellen wurden die bereits erwähnten Kenngruppen entnommen, die zur Bildung bzw. Auflösung des Spruchschlüssels notwendig sind. Siehe auch Anhang G.

3.3 Der große Gegenspieler: die Aktion Ultra

Schon vor dem Krieg versuchte man, hinter die Geheimnisse der Enigma zu kommen; damals waren es vor allem Polen und Frankreich, die entsprechende Anstrengungen unternahmen. Später verlagerten sich diese Tätigkeiten nach England. Dort wurde während des Kriegs zur Entschlüsselung der deutschen Funksprüche die streng geheime Aktion "Ultra" ins Leben gerufen, von der die Öffentlichkeit erstmals 1974 erfuhr. Zentrum des englischen Dechiffrierwesens war die Government Code and Cipher School (GC&CS) in Bletchley Park nordwestlich von London, abgekürzt BP.

Die Aktion Ultra umgab eine Mauer des Schweigens, die bis heute nicht vollständig abgebaut ist. Oberstes Gebot war ein äußerst vorsichtiger Umgang mit den bei der Entschlüsselung gewonnenen Erkenntnissen, damit niemals, unter keinen Umständen, bekannt wurde, aus welcher Quelle sie stammten. Um äußerste Verschwiegenheit zu erreichen, wurde der Kreis der Eingeweihten streng begrenzt. Wenn in Einzelfällen die Informationen einem weiteren Kreis zugänglich gemacht werden mußten, wurde ihre Herkunft sorgfältig verschleiert. Der Schutz dieser Quelle ging so weit, daß man annehmen kann, daß mancher U-Boot-Versorger der Vernichtung zeitweise nur dadurch entgangen ist, daß noch größere Verluste dieser Boote die deutsche Führung mißtrauisch gemacht hätten.

13 M.Dv. Nr.32/3 ("Der Schlüssel M. Allgemeine Bestimmungen"), Ziffer 59.

14 Vgl. Anhang E, die Ziffern 43, 46, 135 und 136.

15 Ein Parameter des Tagesschlüssels ist bekanntlich die Schaltung der Steckerverbindungen. Aus Anhang F sind die Steckerverbindungen für den Monat Mai 1945 zu entnehmen. Die durchgestrichenen Positionen zeigen, daß diese Anweisung bis einschließlich 7. Mai 1945 in Gebrauch war.

Anzeichen deuten darauf hin, daß es den Engländern bereits im Mai 1940 gelang, Teile des Enigma-Verkehrs der Luftwaffe laufend zu dechiffrieren. Der von der Kriegsmarine verwendete Schlüssel, der bestimmte Schwachpunkte der einfacheren Luftwaffenversion nicht kannte, erwies sich für die englischen Kryptologen als eine härtere Nuß. Zunächst gelangen hier nur spärliche Einbrüche, und erst im Frühjahr 1941, als die auf U 110 gemachte Beute ihr Geheimnis preisgegeben hatte, begann eine Phase mehr oder weniger systematischer und regelmäßiger Dechiffrierung der Funksprüche der Marine.[16]

Aus englischen Quellen geht hervor, daß nach Einführung der 4-Walzen-Enigma im Februar 1942,[17] die nur kurze Zeit nach dem Übergang auf den Schlüssel "Triton" erfolgte, Bletchley Park dann wieder vollkommen "blind" war, also den deutschen Funkverkehr nicht mehr mitlesen konnte [49]. Erst im Dezember desselben Jahrs konnten die Engländer wieder zunehmend in den Funkverkehr des B.d.U. "einbrechen".[18] Bis dahin vergingen etwa 10 Monate, in denen sich die U-Boote in relativer Sicherheit wähnen konnten. Es ist daher verständlich, wenn man auf alliierter Seite die Einführung des Schlüssels M 4 als das hervorstechende Ereignis der deutschen Kryptographie im Zweiten Weltkrieg bezeichnet hat [45, S.210).

Wie Bletchley Park überhaupt hinter die Geheimnisse der Enigma-Maschine kam, war lange Zeit in Nebel gehüllt. Da war natürlich die Erbeutung von Maschinen bzw. ihren Teilen (Walzen) und von Schlüsselmaterial (Einstellungen, Codetabellen usw.) bei verschiedenen Gelegenheiten - von Hardware und Software nach heutigem Sprachgebrauch - , aber das reicht zur Erklärung nicht aus. Denn von Haus aus war das Chiffriersystem so angelegt, daß es auch bei Aufdeckung einiger Betriebsdaten als "einbruchssicher" gelten konnte; dazu trug auch der häufige Wechsel der Schlüsselelemente bei. Wie man heute weiß, lagen die wesentlichen Schwächen der Enigma weniger im System selbst begründet als vielmehr in dessen Handhabung, im "human factor".

Die Arbeitsweise von Bletchley Park läßt sich nicht in einigen Sätzen beschreiben, hierfür sei auf die einschlägige Literatur verwiesen, wie etwa [45] und [50], um nur zwei Standardwerke zu nennen.

Unter großem Einsatz von Menschen und Material - in BP waren 1944 mehr als 7.000 Personen tätig - wurden hier von englischen Kryptologen und ihren Hilfskräften verschiedene methodische Ansätze entwickelt, um in den Schlüssel M einzudringen. Ein Ansatz bestand darin, über erbeutete bzw. rekonstruierte Doppelbuchstabentauschtafeln Rückschlüsse auf die

16 Was den U-Boot-Krieg anbelangt, so wurden die dabei gewonnenen Erkenntnisse anfänglich nur dazu genutzt, Geleitzüge um Aufstellungen von U-Booten herumzuführen; eine offensive Nutzung erfolgte erst in einer späteren Kriegsphase [55, S.81/82].

17 Der Schlüssel M 4 wurde unter der Typenbezeichnung MZSS, Na 220.900, geführt. Die 4-Walzen-Maschinen tragen Prüfnummern von M 2802 an aufwärts, wie aus der M.Dv. Nr.32/1, Ziffer 47, hervorgeht, vgl. Anhang E.

18 nach der Erbeutung von Schlüsselunterlagen von U 559 im Oktober 1942

verwendeten Kenngruppen zu ziehen, was die Maschinenlaufzeiten verkürzen konnte.[19] Dazu muß man wissen, daß BP versuchte, die jeweilige Walzenstellung mit Hilfe von aufwendigen elektromechanischen Vorrichtungen ("bombe" in Anlehnung an die Bezeichnung "bomba" für das polnische Vorgängermodell) zu ermitteln.

Eine andere Methode wurde dort praktiziert, wo man annehmen konnte, daß sich hinter einem Enigma-Text ein bestimmter Klartext verbarg; oftmals ging es dabei nur um einzelne Buchstaben oder ein einziges Wort. Nehmen wir an, den Engländern war aus der Funkbeobachtung bekannt, daß eine Funkstelle täglich zur gleichen Zeit eine Meldung an den F.d.U. West absetzte, sie konnten also vermuten, daß der Spruchbeginn "An F.d.U. West..." lautete. Oder eine Landfunkstelle hatte mehrere Tage hintereinander keine besonderen Vorkommnisse zu melden. Die Sprüche werden sich dann bei dem stereotypen Charakter solcher Meldungen von Tag zu Tag wenig oder gar nicht voneinander unterschieden haben, was einen Ansatz zur Auflösung des Schlüssels eröffnete. Die Bletchley-Leute sprachen in diesem Fall von "cribs".[20]

Viele "cribs" stammten aus identischen oder nahezu identischen Funksprüchen, die gleichzeitig mit der Enigma und einem anderen, leichter zu lösenden Schlüsselsystem gesendet wurden (im Bletchley-Jargon "kisses" = Küsse genannt). Ein Beispiel dafür sind Meldungen, die mit dem Schlüssel M an U-Boote und mit dem Werftschlüssel nach M.Dv. Nr.103, einem einfacheren Handschlüsselverfahren, an andere Einheiten gingen. Hier gab der Klartext der Werftschlüssel-Meldung Hinweise auf den vermutlichen Klartext der Enigma-Meldung, was die Möglichkeit bot, an die Enigma-Einstellung "heranzukommen".

Die Wiederholung identischer oder fast identischer Sprüche mit unterschiedlicher Einstellung der Enigma oder bei Gebrauch verschiedener Schlüsselsysteme war zweifellos ein Schwachpunkt des Systems.[21] Sicherlich haben sich hier manche Funker die Sache leichtgemacht. Andererseits ist bekannt, daß auf diesem Gebiet die Disziplin in der Kriegsmarine von allen Wehrmachtsteilen noch am größten war, gerade weil sich der Funkverkehr der Kaiserlichen Marine im Ersten Weltkrieg als nicht abhörsicher erwiesen hatte. Aber im Lauf des Kriegs waren viele erfahrene Funker gefallen, und der Ausbildungsstand der Nachrückenden sank immer mehr.

19 Diese anfänglich gebrauchte, sehr arbeitsintensive Methode, der sogenannte Banburismus, wurde später aufgegeben. Die Bezeichnung stammt daher, daß bei diesem Verfahren das Papier, in das der Schlüsseltext zur Auswertung "eingelocht" wurde, in der Ortschaft Banbury hergestellt wurde.

20 Der Begriff ist schwer übersetzbar. Gemeint ist vorhandenes Material in Text- oder in anderer Form, das Anhaltspunkte zum Brechen eines Schlüssels oder einer verschlüsselten Meldung liefern kann. Abgestellt wird dabei auf vermutete Übereinstimmungen im Aufbau, im behandelten Gegenstand oder im Ausdruck. Vgl. [50, S.XV].

21 Ein anderer Schwachpunkt, der im Schlüsselverfahren selbst begründet war, bestand darin, daß bei der Verschlüsselung ein Buchstaben niemals in sich selbst verschlüsselt wurde, will sagen, daß ein "a" im Klartext nie ein "a" im Schlüsseltext ergeben konnte.

Die Schlüsselsicherheit wurde durch entsprechende Geheimhaltungsbestimmungen geschützt.[22] Der Schlüssel M selbst war Geheimsache bzw. geheime Kommandosache.[23] Schriftliche Schlüsselmittel wie die einschlägigen Marine Dienstvorschriften oder die Kenngruppentafeln galten als geheime Gegenstände nach § 88 RStGB.

3.4 Ein Beispiel für Ultra-Ergebnisse

Nachdem einzelne Angehörige der ehemaligen Kriegsmarine die entscheidende Rolle von Ultra noch immer mit Entschiedenheit abstreiten,[24] sei hier (nächste Seite) ein Funkspruch wiedergegeben, der in Bletchley Park entschlüsselt und ins Englische übersetzt wurde. Gegenstand ist der Befehl an die U-Boot-Kommandanten Marbach und Brauel, in bestimmten, genau bezeichneten Seegebieten/Marinequadraten Position zu beziehen. Hier sei angemerkt, daß die Marinequadrate aus Gründen der Sicherheit ihrerseits verschlüsselt wurden.[25]

Zur Erläuterung: ZIP und ZTPGU rechts oben bedeuten, daß der Spruch über Bletchley Park lief, 17.621 ist seine Nummer.[26] Absender ist die Naval Section (NS), die Abteilung von Bletchley Park, die für Marineangelegenheiten zuständig war. ADM (3) scheint nichts anderes zu besagen, als daß 3 Kopien an die Admiralität gingen, nämlich an I D 8 G, das Operational Intelligence Centre (OIC), den Geheimen Nachrichtendienst der Admiralität. Der Spruch wurde am 8. Oktober 1943 um 11.26 h GMT von einer der britischen Abhörstationen (Y-Stationen) aufgefangen (TOI = time of interception = Aufnahmezeit). Er ging an demselben Tag um 12.03 h in Bletchley Park ein (TOO = time of origin = Eingangszeit) und wurde

22 Diese sind in der M.Dv. Nr.32/3, Ziffern 50-70, niedergelegt.

23 laut M.Dv. Nr.32/1, Ziffer 111, in Anhang E bzw. M.Dv. Nr.32/3, Ziffer 68

24 Im September 1981 besuchte der Verfasser auf Einladung der "Vereinigung noch funkender Marinefunker" deren Jahresversammlung in Kassel und hat bei dieser Gelegenheit mit den Anwesenden ausgiebig über das Marine-Funkwesen diskutiert. Selbst zu dieser Zeit waren noch manche ehemalige Marine-Funker fest davon überzeugt, daß die Veröffentlichungen über Ultra nach 1974 "großer Unsinn" waren, denn für sie war der Schlüssel M einfach nicht zu knacken, punktum!

25 Die Verschlüsselung erfolgte mit Hilfe des sogenannten Adreßbuchs. Einzelheiten sind in [56] beschrieben.

26 Die entschlüsselten Funksprüche wurden fortlaufend numeriert, beginnend in Mai 1941, als man mit der Erbeutung der Enigma-Unterlagen von U 110 mit einer systematischen Entschlüsselung beginnen konnte. Anfänglich benannte man die Sprüche mit ZTP 1, ZTP 2 usw., wobei Z bedeutet, daß das Material aus einem Maschinenschlüssel, keinem Handschlüssel, gewonnen wurde. TP steht für Teleprinter = Fernschreiber, die Art der Übermittlung. Bald sah man sich durch die Fülle des anfallenden Materials veranlaßt, eine Auffächerung vorzunehmen und neue Serien einzuführen: ZTPG (G für German), ZTPGU (U für U-Boot) usw. Bei Kriegsende gingen die Nummern in diesen Serien in die Tausende. So wurden bereits am 16.6.1944 ZTPG 255.617 und am 22.6.1944 ZTPGU 26.830 erreicht!

nach Bearbeitung am 9. Oktober um 06.10 h an die Admiralität weitergeleitet; die Entschlüsselung nahm also etwas mehr als 18 Stunden in Anspruch. Der Funkspruch wurde auf 7.770 kHz gesendet. Die Briten gebrauchten als Zeitangabe immer GMT, so wie die Deutschen DGZ gebrauchten, selbst im Funkverkehr mit Booten, die etwa in der Straße von Malakka operierten.[27]

ADM(3)

TO I D 8 G ZIP/ZTPGU/17621

FROM N S

7770 KC/S T O O 1203 T O I 1126/8/10/43

K[28]

1) MARBACH IS TO OCCUPY THE SEA AREA BOUNDED BY THE LATITUDE AND LONGITUDE OF SQUARE GRUEN RH 7125 AND SQUARE GRUEN LD 1878.
W/T SERVICE REMAINS THE COASTAL SERVICE.

2) BRAUEL IS TO OCCUPY THE SEA AREA BOUNDED BY THE FOLLOWING POINTS: SQUARE 6897, 8579, 1919, ALL GRUEN FL AND SQUARE GRUEN VH 3261.
W/T SERVICE IN THIS AREA IS IRELAND.

CC FIRST GRP - MARBACH

0610/9/10/43+CEL+DJL

Der Spruch ist im britischen Dokumentationszentrum, dem Public Record Office (PRO) in Kew, London, im Verzeichnis DEFE 3 registriert.

Um auf die mancherorts skeptische Einstellung zu der Rolle, die Ultra gespielt hat, zurückzukommen: Es ist nicht immer leicht, liebgewonnene Vorstellungen aufzugeben, die man über viele Jahre gepflegt hat, aber das liegt in der menschlichen Natur. Schon von Clausewitz hat das vor nahezu 200 Jahren erkannt und formuliert. Er hat seine Feststellungen gewiß nicht ohne Grund getroffen, und insoweit haben sich die Menschen nicht geändert.

Werfen wir noch einen Blick auf die Rolle der Funkaufklärung auf deutscher Seite. Bonatz beschreibt in [57] und [58], wie ein Großteil des Funkverkehrs der britischen Marinestreitkräfte bis 1942 entschlüsselt und mitgelesen werden konnte. Die daraus gewonnenen Erkenntnisse wurden natürlich unter anderem auch vom B.d.U. dazu genutzt, um die U-Boote

27 Im St.Kr.Bef. des B.d.U. Nr.200 ("Der U-Bootsfunkdienst") zu M.Dv. Nr.97 heißt es: "**Alle Uhrzeiten** in Befehlen und Funknachrichten rechnen nach **deutscher gesetzlicher Zeit** (DGZ), wenn nicht ausdrücklich anders vermerkt." An Bord gab es demzufolge zwei Zeitangaben: die DGZ für den Funkverkehr und die jeweils geltende Orts-/Zonenzeit für Navigationszwecke.

28 Ralph Erskine macht mich darauf aufmerksam, daß der Buchstabe "K" auf vergleichbaren Dokumenten nicht figuriert. Es könnte sich demnach um einen Tipp- oder Übertragungsfehler handeln.

über die Bewegungen der Geleitzüge zu informieren. Irgendwann im Jahr 1943 kamen beim xB-Dienst, wie die Funkaufklärung auch genannt wurde, der Verdacht auf, daß die Engländer (tief) in den deutschen Funkverkehr eingedrungen waren, da einzelne Meldungen, die an die Geleitzüge übermittelt wurden, nur aus (entschlüsselten) deutschen Funksprüchen stammen konnten. Wie bereits angedeutet, kam man nach einer internen Untersuchung zu dem Ergebnis, daß die Briten/Alliierten unmöglich den Schlüssel M "geknackt" haben konnten und, falls das wirklich der Fall gewesen sein sollte, der zeitliche Aufwand für die Dechiffrierung viel zu groß wäre, um dem Gegner noch strategische Vorteile bieten zu können [59].

Die Briten kamen ihrerseits im Verlauf des Jahrs 1943 durch Ultra dahinter, daß die Deutschen in ihr eigenes Codesystem eingedrungen waren. Sie änderten daraufhin kurzfristig ihr System und brachten damit eine wichtige Quelle für die Deutschen zum Versiegen. Das neue System, ein einmalig zu verwendender Schlüssel, "one-time pad" genannt, war kaum aufzulösen, obwohl es Mitte 1944 gelang, auch hier gewisse Einbrüche zu erzielen [57],[58].

3.5 Enigma - offene Fragen

Um soweit wie möglich auf praktische Erfahrungen von Zeitzeugen zurückgreifen zu können, hat der Verfasser über die Marine-Funk-Runde e.V. (MF-Runde) einen Fragebogen an eine Reihe von Sendeamateuren verschickt, die während des Kriegs als Funker auf U-Booten Dienst getan haben. Die dabei von Horst Werner geleistete Hilfe war unschätzbar, wie das Echo auf diese Aktion zeigt [60]-[63].

Eine Frage lautete, ob die Befragten Auskunft über den Einsatz eines geheimnisvollen Zusatzgeräts, "Schreibmax" genannt, an Bord geben könnten.[29] Die Antworten waren mit zwei Ausnahmen negativ, was aber nicht dagegen spricht, diese beiden hier zu berücksichtigen [53],[60]. Der fragliche Zusatz hat mit der eigentlichen Ver- oder Entschlüsselung nichts zu tun, er stellt vielmehr eine Erleichterung bei der Bearbeitung von Schlüssel-M-Sprüchen dar, die sich damit schneller und dadurch effizienter bearbeiten ließen. Und zwar wurde hier anstelle des Glühlampenfelds für die Anzeige des verschlüsselten Texts bzw. des Klartexts eine Druckereinheit angeschlossen, die auf einem Papierstreifen die entsprechenden Buchstaben ausdruckte.

Die Folge der Bilder 2 bis 5 zeigt die Herrichtung des Schlüssels M 4 für die Verwendung des Schreibmax. In Bild 2 befindet sich die Maschine in ihrem normalen Zustand. In Bild 3 ist der Deckel abgenommen (d.h. nach der Seite herausgeschoben) und die Abdeckung des Glühlampenfelds mit den transparenten Buchstaben abgenommen. In Bild 4 sind die Glühlampen herausgeschraubt und anstelle des Deckels der Schreibmax eingeschoben. In Bild 5 ist der Schreibmax heruntergeklappt und verriegelt. Die an dessen Unterseite angebrachte Kontaktleiste (vgl. Bild 4) stellt die Verbindung zu den Fassungen der Glühbirnen her. Statt eine bestimmte Lampe zum Aufleuchten zu bringen, wird jetzt ein tintengetränktes Typenrad so weit gedreht, bis die gewünschte Position (der gewünschte Buchstabe) eingestellt ist. Dann wird ein Hämmerchen ausgelöst, das mit einem kräftigen Anschlag den Buchstaben auf einen Papierstreifen von 11,5 mm Breite druckt.

29 Schreibzusatz MZSE, Na 220.920

Bild 5: *Der Schlüssel M 4 mit aufgesetztem Schreibmax*

Das Gerät selbst war äußerst kompliziert, hatte aber einen großen Vorteil: Während normalerweise zwei Mann zur Bedienung nötig waren - der eine tippte den Text des Funkspruchs in die Maschine, der zweite notierte die aufleuchtenden Buchstaben - , wurde der zweite Mann durch diese Mechanik entbehrlich, und das sowohl beim Ver- wie beim Entschlüsselungsvorgang.

Fritz Deters bemerkt zu diesem Thema, daß die in der U-Boot-Waffe eingesetzten Geräte und Verfahren nicht einheitlich waren und somit durchaus Unterschiede in der Ausrüstung von Boot zu Boot bestanden haben; das würde die unterschiedlichen Antworten auf meine Frage nach dem Schreibmax erklären.

Eine andere Frage galt dem Gebrauch der sogenannten "Enigma-Uhr", auch als "Gerät E.U." bezeichnet, vgl. Bild 6. Das war ein Kästchen, das einen Drehschalter mit 40 Schaltstellungen und zwei Sätze mit jeweils 10 Kabeln enthielt. Das eine Ende der Kabel war mit "xa", das andere mit einem roten "xb" gekennzeichnet, wobei x für die Nummer des Kabelsatzes steht. (Die Kabel eines Satzes trugen die gleiche Nummer und konnten so nicht verwechselt werden.) Zweck des Geräts war ein schneller Wechsel der Kabelverbindungen im Steckerbrett mit Hilfe eines in dem Kästchen fest verdrahteten Algorithmus. Mit der Schalterstellung 00 war es möglich, dieses System zu umgehen und die Kabel als normale Verbindungen durchzuschalten.

Das Typenschild der erhalten gebliebenen Enigma-Uhren gibt u.a. Auskunft darüber, ob das betreffende Gerät für das Heer (H) oder die Luftwaffe (L) bestimmt war; die Frage nach der Benutzung auch in der Kriegsmarine ergab keinerlei Aufschlüsse. Fast alle bekannten Enigma-Uhren stammen aus Funden in Norwegen, so auch das abgebildete Exemplar. Vermutlich wurden die Geräte in Funkzentralen verwendet, wo man im Verkehr mit nachgeordneten Stellen schnell unterschiedliche Kabelverbindungen schalten mußte. Aber die Anzahl der Schaltmöglichkeiten war begrenzt (insgesamt 39). Auch ob die "Uhren" mit anderen als den gewöhnlichen Heeres- und Luftwaffen-Enigmas zusammen eingesetzt wurden, ist nicht bekannt.