Edition TMW

Geheimsache Enigma

Geschichte und Kryptologie der legendären Verschlüsselungsmaschine

Wolfgang Pensold, Otmar Moritsch

technisches museum wien

Geheimsache Enigma

Geschichte und Kryptologie der legendären Verschlüsselungsmaschine

Herausgeber: Technisches Museum Wien mit Österreichischer Mediathek
Koordination: Stephan Schulz
Autor/Redaktion: Wolfgang Pensold, Otmar Moritsch
Grafik: Ursula Emesz
Fotografien: Gerhard Sedlaczek

1. Auflage, 2018

ISBN 978-3-903242-11-1

Edition TMW

Geheimsache Enigma

Geschichte und Kryptologie der legendären Verschlüsselungsmaschine

Wolfgang Pensold, Otmar Moritsch

Wien 2018

Inhalt

1 *„Immer und immer wieder spielt in Politik und Heerwesen, in Krieg und Frieden, in Industrie und Handel die geheime Uebermittlung wichtiger Nachrichten eine große Rolle. Entscheidende Schlachten zu Wasser und zu Lande und am grünen Tisch im Verhandlungssaal sind verlorengegangen, weil der Gegner über bessere Mittel zur Geheimhaltung verfügte, oder weil er die geheimen Nachrichten des anderen wegen Mangels einer zuverlässigen Methode entziffern konnte, oder weil die mühsamen handschriftlichen Systeme zu langsam die Nachrichten lieferten und bei starker Beanspruchung völlig versagen mußten."*

Aus einer Werbebroschüre für die Verschlüsselungsmaschine Enigma; Chiffriermaschinen Aktiengesellschaft, Berlin.

Vorwort

Der Band 9 der Edition TMW, der sich der legendären deutschen Verschlüsselungsmaschine Enigma widmet, erlebt seine zweite Auflage. Die geheimnisumwitterte Maschine, die während des Zweiten Weltkrieges gewährleisten musste, dass deutscher militärischer Funkverkehr zu Land und auf See von der Gegenseite nicht mitgelesen werden konnte, stößt auf reges Interesse. Nicht weniger gilt dies für die Versuche polnischer und französischer, später auch britischer und amerikanischer Mathematiker, die Codes der Enigma zu knacken. Allzu oft war dies ein Wettrennen auf Leben und Tod. Mit Mitteln der Spionage, militärischen Beutezügen, vor allem aber kryptologischem Genie und elektronischen Rechenmaschinen rangen die Alliierten der Enigma letztlich ihr Geheimnis ab.
In der jüngeren Vergangenheit wurde die Enigma zum Hauptdarsteller in Bestseller-Romanen und erfolgreichen Kinofilmen. Darüber hinaus entwickelte sie sich zu einem gefragten Sammlerobjekt. Obwohl im Zuge des Zweiten Weltkrieges geschätzte 100.000 bis 200.000 Exemplare gefertigt wurden, ist sie heute vergleichsweise rar. Das liegt daran, dass die mit ihr befassten Nachrichtensoldaten zu Kriegsende angewiesen waren, ihre Exemplare zu zerstören oder in einem Gewässer zu versenken, damit sie nicht in die Hände der Gegner fielen. Aus diesem Grund werden bis heute verrostete Enigmas durch Taucher aus Seen oder aus dem Meer geborgen. Gelegentlich finden sich auf Dachböden vollkommen unversehrte und intakte Exemplare, die der systematischen Vernichtung aus welchen Gründen auch immer entgangen sind. Solche Stücke werden mittlerweile um sechsstellige Eurobeträge versteigert.
Das Technische Museum verfügt über drei Enigmas, von denen eine auf Ebene 4 des Hauses in den medien.welten dauerhaft ausgestellt ist. Direkt daneben befindet sich eine interaktive Medienstation, die Interessierten Schritt für Schritt Bedienung und Funktionsweise der Maschine nachzuvollziehen erlaubt, und der vorliegende Band „Geheimsache Enigma“ liefert dazu eine umfassende Hintergrundgeschichte samt kryptologischer Sezierung ihrer Schlüssel.

Peter Aufreiter
Generaldirektor Technisches Museum Wien

GESCHICHTE


30.

Pionierära: Marian Rejewski und die Enigma

Nach Jahren erbitterter Materialschlachten mit Millionen von Opfern endet im Herbst 1918 der Erste Weltkrieg mit einer Niederlage der Mittelmächte. In Deutschland wie in Österreich-Ungarn stürzt die monarchistische Staatsform und die Republik tritt an ihre Stelle. Im allgemeinen Chaos lösen sich die Armeen auf, doch beginnt die deutsche Oberste Heeresleitung umgehend mit der Bildung von Freiwilligenverbänden. Diese so genannten *„Freikorps"* führen in weiterer Folge im Osten einen irregulären Grenzkrieg gegen sowjetrussische und polnische Truppen. Kommandiert werden sie von Offizieren der alten kaiserlichen Armee, die die nunmehrige Republik und insbesondere die von ihr ausgesprochene Kapitulation aus tiefster Überzeugung ablehnen. Aus diesen Freikorps geht im März 1919 die *„Vorläufige Reichswehr"* hervor. Sie stellt ein Bekenntnis zur Wiederaufrüstung dar, wie sie von der deutschen Heeresführung geplant, von den Siegermächten des Weltkrieges jedoch strikt untersagt wird. In den Versailler Friedensverträgen vom Juni 1919 beschränken sie das deutsche Heer auf 100.000 Berufssoldaten, die Marine auf 15.000. Sie verbieten den Besitz von Schlachtschiffen, U-Booten, Panzern, Flugzeugen, schweren Artilleriewaffen sowie das Einrichten eines Generalstabs, um sicherzustellen, dass von Deutschland keine Kriegsgefahr mehr ausgehen könne. Eine Kommission der Alliierten überwacht die Einhaltung dieser Bestimmungen. Seitens der Reichswehr wird jedoch alles getan, um die Kontrollorgane hinters Licht zu führen. Formell vollzieht man die Abrüstung, doch im Geheimen wird schon früh an der Wiederaufrüstung gearbeitet.

Das vorrangige Feindbild ist die eben erst entstandene, unabhängige Republik Polen, der durch die Versailler Friedensverträge Gebiete zugesprochen wurden, die bislang zum Deutschen Reich gehörten. Die deutsche Heeresleitung will das neue Staatsgebilde schlicht wieder auslöschen, und hofft dabei auf sowjetische Unterstützung, nachdem die junge polnische Republik auch im Osten gegen Sowjetrussland um seine Grenzen kämpft. Allerdings gelingt der polnischen Armee dort nach anfänglichen schweren Rückschlägen ein entscheidender Sieg. Der Erfolg beruht auf Erkenntnis-

2 *Funkwagen der deutschen Reichswehr in den 1920er Jahren*

sen von Funkhorcheinheiten, die die Absichten der gegnerischen Führung erlauschen konnten. Darin zeigt sich die Bedeutung der Funkaufklärung, die in den Jahren des Weltkrieges ein unverzichtbares Kriegsmittel geworden ist.
Die Kämpfe zwischen polnischen und russischen Truppen werden jedoch auch in Deutschland belauscht. Für die deutsche Generalität ist es eine willkommene Möglichkeit, Einblick in die Funkgewohnheiten künftiger Kriegsgegner zu nehmen, und eine gute Gelegenheit zur Schulung des eigenen Horchdienstes, der zu dieser Zeit Gestalt annimmt.
In mehreren deutschen Städten entstehen militärische Nachrichten-Abteilungen, deren jede aus 300 Mann besteht. Sie setzen sich aus Einheiten für Brieftauben, Fernsprech- und Funkeinheiten sowie Einheiten zum Abhören von fremdem Funkverkehr zusammen. Neben Pferden und Mauleseln verfügen sie bald auch über moderne Fahrzeuge wie Motorräder, Personenkraftwagen, Lastkraftwagen und Omnibusse. Gefunkt wird anfangs mit einigen wenigen fahrbaren und tragbaren Funkstationen aus Weltkriegsbeständen, die von den Alliierten genehmigt worden sind. Diese alten Gerätschaften werden jedoch ebenfalls bald durch moderne ersetzt. Damit die nach dem Morsealphabet gefunkten Nachrichten möglichst schnell und fehlerlos übermittelt werden, wird der Funkbetrieb im Exerzierdienst perfektioniert. Mit der Stoppuhr werden die Soldaten gedrillt, um den gesamten Ablauf vom Verschlüsseln und dem Durchgeben bis zum Entschlüsseln und schließlich dem Übermitteln an die jeweilige Kommandozentrale kurz zu halten. Dabei geht man davon ab, die Funkübungen bei Kirchenstille durchzuführen, beschäftigt vielmehr die halbe Kompanie damit, Störgeräusche in den Äther zu schicken, um die Funker der anderen Hälfte bei der Erfüllung ihrer Aufgabe zu fordern.
Darüber hinaus richtet die Reichswehr in diversen Städten auch stationäre Horchdienste ein. Dort sitzen Funkhorcher an ihren Empfangsgeräten und lauschen durch Kopfhörer in den Äther. Ihre Aufgabe ist es, Funksprüche fremder Armeen aufzuschnappen und die Morsezeichen zu notieren. Da dieser Funkverkehr der Geheimhaltung wegen oft chiffriert erfolgt, sind die Horchstellen auch mit Entschlüsselungsspezialisten besetzt. Hochgradig verschlüsselte Funksprüche gehen an eine zentrale Chiffrierstelle im Reichswehrministerium in Berlin, die den Entzifferungsdienst wie auch die Auswertung der Ergebnisse besorgt. Die Generalität will damit Erkenntnisse über den Stand der Rüstung sowie über militärische Aktivitäten möglicher Kriegsgegner bekommen. Und es gibt viele mögliche Kriegsgegner in diesen Tagen. Die im Westen Deutschlands gelegenen Stationen belauschen vorwiegend britischen und französischen Heeresfunkverkehr, die östlich gelegenen polnischen, tschechischen und russischen.

1925 gelingt es in den verschlüsselten Funkverkehr polnischer Fliegerverbände einzubrechen und tausende Funksprüche mitzulesen. Die deutsche Führung kann dadurch die meisten Standorte der polnischen Luftwaffe eruieren und erfährt von konkreten Aufrüstungsplänen. Als man in Warschau die Misere bemerkt, übt man sich in Schadensbegrenzung. Man versucht den Deutschen über Doppelagenten einen falschen Funkschlüssel unterzuschieben und funkt hunderte fingierte Botschaften, während die echte Korrespondenz per Kurier oder über sichere Telefonleitungen abgewickelt wird.

Zur selben Zeit versucht ein Berliner Ingenieur namens Arthur Scherbius eine von ihm konzipierte Maschine auf den Markt zu bringen, die einer elektrischen Schreibmaschine ähnelt. Ihre Funktion besteht aber nicht im Niederschreiben von Nachrichten, sondern darin, sie in Chiffren umzuwandeln, damit diese seitens Unbefugter nicht mitgelesen werden können. Bezeichnenderweise trägt sie den Namen *„Enigma"*, was auf Griechisch *„Rätsel"* bedeutet. Nur der legitime Empfänger kann die chiffrierte Nachricht mithilfe einer identischen Maschine in Klartext rückwandeln. Während eine frühe Ausführung noch behäbig und unhandlich und vor allem für den Büro- oder Kanzleibetrieb konzipiert ist, hat ein batteriebetriebenes Folgemodell die Größe einer Reiseschreibmaschine. Es wiegt nur elf, zwölf Kilo, weil es keine Typenhebeln zur Niederschrift der Chiffren besitzt. Stattdessen hat es ein elektrisches Anzeigefeld mit 26 Lampen – je eine für jeden Buchstaben des Alphabets. Eingebaut in einen aufklappbaren Holzkoffer, erweist sich dieses Modell als gut transportierbar und auch für militärischen Einsatz geeignet. Im Februar 1926 wird es bei der deutschen Kriegsmarine eingeführt.
Zwei Jahre danach ereignet sich in Wien ein bemerkenswerter Vorfall, nämlich die behördliche Unterdrückung eines einschlägigen Buches. Autor ist Andreas Figl, ein früherer Chiffrierexperte der k. u. k. Armee, der nun in der Chiffrierabteilung des österreichischen Außenamts tätig ist. Figl hat im Frühjahr 1926 einen Band mit dem Titel *Systeme des Chiffrierens* herausgebracht, in dem er sich unter anderem mit der Enigma beschäftigt und in dem er auch einen zweiten Band mit dem Titel *Systeme des Dechiffrierens* ankündigt. Er verursacht damit Aufregung. Auf Intervention des österreichischen Heeresministeriums wird das in Druck befindliche Buch aus dem Verkehr gezogen. Figl vermutet den Ursprung des Verbots bei der deutschen Generalität, die nun für das aufrüstende deutsche Heer ebenfalls auf die Enigma zurückgreift. Durch das Verbot soll wohl verhindert werden, dass spezielles Fachwissen um das Einbrechen in das Schlüsselverfahren in eine breite Öffentlichkeit gelangt. Allerdings ist die Enigma – ursprünglich

3 *Die Enigma*

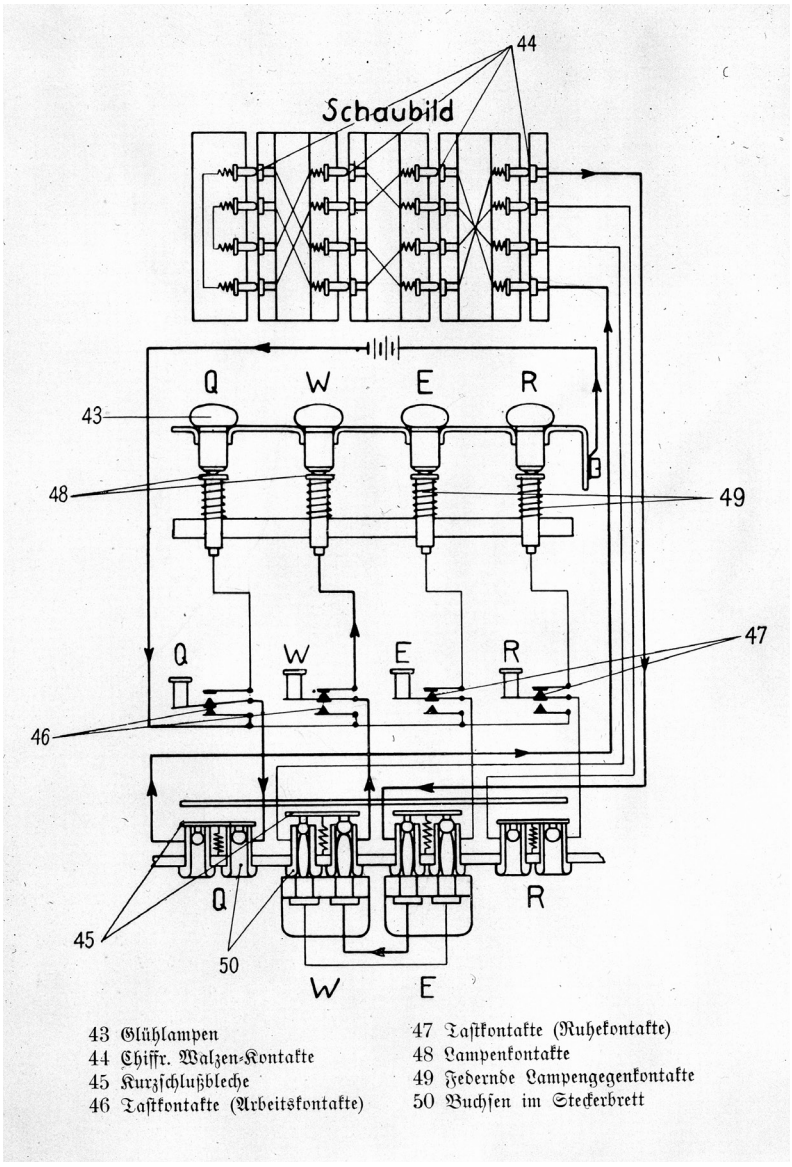
am freien Markt angeboten – in Zeitschriften und Werbebroschüren bereits mehrfach öffentlich besprochen worden. Vor Figl hat Scherbius selbst ihre Konstruktion und Funktionsweise dargelegt. Und auch der Wiener Kriminalist Siegfried Türkel beschreibt in seinem 1927 erschienenen Buch *Chiffrieren mit Geräten und Maschinen* diverse Modelle samt Schlüsselverfahren und Abbildungen mit Detailansichten.
Die Enigma ist längst kein Geheimnis mehr, wird von Interessenten aus verschiedenen Ländern legal erworben. Aber selbstverständlich verfügen

die vom deutschen Militär eingeführten Modelle über Schlüsselwalzen mit geänderter Verdrahtung.

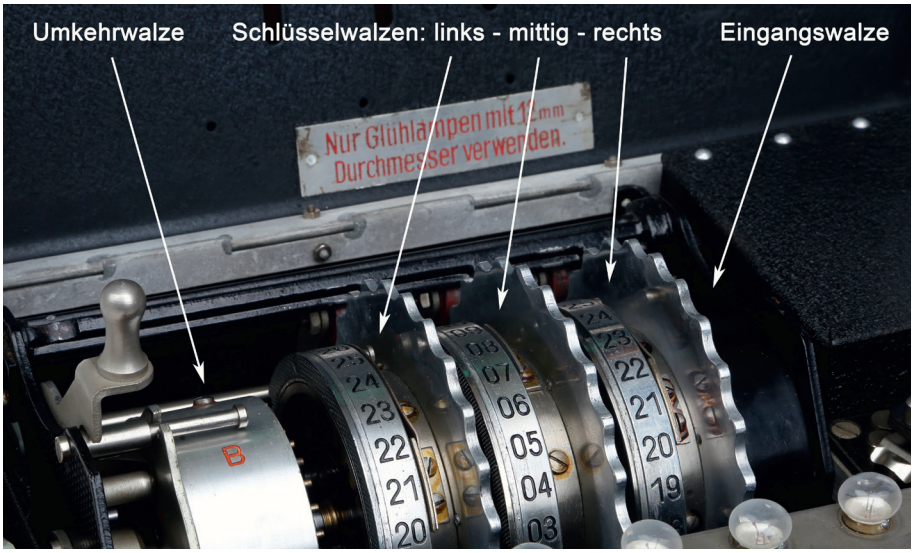
Die Einführung der Enigma für den deutschen militärischen Nachrichtenverkehr zeitigt rasch Erfolge. Während so manches überkommene Handschlüsselverfahren im Ausland geknackt worden ist, ist das Mitlesen von Enigma-Nachrichten nicht möglich. Auch beim Generalstab des polnischen Heeres in Warschau registriert man, dass unter aufgefangenen deutschen Funksprüchen der Anteil derer wächst, die sich nicht entziffern lassen. Man vermutet, dass es sich um maschinenverschlüsselte Sprüche handelt und sucht Unterstützung bei Experten.
Angehörige des Geheimdiensts halten am Mathematischen Institut der Universität Posen Ausschau nach talentierten Studenten, die man für einen Lehrgang in Kryptologie – der Wissenschaft der Verschlüsselung – interessieren könnte. Dass man dafür gezielt in die ehemalige preußische Provinz geht, hat den Grund, dass in dieser Region viele Studenten auch noch Deutsch sprechen, was eine elementare Voraussetzung dafür darstellt, Chiffren deutscher Texte entziffern zu können.
Eine Gruppe an Studenten wird für einen Lehrgang in einer Posener Kaserne rekrutiert. In den ersten Wochen werden die Teilnehmer in die Geschichte des Verschlüsselungswesens eingeführt und mit den wichtigsten Schlüsselverfahren vertraut gemacht. In weiterer Folge werden sie dem *„Biuro Szyfrów"*, der kryptologischen Abteilung des polnischen Generalstabs, zugewiesen. Diese Abteilung sorgt neben der Chiffrierung des Funkverkehrs der polnischen Armee auch für Funkaufklärung nach Osten und Westen samt der Entschlüsselung und Entzifferung russischer Chiffren bzw. deutscher. Die Studenten werden zunächst in einer Posener Außenstelle in Kellerräumen der örtlichen Kommandantur auf chiffrierte deutsche Funksprüche angesetzt. Es ist ein Test, den ihre Auftraggeber dazu nutzen, sie zu beobachten, um eine endgültige Auswahl zu treffen. Im September 1932 werden der 27jährige Marian Rejewski, der 25jährige Henryk Zygalski und der 23jährige Jerzy Różycki als die vielversprechendsten Kandidaten ausgewählt. Fortan arbeiten sie im Generalstabsgebäude in Warschau. Als Kopf der Gruppe erhält Rejewski einen besonderen Auftrag. Er soll sich mit den mysteriösen Chiffren auseinandersetzen, die jetzt immer häufiger auftreten – mit den Chiffren der Enigma.

Die Chiffriermaschine Enigma steht für eine neue Ära – die Technisierung des bislang durch handschriftliche Verfahren dominierten Chiffrierwesens. Mit ihrer aus 26 Tasten bestehenden Tastatur erinnert sie nur äußerlich an eine Schreibmaschine. In ihrem Inneren verbirgt sich ein dichtes

Verdrahtungsgeflecht. Dieses sorgt dafür, dass der Strom, der mit jedem Tastendruck abgesetzt wird, einen bestimmten Weg durch die Maschine hindurch nimmt und dem gedrückten Buchstaben – etwa einem *A* –, am Ende einen Chiffrebuchstaben – etwa ein *X* – zuweist, der dann auf dem Anzeigefeld aufleuchtet.

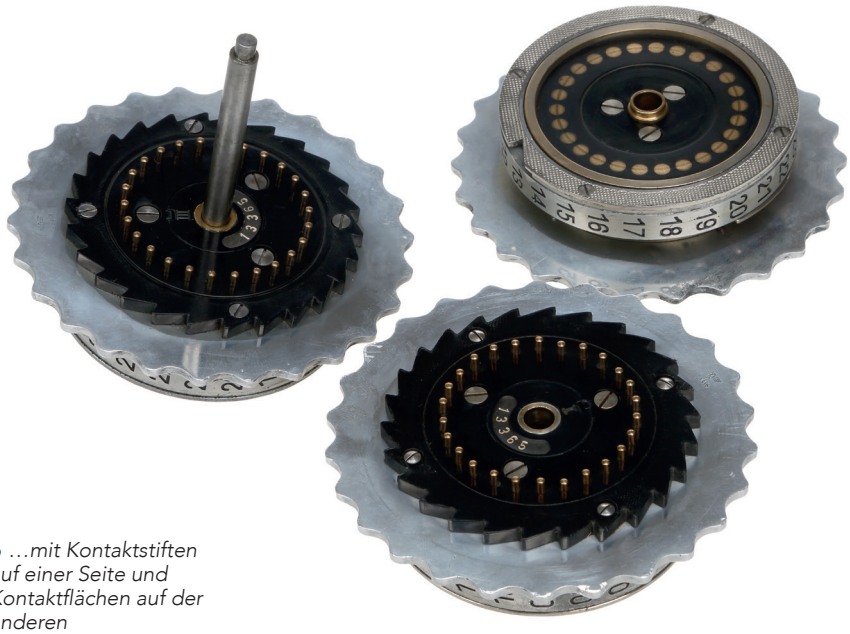


4 *Der Stromkreis der Enigma*



5 *Die Schlüsselwalzen der Enigma...*

Dafür verantwortlich sind mehrere elektromechanische Bauteile. Von der Tastatur führt die Verdrahtung zunächst zu einer starr montierten Eingangswalze, die rechts in der Maschine, oberhalb des Anzeigefelds, sitzt. Diese Eingangswalze weist 26 kranzförmig angeordnete Kontakte für die Buchstaben des Alphabets auf, die trivial mit den Tasten verkabelt sind: *A* mit *A, B* mit *B, C* mit *C* usw.; ein Umstand, der noch Bedeutung bekommen soll.
An der Eingangswalze liegen linker Hand drei nebeneinander in die Maschine eingesetzte Schlüsselwalzen an. Jede von ihnen weist an ihrer rechten Seitenfläche einen Kranz aus 26 Kontaktstiften auf und an der linken einen ebensolchen aus Kontaktflächen. Jeder Kontaktstift der rechten Seite ist im Walzeninneren mit einer der Kontaktflächen auf der anderen verdrahtet; bei jeder Walze nach einem anderen Muster.
Der Strom fließt also von der gedrückten Taste über den entsprechenden Kontaktstift der Eingangswalze in die anliegende rechte Schlüsselwalze. In deren Innerem wird er entsprechend der Verdrahtung an eine ausgangsseitige Kontaktfläche geleitet. Von dort fließt er über den an dieser Stelle anliegenden Kontaktstift der mittleren Schlüsselwalze und gelangt über deren innere Verdrahtung an die zugehörige Ausgangskontaktfläche; das Gleiche vollzieht sich in der linken Schlüsselwalze. Aufgrund der Tatsache, dass die Verdrahtungen der drei Schlüsselwalzen unterschiedlich sind, hat die Reihenfolge, in der die Walzen in die Maschine eingesetzt sind, Auswirkungen auf den Weg, den der Strom nimmt, und damit auf die Verschlüsselung.



6 *…mit Kontaktstiften auf einer Seite und Kontaktflächen auf der anderen*

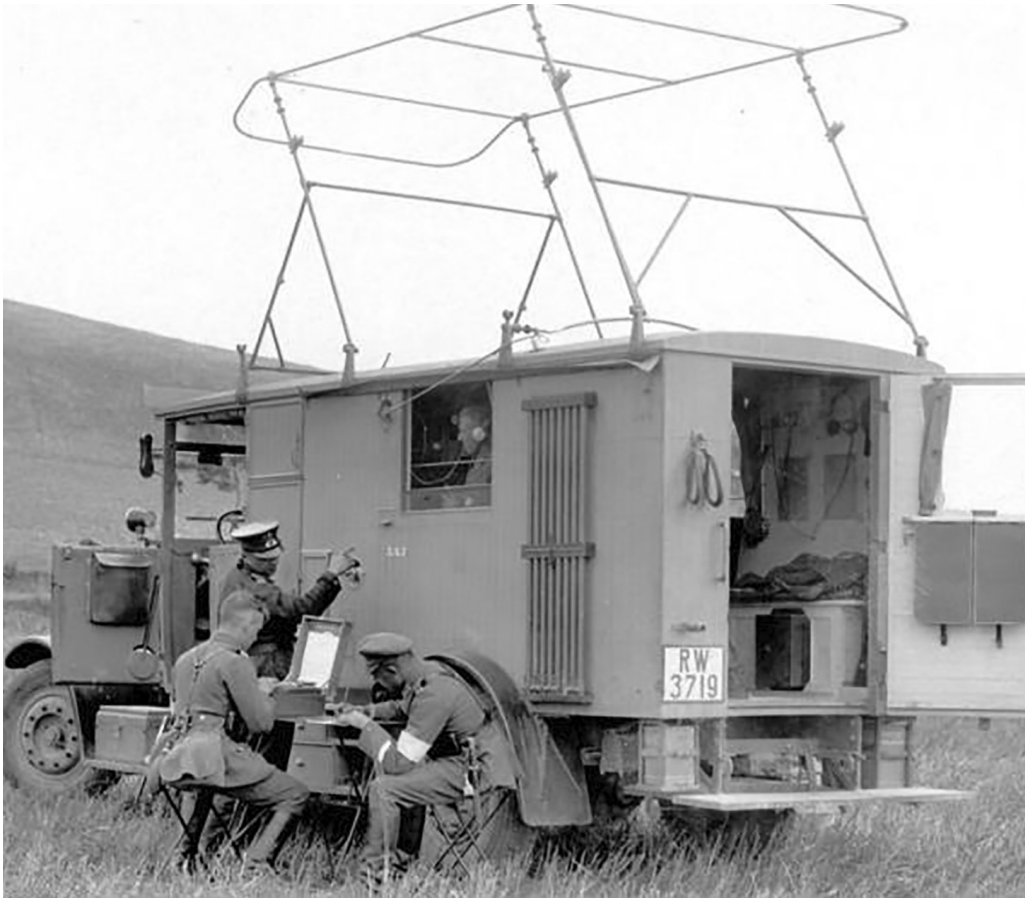
An die drei Schlüsselwalzen schließt linker Hand eine starr montierte Umkehrwalze an, die den Abschluss des Walzensatzes bildet. Ihre 26 Kontaktstifte sind zu 13 Paaren verdrahtet. Der aus der linken Schlüsselwalze kommende Strom wird am anliegenden Kontakt aufgenommen und über den zugehörigen Ausgangskontakt wieder durch die Verdrahtung der drei Schlüsselwalzen hindurch zurückgeleitet. Dabei nimmt der Strom naturgemäß einen anderen Weg als am Hinweg.
Die drei Schlüsselwalzen sitzen überdies drehbar gelagert auf einer Achse, wodurch jede für sich in 26 verschiedene Stellungen gedreht werden kann. Eine Zahnradmechanik sorgt dafür, dass sich bei jedem Tastendruck auf der Tastatur die ganz rechts eingelegte Walze um einen Drehschritt weiterdreht. Ein solcher Drehschritt verändert die Gesamtverdrahtung der Maschine und verstärkt damit die Verschlüsselung, denn er verhindert, dass bei mehrfachem Drücken des gleichen Buchstabens auf der Tastatur dieselben Chiffren zugewiesen werden. Und damit das Chiffriermuster nach einer Umdrehung der ersten Walze nicht wieder von vorn beginnt, lässt eine Übertragskerbe auch die mittlere um einen einzelnen Drehschritt mit rotieren, wenn die Kerbe den Anschlag passiert. Von da an dreht sich die mittlere Walze nach allen 26 Drehschritten der rechten jeweils um einen Schritt mit. Analog funktioniert der Übertrag zwischen der mittleren und der linken Walze.

Das Walzengetriebe arbeitet also ähnlich einem mehrstelligen Zählwerk: die ganz rechts eingesetzte Walze dreht sich bei jedem Tastendruck, während die mittlere sich selten bewegt (alle 26 Schritte der ersten) und die linke nur sehr selten (alle 26 mal 26, also 676 Schritte). Insgesamt erzeugt das Werk 17.576 verschiedene Stellungen, die die drei Walzen zueinander einnehmen können. Faktisch sind es aufgrund der besonderen Konstruktion der Übertragsmechanik 16.900, da die mittlere Walze an einer bestimmten Stelle einen doppelten Drehschritt absolviert, nämlich dann, wenn sie von der rechten einen Übertrag bekommt, während im nächsten Schritt ihr Übertrag für die linke ansteht.
Erst nach einem Durchlauf durch alle möglichen Stellungen der drei Walzen – eine Maschinenperiode – würden sich die Walzenstellungen und mit ihnen die Chiffrezuweisungen wiederholen. Dies erscheint für den praktischen Betrieb jedoch bedeutungslos, da Funksprüche möglichst kurz gehalten werden müssen.
Im Unterschied zu ihren zivilen Vorläufern weist die militärische Version der Enigma überdies eine Neuerung auf, die ihre Verschlüsselung vollends unangreifbar machen soll. An ihrer Vorderseite befindet sich ein Steckerfeld mit Buchsen für alle Buchstaben des Alphabets. Die Buchsen lassen sich mithilfe von beiliegenden Kabeln paarweise verbinden, was zur Folge hat, dass die betreffenden Buchstaben gegeneinander ausgetauscht werden. Verkabelt man beispielsweise *A* mit *K* und tippt danach auf der Tastatur ein *A* ein, so wird es als *K* in die Maschine geleitet; tippt man ein *K*, geht ein *A* hinein. Wird also ein am Steckerfeld gesteckter Buchstabe auf der Tastatur gedrückt, läuft der Strom zunächst durch die Steckerverbindung, danach durch die Schlüsselwalzen und über die Umkehrwalze wieder zurück durch die Schlüsselwalzen und eine allfällige Steckerverbindung, bevor am Ende die zugewiesene Chiffre am Anzeigefeld aufleuchtet. Dann muss die Chiffre umgehend aufgeschrieben werden, denn mit Auslassen der Taste erlischt das Lämpchen.

Die Enigma mag manch Eingeweihtem als ein Wunderwerk der Technik erscheinen, das eine astronomisch hohe Zahl an Verschlüsselungsmöglichkeiten erzeugt. Die drei Schlüsselwalzen eröffnen grundsätzlich 26 mal 26 mal 26 – also 17.576 – mögliche Wege, die der Strom durch die Maschine nehmen kann. Die drei Walzen können in sechs verschiedenen Reihenfolgen in die Maschine eingesetzt werden, deren jede andere Chiffrierungen nach sich zieht. Dadurch erhöht sich die Verschlüsselungskapazität durch den Faktor sechs auf über 105.000 Möglichkeiten. Dazu kommt die enorme Kapazität des Steckerbretts. Das Stecken von nur sechs Buchstabenpaaren eröffnet rund 100 Milliarden Kombinationsmöglichkeiten.

Insgesamt ergibt sich damit eine Zahl von zehn Billiarden Möglichkeiten.[1] Eine schier unüberwindliche Hürde!
Doch die schillernde Zahl überstrahlt strukturelle Schwächen. Der starre Schrittmodus der rechten Walze – mit jedem Tastendruck erfolgt ein einzelner Drehschritt – sowie die exakt 26stelligen Übertragszyklen erleichtern Versuche von außen, in die Schlüssel einzubrechen. Eine weitere Schwachstelle ist die Umkehrwalze. Aufgrund der Tatsache, dass sie den Chiffrierprozess durch die ganze Maschine zurückleitet, funktioniert die Enigma invers. Das heißt, wenn an einer bestimmten Maschinenstellung ein *A* zu einem *K* wird, würde bei derselben Stellung auch ein *K* zu einem *A*. Diese baulich bedingte Eigenschaft hat den Vorzug, dass Ver- und Entschlüsseln mit ein und derselben Schlüsseleinstellung erfolgen können. Die dabei verursachten festen Beziehungen zwischen Klarbuchstaben und Chiffren kommen jedoch auch Versuchen Außenstehender entgegen, in die Enigma-Schlüssel einzubrechen, und zwar in zweierlei Hinsicht. Zunächst reduziert die Bauweise die theoretisch mögliche Verschlüsselungskapazität. Ein *A* kann niemals zu einem *A* werden, ein *B* niemals zu einem *B*, ein *C* nicht zu einem *C* usw. Diese Eigenschaft erlaubt das Entwickeln von Einbruchsstrategien auf semantischer Ebene. Denn der Umstand, dass kein Buchstabe in sich selbst übergehen kann, bedeutet, dass sich gesuchte Worte in einem Chiffretext nur dort verbergen können, wo ihre Buchstaben nicht auf ihresgleichen fallen. Gelingt es, ein Wort, von dem man weiß, dass es im Text vorkommen muss, auf diese Weise exakt zu lokalisieren, hat man ein gültiges Chiffriermuster über mehrere Stellen hinweg gefunden und damit ein gutes Stück des Weges zur Schlüsseleinstellung, mit der der Spruch chiffriert worden ist, geschafft. Man muss jetzt nur noch die Stelle in der Maschinenperiode finden, an der die mehrstellige Sequenz erzeugt wird – was noch schwierig genug ist. Diesem methodischen Ansatz wird in den nächsten Jahren dennoch große Bedeutung zukommen.
Eine der größten Schwächen der Enigma besteht aber wohl darin, dass alle Exemplare mit identisch verdrahteten Schlüsselwalzen arbeiten und ein regelmäßiger Ersatz dieser Walzen durch anders verdrahtete nicht vorgesehen ist. Für die Kryptologen der Gegenseite bedeutet dies letzten Endes, dass sie vergleichsweise viel Zeit haben und ihnen viele Chiffren zur Verfügung stehen, um die Walzen zu rekonstruieren, was sie im Übrigen auch nur ein einziges Mal tun müssen. Auch dies wird den Lauf der Enigma-Geschichte wesentlich mitbestimmen.

[1] Siehe im Abschnitt *Kryptologie* das Kapitel *Die Möglichkeiten der Enigma*



7 *Funkverkehr der Reichswehr mit Enigma-Verschlüsselung*
Ende der 1920er Jahre

Eine gewissermaßen systemisch bedingte Schwäche der Enigma resultiert aus dem Umstand, dass die Exemplare der verschiedenen Einheiten eines Verbands identische Maschineneinstellungen verwenden müssen, um miteinander kommunizieren zu können. Die Einheiten müssen dazu von der zentralen *„Chiffrierstelle im Reichswehrministerium"* in Berlin regelmäßig mit vorgedruckten *„Schlüsseltafeln"*, die die vorzunehmenden Einstellungen für einen Monat im Voraus enthalten, versorgt werden. Die Verteilung einer Vielzahl solcher streng geheimen Unterlagen beinhaltet jedoch ein hohes Risiko, dass sie dem Gegner in die Hände fallen. Übermittelt werden sie deshalb durch besondere militärische Kuriere; eine Beförderung mit der regulären Post, der Feldpost oder ganz allgemein mit Flugzeugen ist ausdrücklich verboten.

Diese Schlüsselunterlagen legen fest, was jeder Schlüssler vor Inbetriebnahme seiner Enigma einzustellen hat. So muss er zunächst sechs bestimmte *„Steckerverbindungen"* an den Buchsen des Steckerfelds herstellen. Dann hat er den Maschinendeckel der Enigma zu öffnen und die Walzen in einer bestimmten Reihenfolge in die Maschine einzusetzen (*„Walzenlage"*). Ebenfalls nach den Vorgaben ist die *„Ringstellung"* einzustellen. Diese bezieht sich auf den Beschriftungsring, den jede Walze besitzt. Er umschließt die Walze und erlaubt die Beschriftung, die von 01 bis 26 reicht (von A bis Z bei der Marine-Enigma), in jede beliebige Stellung zu drehen. Die Ringstellung verändert die Beschriftung gegenüber dem mit den Verdrahtungen versehenen Walzenkern. Sie berührt damit den elektromechanischen Verschlüsselungsprozess an sich nicht, verschleiert jedoch die geltende Schlüsseleinstellung und erschwert dadurch Entschlüsselungsversuche durch Außenstehende erheblich.
Nach Einstellung der Ringe ist der Maschinendeckel zu schließen und an den Walzen die so genannte *„Grundstellung"* einzustellen. Dazu sind die Walzen an ihren Kämmen, die durch den Maschinendeckel ragen, solange weiterzudrehen, bis die in den Schlüsselunterlagen verlangte Stellung, beispielsweise *B-C-A*, in den im Deckel eingelassenen Sichtfenstern zu sehen ist – also die entsprechenden Ziffern *02-03-01*. Als

8 *Schlüsselwalze mit Ring und Übertragskerbe*

Datum	Walzenlage	Ringstellung	Grundstellung
4.	I III II	16 11 13	01 12 22

Steckerverbindung	Kenngruppen-Einsatzstelle ..... Gruppe	Kenngruppen
CO DI FR HU JW LS TX	2	adq nuz opw vxz

9 *Einstellungen eines Tagesschlüssels*

Einstellungen des *„Tagesschlüssels"* sind Ringstellungen, Grundstellung und Steckerverbindungen täglich gemäß den Vorgaben zu ändern, während die Reihenfolge der Walzen – die *„Walzenlage"* – anfangs noch drei Monate lang gültig bleibt.

Die Einstellungen des allgemeinen Tagesschlüssels reichen für sicheren Funkverkehr jedoch nicht aus. Gelingt es der Gegenseite, eine bestimmte Menge an Funksprüchen aufzufangen, die mit denselben Einstellungen verschlüsselt worden sind, ist es ihr grundsätzlich möglich, die zugrunde liegenden Schlüsseleinstellungen zu rekonstruieren. Deshalb existiert eine weitere Ebene der Verschlüsselung: der individuelle Spruchschlüssel. Er wird nicht vorgegeben, sondern von jedem Schlüssler für jeden Funkspruch frei gewählt. Der Schlüssler wählt drei beliebige Buchstaben – etwa *A, F* und *E* – und tippt sie zwei Mal hintereinander auf seiner auf den Tagesschlüssel eingestellten Enigma ein. Die daraus resultierenden sechs Chiffren werden notiert. Danach stellt er die Walzen auf die drei Buchstaben des gewählten Spruchschlüssels *A-F-E* ein – also eigentlich auf die entsprechenden Ziffern *01-06-05* – und chiffriert mit dieser Einstellung die zu übermittelnde Nachricht; die jeweils aufleuchtenden Chiffren werden ebenfalls notiert. Verschlüsselt wird im Übrigen zumeist von zwei Mann: Einer tippt den Text in die Maschine und diktiert die jeweils aufleuchtenden Buchstaben, die der andere auf das entsprechende Formular schreibt.

Nach dem Verschlüsseln werden die Chiffren vom Funker via Morsetaste in einem Tempo von 60, 70 und mehr Buchstaben pro Minute abgesetzt. Dem so genannten *„Spruchkopf"* mit diversen Routinefunkzeichen folgen die sechs Chiffren des Spruchschlüssels, der auf diese Weise doppelt gesendet wird, um etwaigen Übermittlungsfehlern, wie sie beim Funk

durch atmosphärische Störungen immer wieder auftreten, zu begegnen. Dann kommen die Chiffren der eigentlichen Nachricht.
Der Empfänger hört den Funk ab und notiert die im Kopfhörer piepsenden Morsezeichen. Entschlüsselt wird auf einer Enigma, die auf denselben Tagesschlüssel eingestellt ist wie die des Absenders. Darauf tippt der zuständige Schlüssler zunächst die sechs Chiffren, von denen er weiß, dass sie den Spruchschlüssel bilden. Er erhält – so kein Übermittlungsfehler vorliegt – zwei Mal dieselbe Buchstabengruppe – *AFEAFE*. Dann stellt er den Spruchschlüssel *A-F-E* auf seiner Maschine ein, indem er die Walzen dreht, bis die entsprechenden Ziffern *01-06-05* in den Sichtfenstern im Maschinendeckel erscheinen. Mit dieser Einstellung kann er die Nachricht entschlüsseln, indem er sie Chiffre für Chiffre eintippt. Am Anzeigefeld erscheint dann Buchstabe für Buchstabe der Klartext.

Aus Sicherheitsgründen erhalten die Schlüssler von ihren Vorgesetzten immer nur die Schlüsselunterlagen für die nächsten beiden Tage ausgehändigt. Dem Gegner soll selbst im schlimmsten Fall einer Erbeutung möglichst wenig Geheimmaterial in die Hände fallen. Dies gilt auch für abgelaufene Unterlagen, die nach zwei Tagen zu verbrennen sind, denn auch daraus könnte man Rückschlüsse auf Schlüsselverfahren und sogar auf die Verdrahtung der Enigma ziehen. Selbstverständlich ist auch dafür Sorge zu tragen, dass das Geheimnis um die Enigma selbst gewahrt bleibt. Sie gilt als geheimer Gegenstand im Sinne der *„Verschlußsachen-Vorschrift"* und ist entsprechend zu behandeln. Fehlverhalten in Bezug auf Schlüsselunterlagen und –maschinen gilt als militärischer Ungehorsam und unterliegt erheblicher Strafandrohung.
Bei einem Einsatz im Kriegsgebiet sind überdies sämtliche Unterlagen und Maschinen jederzeit zur Vernichtung bereitzuhalten. Es wird angeordnet, lieber zu früh und unnötig zu vernichten, als zu lange zuzuwarten und damit zu riskieren, dass ein rechtzeitiges Vernichten unmöglich werden könnte. Fallen dem Gegner dennoch Unterlagen und Maschinen in die Hände, sind so schnell wie möglich die vorgesetzten Dienststellen davon in Kenntnis zu setzen, die rasch reagieren müssen, um größeren Schaden abzuwenden.
Grundsätzlich scheinen die Verantwortlichen bezüglich der Sicherheit der Enigma aber recht zuversichtlich zu sein. Das komplexe Schlüsselverfahren würde verhindern, dass die Gegenseite den geheimen Funkverkehr mitlesen könne, selbst wenn ihr eine Enigma oder Schlüsselunterlagen in die Hände fielen. Ohne Unterlagen sei die Maschine weitgehend wertlos, wie andererseits auch keine erbeuteten Unterlagen helfen würden, solange die Verdrahtungsmuster der Walzen unbekannt seien. Und sogar

im schlimmsten aller Fälle – wenn dem Gegner beides in die Hände fiele – ende die Möglichkeit des Mitlesens spätestens mit der Ausgabe neuer Schlüsselunterlagen. Abgesehen davon ist zur Überbrückung solcher Notfälle ein händisches Schlüsselverfahren vorgesehen, auf das alle Beteiligten rasch wechseln können und das ersatzweise auch bei Störungen einer einzelnen Enigma verwendet werden kann.
Man sieht sich auf deutscher Seite gut gerüstet für den Krieg. Doch für Zuversicht besteht kein Grund, wie sich andernorts zeigt.

In Warschau hat Marian Rejewski seine Arbeit an dem streng geheimen Projekt *„Enigma"* aufgenommen. Die Herausforderung ist groß für den jungen Mathematiker. Außer aufgefangenen Funksprüchen steht ihm zunächst nur ein frühes Maschinenmodell zur Verfügung, das der polnische Geheimdienst Jahre zuvor besorgt hat. Mit diesem Exemplar lassen sich die Funksprüche des deutschen Militärs natürlich nicht entziffern, da die militärische Enigma mit dem zusätzlichen Steckerbrett und neu verdrahteten Schlüsselwalzen ausgestattet ist. Zumindest aber kann Rejewski daran Grundlegendes wie Aufbau und Konstruktion studieren und Funktionselemente wie die Schlüsselwalzen und das zählwerkartige Schrittprinzip.

10 *Marian Adam Rejewski, Jg. 1905*

Dabei fällt ihm auf, dass bei sehr kurzen Texten zumeist nur die rechte Walze rotiert, während die beiden anderen stillstehen. Erkenntnisse wie diese finden Eingang in seine Überlegungen.

Darüber hinaus beschäftigt sich Rejewski mit chiffrierten deutschen Funksprüchen, die von polnischen Horchstationen aufgefangen werden. Dabei erkennt er bei einer am Beginn der Sprüche stehenden Gruppe aus sechs Chiffren bemerkenswerte Gesetzmäßigkeiten. Sind die jeweils ersten gleich, so auch die vierten, wie bei folgenden Beispielen: *FCLWND, FRTWTO, FGIWSA*. Dieselbe Gesetzmäßigkeit findet er in anderen Sprüchen bei Chiffren an den zweiten und fünften sowie den dritten und sechsten Stellen. Rejewski schließt daraus korrekterweise, dass er es mit zwei Dreiergruppen zu tun hat, von denen die zweite eine Wiederholung der ersten darstellt. Im Kern handelt es sich also um eine dreistellige Buchstabenkombination, was angesichts dreier einstellbarer Walzen den Schluss nahelegt, dass es sich um einen dreistelligen Schlüssel handelt, der die für die Chiffrierung benutzte Ausgangsstellung der Walzen bezeichnet und in chiffrierter Form mitgesendet wird. Damit ist der Modus des Spruchschlüssels durchschaut.
Eine weitere Entdeckung ist die, dass besagte sechs Chiffren bei manchen Funksprüchen identisch sind und offensichtlich auf identisch eingestellte Enigmas, also auch auf dieselben Spruchschlüssel, zurückgehen. Von der Wahrscheinlichkeit her gesehen, sollte es nur sehr selten vorkommen, dass mehrere Funker denselben Spruchschlüssel frei wählen. Tatsächlich aber zeigen sich im aufgefangenen Material markante Häufungen. Es ist naheliegend, dass sich dahinter triviale Schlüssel wie *A-A-A* oder *A-B-C* verbergen, die ihrer leichten Merkbarkeit wegen häufiger verwendet werden als andere. Und tatsächlich erweist sich die am häufigsten vorkommende Variante zumeist als diejenige, der die trivialste Buchstabenkombination zugrunde liegt, nämlich *A-A-A*. Spruchschlüssel wie diesen kann Rejewski also einfach erraten. Er hat damit eine Schwachstelle gefunden, die ihn in die Lage versetzt, ein Stück weit in die Enigma einzubrechen.
Den Ausgangspunkt bildet seine Vermutung, dass die markanten sechs Chiffren einen dreistelligen, zweifach gesendeten Spruchschlüssel bilden. Das Besondere daran ist die Wiederholung. Sie lässt Beziehungen entstehen, die der Mechanik der Maschine entspringen und deshalb auch umgekehrt Anhaltspunkte für die Rekonstruktion dieser Mechanik liefern müssen. Es ist ein und derselbe – wenn auch zunächst unbekannte – Klarbuchstabe, der an der ersten Stelle etwa zu einem *F*, und drei Stellen weiter, an der vierten Stelle, etwa zu einem *W* chiffriert wird. Wenn sich bei besagtem Funkspruch zudem die Klarbuchstaben des verwendeten

Spruchschlüssels erraten lassen – etwa die gehäuft vorkommende Kombination *A-A-A* –, so kann man daraus ableiten, dass es ein *A* ist, das an der ersten Stelle zu einem *F* und an der vierten zu einem *W* wird. Aus der inversen Konstruktion der Enigma folgt weiters, dass, wenn ein Klarbuchstabe *A* an der ersten Stelle zur Chiffre *F* wird, auch ein Klarbuchstabe *F* an der ersten Stelle zur Chiffre *A* werden muss. Das heißt, Rejewski kann nun bei allen aufgefangenen Funksprüchen, deren erste Chiffre des Spruchschlüssels ein *A* ist, den Klarbuchstaben *F* dahinter identifizieren. Dasselbe gilt für die Beziehung zwischen *A* und *W* an der vierten Stelle. Aus den zweiten und fünften sowie den dritten und sechsten Chiffren anderer Funksprüche lassen sich in analoger Weise Beziehungen ableiten. Am Ende reichen 60 bis 80 aufgefangene Funksprüche eines Tages, um alle Chiffren herzuleiten, die die Enigma an diesem Tag jedem Buchstaben des Alphabets an jeder der sechs Stellen zuweist. Diese *„charakteristischen Transformationen des Tages"*, wie Rejewski sie nennt, repräsentieren eine Art Vokabular, das es erlaubt, die Chiffren aktueller Spruchschlüssel in ihre Klarbuchstaben zu übersetzen.[2]
Diese vergleichsweise einfache Methode beruht zu einem guten Teil auf der Fahrlässigkeit deutscher Schlüssler, die auf simple Spruchschlüssel wie *A-A-A* zurückgreifen. Darin spiegelt sich eine Schwachstelle, die der menschliche Faktor ins Spiel bringt. Dem Schlüssler alleine die Schuld zu geben, greift aber zu kurz. Denn, ermöglicht wird Rejewskis Methode nicht zuletzt durch die allgemeine Verfahrensweise, dass alle Funker dieselben Schlüsseleinstellungen benutzen müssen, also dieselbe Walzenlage, dieselben Steckerverbindungen sowie dieselbe Grundstellung. Das bedeutet, dass die Chiffren ihrer Spruchschlüssel miteinander vergleichbar sind und zueinander in Beziehung gesetzt werden können. Das erst ermöglicht es Rejewski, in die Enigma einzubrechen, wenn auch zunächst nur in die sechs Stellen des Spruchschlüssels. Die eigentlichen Nachrichten kann er noch nicht entziffern, dazu fehlt ihm die Maschine – sprich: die Verdrahtung der Walzen. Dahingehend erhält er jedoch unerwartete Unterstützung.

Ein in der Chiffrierabteilung der Reichswehr in Berlin beschäftigter Deutscher namens Schmidt liefert zu dieser Zeit gegen Bezahlung streng geheime Dokumente an den französischen Geheimdienst. Er händigt Gustave Bertrand, einem Angehörigen des französischen *„Service de Renseignement"*, unter anderem eine Gebrauchsanleitung und eine Schlüsselanleitung für die Enigma aus. Bertrand persönlich bringt das

[2] Siehe im Abschnitt *Kryptologie* das Kapitel *Charakteristische Transformationen und Zyklen des Tages*

brisante Material in geheimer Mission nach Warschau, in die Metropole des Verbündeten Polen. Dort übergibt er es dem Leiter des polnischen Chiffrierbüros Gwido Langer. Es beginnt eine arbeitsteilige Kooperation, im Rahmen derer sich die französische Seite um zusätzliches geheimdienstliches Material zur Enigma zu bemühen verspricht und die polnische um die Rekonstruktion der Maschine.
Im Dezember 1932 erhält Rejewski die Enigma-Unterlagen ausgehändigt – Kopien der von der deutschen Chiffrierstelle herausgegebenen Gebrauchsanleitung, einer Schlüsselanleitung sowie der Tagesschlüssel für die Monate September und Oktober 1932. Das Material verspricht einen Durchbruch. So lässt die Gebrauchsanleitung den wichtigsten Unterschied zwischen der Heeres-Enigma und früher frei käuflichen zivilen Modellen deutlich werden – auf einer Abbildung ist das Steckerbrett erkennbar. Nicht enthalten sind in den Unterlagen Angaben über die Verdrahtung der Walzen, die man für einen Nachbau der Enigma freilich braucht. Mittels der vorliegenden Schlüsseleinstellungen, einiger mathematischer Theoreme und vielen Chiffren aufgefangener deutscher Funksprüche ist es Rejewski dann aber möglich, die Walzenverdrahtung zu errechnen.
Rejewski beschreibt die Enigma als Gleichung und ihre einzelnen Baugruppen wie das Steckerbrett, die Eingangswalze, die drei Schlüsselwalzen und die Umkehrwalze als Unbekannte. Da er davon ausgeht, dass für die Chiffrierung des lediglich aus sechs Stellen bestehenden Spruchschlüssels zumeist nur die rechte, immer drehende Walze maßgeblich ist, begreift er Drehungen der beiden anderen Walzen ihres seltenen Auftretens wegen als rechnerisch vernachlässigbar. Er fasst die mittlere und die linke Walze sowie die Umkehrwalze zu einer fixen, wenn auch unbekannten Größe zusammen. Dadurch reduzieren sich die Unbekannten in der Gleichung und diese wird durch Einsetzen bekannter Werte lösbar. An Bekanntem kann er die aktuellen Steckerverbindungen einsetzen, die in den Spionageunterlagen enthalten sind, sowie die charakteristischen Transformationen, die er aus erratenen Spruchschlüsseln des betreffenden Tages herleitet. Unerwartete Schwierigkeiten bereitet ihm die Bestimmung der Fixverdrahtung zwischen Tastatur und Eingangswalze. Er versucht zunächst die Verdrahtungsweise der früheren, zivilen Version der Enigma, bei der gemäß der Reihenfolge auf der Tastatur *A* mit *Q, B* mit *W, C* mit *E* usw. verbunden ist. Doch liegt er damit falsch. Nach erfolgloser Fehlersuche in seinen Gleichungen probiert er die simpelste aller denkbaren Möglichkeiten aus und nimmt Verbindungen von *A* mit *A, B* mit *B, C* mit *C* usw. an, führt sämtliche Berechnungen neuerlich aus und – kommt zu Klartext. Es ist kaum zu glauben, aber die triviale Verdrahtung bildet die Lösung. Die Konstrukteure der Enigma haben hier auf eine zusätzliche, fix verdrahtete Verwürfelung

verzichtet, wohl im guten Glauben, dass diese verzichtbar sei, nachdem die Maschine mit dem Steckerbrett ohnehin über schier endlose Verwürfelungspotenziale verfügt. Ein Fehler.

Rejewski hat nun das Verdrahtungsmuster der rechts liegenden Walze herausgefunden. Da die Spionageunterlagen von September und Oktober 1932 einen Quartalssprung abdecken, an dem von deutscher Seite ein planmäßiger Wechsel der Walzen vollzogen wird, kann er mit derselben Methode gleich auch jene Walze berechnen, die ab Oktober an dieser Stelle eingelegt ist. Bei zwei bekannten Walzen, deren Verdrahtung er nunmehr in seine Gleichungen einsetzen kann, stellt die Berechnung der noch ausständigen dritten und der Umkehrwalze für ihn kein allzu großes Problem mehr dar.
In weiterer Folge kann Rejewski deutsche Funksprüche entziffern – wenn auch nur im händischen Verfahren, durch Berechnung mithilfe von Papier und Bleistift. Ein Enigma-Nachbau steht ihm noch nicht zur Verfügung. Ungeachtet dessen lassen sich jetzt auch die Überträge an den Schlüsselwalzen lokalisieren. Rejewski braucht dazu lediglich aktuelle Sprüche Chiffre für Chiffre zu entziffern, bis irgendwann kein Klartext mehr erscheint. An dieser Stelle muss während des Chiffrierprozesses ein Übertrag geschehen sein. Er kann dies überprüfen, indem er in der weiteren Berechnung einen Drehschritt der mittleren bzw. der linken Walze (deren Verdrahtungsmuster er nun ja kennt) simuliert. Wenn danach wieder Klartext auftaucht, hat er die Stelle, an der der Übertrag sitzt, und damit die Walze, die ihn verursacht hat, gefunden. Auf diese Weise kann er in der Folge die Positionen der Übertragskerben aller Walzen bestimmen.[3]
Rejewski hat damit die vollständige Verdrahtung der Enigma hergeleitet. Jetzt können Baupläne gezeichnet und der Nachbau der Maschine kann in Angriff genommen werden. Das Biuro Szyfrów gibt zu Beginn des Jahres 1933 bei einer dem Militär nahestehenden Warschauer Firma 15 Exemplare in Auftrag. Es dauert nicht lang, bis die Maschinen geliefert werden und, nach einigen Anlaufschwierigkeiten, problemlos arbeiten.
Der neuerliche Durchbruch kommt rechtzeitig zur Machtübernahme der Nationalsozialisten in Deutschland. Als Adolf Hitler im Januar 1933 Reichskanzler wird, sind die Polen in der Lage, deutsche militärische Funksprüche mitzulesen. Und dies scheint angesichts des aggressiven Programms der neuen Machthaber in Berlin dringend geboten. Wie sich später herausstellen wird, sind Hitlers Ziele Wiederaufrüstung in großem Stil, Neuauflage des Krieges und Eroberung von riesigen Gebieten Osteuropas unter

[3] Siehe im Abschnitt *Kryptologie* das Kapitel *Berechnung der Enigma*

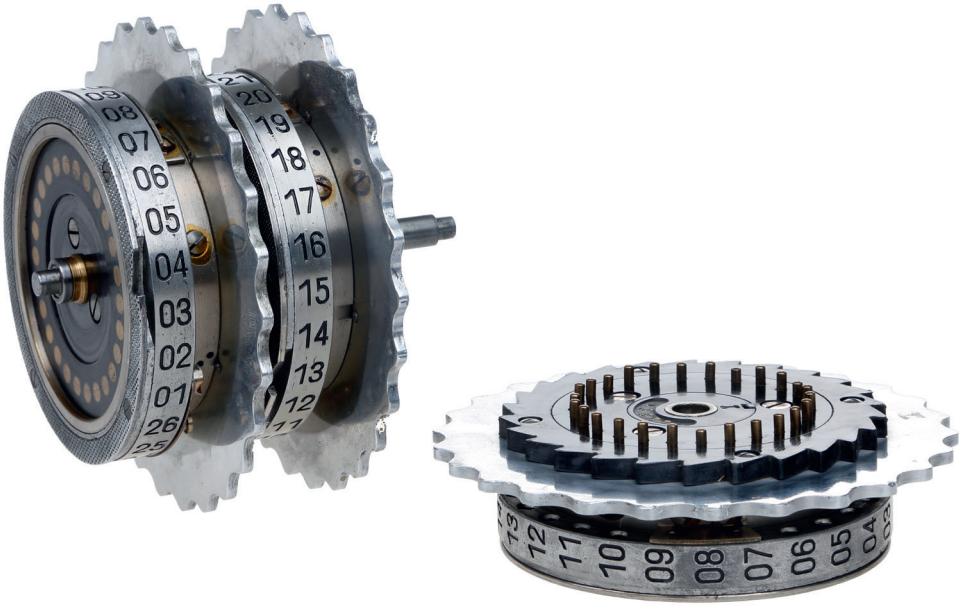
Versklavung und Ausrottung der ansässigen Bevölkerung. Vieles davon bleibt zwar noch unausgesprochen, doch ist man in Warschau aufs Höchste alarmiert.

Es folgt eine Phase angespannter Routine. Jeden Tag aufs Neue müssen deutsche Funksprüche entziffert werden. Dabei können sich Rejewski und seine Kollegen nach wie vor auf erratene Spruchschlüssel stützen. Denn, nachdem den deutschen Schlüsslern die Verwendung dreier identischer Buchstaben untersagt wird, weichen manche von ihnen auf andere markante Dreierkombinationen aus, die ähnlich leicht merkbar und dadurch auch ähnlich leicht erratbar sind. Außerdem registriert Rejewski, dass mit dem Verbot dreier gleicher Buchstaben auch Varianten mit zwei gleichen Buchstaben gemieden werden. Dies kommt ihm sehr entgegen, weil sich dadurch die Menge der möglichen Spruchschlüssel insgesamt stark reduziert.
Die erratenen Spruchschlüssel erlauben weiterhin die charakteristischen Transformationen herzuleiten, also das Vokabular des Tages, das ausweist, in welche Chiffren die Buchstaben des Alphabets an den sechs Spruchschlüsselstellen übergehen. Dies zu wissen, ist für das tägliche Schlüsselbrechen von essentieller Bedeutung, denn es erlaubt herauszufinden, welche der Walzen rechts eingesetzt ist.
Zu diesem Zweck entwickelt Rejewski ein spezielles Rasterverfahren („*metoda rusztu*"),[4] das ihm ermöglicht, aus dem spezifischen Einfluss der rechts liegenden Walze zu bestimmen, um welche Walze es sich handelt. Er stellt zunächst für jede der Walzen einen Kartonbogen her, auf dem in tabellarischer Form verzeichnet ist, welche Chiffren sie an jeder ihrer 26 Drehstellungen allen 26 Buchstaben des Alphabets zuweist. In der ersten Zeile der Tabelle stehen die Zuweisungen, die an der ersten Drehstellung der Walze erfolgen, in der zweiten darunter die der zweiten usw. Zwischen den Zeilen der Tabelle befinden sich Leerzeilen. Analog dazu erstellt Rejewski aus den Transformationen des Tages eine Kartonmaske, worauf in sechs Zeilen für jede der sechs aufeinanderfolgenden Stellen die Chiffren verzeichnet sind, welche jedem Buchstaben des Alphabets zugewiesen werden. Die Zeilen hier sind durch ausgestanzte Leerzeilen getrennt.
Zur Analyse legt Rejewski die sechszeilige Maske so auf einen der Bögen, dass die ersten sechs Zeilen des Bogens in den Leerzeilen erkennbar werden. Dann gleicht er in einem komplizierten Verfahren die Zeilen von Maske und Bogen miteinander auf Ähnlichkeiten ab. Findet sich dabei

[4] Siehe im Abschnitt *Kryptologie* das Kapitel *Rastermethode*

keine, wird die Maske auf dem Bogen um eine Zeile runtergeschoben und neuerlich über sechs Zeilen hinweg abgeglichen. Liefert der ganze erste Bogen kein Ergebnis, folgt der nächste. Tauchen die Ähnlichkeiten letztlich auf einem Bogen auf, ist die Walze, die rechts liegen muss, samt der Drehstellung, in der sie steht, gefunden. Im Zuge eines derartigen erfolgreichen Abgleichs lassen sich dann gleich auch Steckerverbindungen rekonstruieren.

Nun fehlen noch Lage und Stellung der mittleren und der linken Walze. Zu ihrer Bestimmung bedient sich Rejewski zunächst einer manuellen Methode. Er testet auf einer der nachgebauten Enigmas alle 1.352 Maschinenstellungen händisch aus, die die verbleibenden beiden Walzen zur bereits identifizierten rechten Walze einnehmen können. An jeder der Stellungen tippt er die sechs Chiffren aktueller Spruchschlüssel ein, bis zwei Mal hintereinander dieselben drei Buchstaben auftauchen – der Spruchschlüssel. Ist dies der Fall, kann er sichergehen, Klartext vor sich zu haben, und das bedeutet nicht weniger, als dass die Walzen der Nachbau-Enigma, mit der er arbeitet, an der gesuchten Schlüsselstellung stehen.
Um den Ablauf zu beschleunigen, ersetzt Rejewski in weiterer Folge die händische Suchmethode durch einen Katalog, nach dessen Fertigstellung er die gesuchten Walzen und ihre jeweilige Stellung relativ einfach nachschlagen kann.
Was ihm jetzt noch fehlt, sind die aktuellen Ringstellungen. Um sie herauszufinden, bedient er sich der so genannten *„ANX"*-Methode. Aus Erfahrung weiß er mittlerweile, dass viele deutsche Sprüche streng korrekt mit *ANX* beginnen – nämlich *„AN"* zur Adressierung des Empfängers und *„X"* anstelle einer Leerstelle vor dem darauffolgenden Namen. Die Anredephrase ist naturgemäß auch immer an der in etwa gleichen Stelle positioniert, nämlich am Beginn der Nachricht.
Rejewski sucht also einen chiffrierten Funkspruch, von dem er annimmt, dass er diese Anredefloskel enthält. Und um die drei Chiffren zu finden, hinter denen sich die Klarbuchstaben *ANX* verbergen, rattert er alle 17.576 möglichen Maschinenstellungen von *01-01-01* bis zu *26-26-26* im Schnelldurchgang durch. Er hält dazu die Taste der ersten Chiffre gedrückt und dreht gleichzeitig die rechte Walze fortlaufend um je einen Drehschritt weiter, bis am Anzeigefeld ein *A* aufleuchtet. Beim Eintippen der nächsten Chiffre müsste ein *N* aufleuchten, so es sich um die gesuchte Maschinenstellung handelt. Ist dies nicht der Fall, geht er einen Drehschritt zurück, hält weiter die erste Chiffre gedrückt bis zum nächsten *A* und probiert neuerlich, ob ein *N* folgt. Er wiederholt dies so lange, bis anschließend bei gedrückter zweiter Chiffre ein *N* auftaucht. Leuchtet



11 *Die Einstellung der Ringe verschleiert den Schlüsssel*

N auf und unmittelbar danach bei gedrückter dritter Chiffre auch noch *X*, hat er eine Stellung innerhalb der Maschinenperiode gefunden, die *ANX* liefert. Derer kann es jedoch mehrere geben, von denen nur eine die gesuchte Schlüsselstellung darstellt. Ob er die richtige gefunden hat, kann Rejewski ausprobieren, indem er weitere Chiffren des betreffenden Spruchs eintippt. Entsteht Klartext, ist er am Ziel. Dann hat er die Stellung des Spruchschlüssels gefunden, die sich mangels der Ringstellungen freilich noch nicht benennen lässt. Allerdings lassen sich jetzt die Ringe folgendermaßen nachjustieren: Steht die auf die neutralen Ringstellungen *01-01-01* eingestellte Nachbau-Enigma beispielsweise auf *C-C-F* und der echte Spruchschlüssel lautet gemäß dem zugehörigen Funkspruch etwa *G-G-H*, so bilden die Differenzwerte die gesuchten Ringstellungen *05-05-03* (neutrale Ringstellung *01-01-01* plus vier bzw. vier bzw. zwei Drehschritte).
Damit hat Rejewski nach der Enigma selbst auch ihre Schlüssel entzaubert. Es ist eine außergewöhnliche Leistung des jungen Mathematikers, ohne Zweifel. Aber natürlich profitiert er maßgeblich von dem Umstand, dass die deutsche Chiffrierstelle lange Zeit hindurch keine wesentlichen

Änderungen im Schlüsselverfahren vollzieht. Das erst ermöglicht ihm, seine Berechnungen Schritt für Schritt zu vollenden.
Für die polnische Führung ist der Erfolg von unschätzbarem Wert. Man ist trotz eines bestehenden Nichtangriffspakts mit Deutschland misstrauisch und bemüht, die dort vor sich gehende Aufrüstung genau zu beobachten, um abschätzen zu können, wann das Land kriegsbereit sein wird.
Die Entzifferung der Funksprüche stellt eine willkommene Möglichkeit dar, dem feindseligen Nachbarn in die Karten zu blicken. Dazu wird das Biuro Szyfrów in Warschau um einige Kryptologen aufgestockt, um fortan rund um die Uhr zu arbeiten. Es ist ein Kampf gegen einen geheimen, zunehmend stärker werdenden Gegner. In den folgenden Jahren verzeichnen Rejewski und seine Kollegen immer wieder Verschärfungen des Enigma-Schlüsselverfahrens, deren jede innerhalb kürzester Frist bewältigt werden muss, um den überlebenswichtigen Zugang zum deutschen Funkverkehr nicht zu verlieren.

H. Dv. g. 13
L. Dv. g. 13

Prüf-Nr. 967

Geheim!

Gebrauchsanleitung

für die

Chiffriermaschine Enigma

Vom 12. 1. 1937

Berlin 1937
Gedruckt in der Reichsdruckerei

Aufrüstung der Enigma
für den Kriegseinsatz

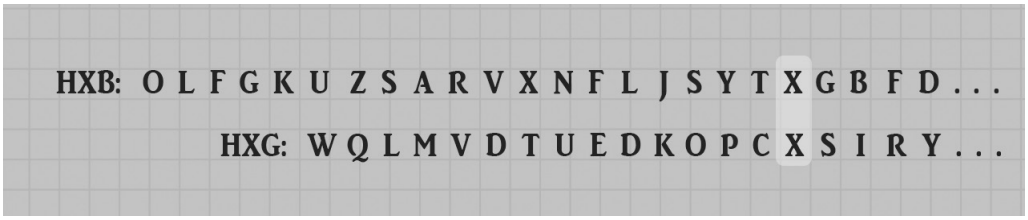
Der deutsche Reichskanzler Adolf Hitler lässt seinen Generälen gegenüber keine Zweifel daran, die Versailler Friedensverträge aufkündigen und einen neuerlichen Krieg beginnen zu wollen. Er will die Niederlage von 1918 revidieren und in Osteuropa *„Lebensraum für das deutsche Volk"* erobern. Noch aber ist die Reichswehr zu schwach für Militäraktionen. Bedächtiges Auftreten sei nötig, warnen die Generäle, um keine Maßnahmen der Gegner zu provozieren, sowie beständiges Weiterrüsten, um zu gegebener Zeit für den Krieg bereit zu sein. Bis 1938 will man über eine gut ausgerüstete Streitmacht von einer halben Million Mann verfügen, zu deren Lenkung eine speziell ausgebildete Nachrichtentruppe aufgestellt wird. Ihr wird die Aufgabe übertragen, Vorkehrungen für einen reibungslosen Nachrichtenverkehr im Kriegsfall zu treffen. Das im Hinterland sitzende Oberkommando soll jederzeit mit Kommanden der Armeen an diversen Fronten Verbindung halten können. Darüber hinaus sind die zahlreichen, über das ganze Reichsgebiet verstreut entstehenden militärischen Niederlassungen in das Netzwerk einzubinden, damit sie untereinander über Telefon- und Fernschreibleitungen, aber auch per Funk kommunizieren können. Der überwiegende Teil des Nachrichtenverkehrs soll zwar über Drahtleitungen abgewickelt werden, die als relativ sicher gelten. Doch müssen natürlich auch Vorbereitungen für den Funkverkehr getroffen werden, der schwerer zu organisieren und riskanter, oft aber unverzichtbar ist. So bedarf es eines regulierenden Frequenzplans, der verhindert, dass sich die zahllosen vorgesehenen Funkstationen gegenseitig stören. Das Personal ist entsprechend auszubilden und eine möglichst unangreifbare Verschlüsselung des Nachrichtenverkehrs sicherzustellen, wofür unter anderem Enigmas in großer Zahl hergestellt und in Betrieb genommen werden. Es sind Enigmas ganz unterschiedlichen Typs, die bei Institutionen wie der Reichsbahn, dem Geheimdienst *„Abwehr"* oder den Wehrmachtteilen Verwendung finden, was hauptsächlich dem Bemühen entspringt, die eigene Schlüsselsicherheit durch Abschottung von den anderen zu erhöhen. Dieser Abschottung steht jedoch die Notwendigkeit entgegen,

dass verschiedene Truppenteile möglichst rasch und einfach miteinander kommunizieren können sollen. Aus diesem Grund erhält ab Juni 1935 die Kriegsmarine, die bislang ein eigenes Enigma-Modell verwendet hat, dasselbe Modell, das Heer und Luftwaffe verwenden. Dadurch wird verschlüsselte Kommunikation zwischen den drei Wehrmachtteilen deutlich erleichtert; es müssen lediglich dieselben Tagesschlüssel benutzt werden.
Die Verwendung eines gemeinsamen Systems birgt freilich Gefahren. Gelingt dem Gegner bei einem der Wehrmachtteile ein Einbruch, sind die beiden anderen ebenfalls bedroht. Vor allem seitens der Kriegsmarine zeigt man sich besorgt, dass die Verwendung derselben Enigma das allgemeine Sicherheitsniveau senke, was insbesondere Marine-Einheiten gefährde, die auf keinen Alternativkanal ausweichen könnten. Schließlich stellt Funk die einzige Möglichkeit dar, zu und zwischen Schiffen und Booten auf See Kontakt zu halten. Zur Kompensation erhält die Marine zusätzliche Schlüsselwalzen. Während die Enigma von Heer und Luftwaffe über die Walzen *I* bis *III* verfügt und ihre Schlüssel somit auf einer von sechs möglichen Walzenlagen basieren, hat die Marine neben den Walzen *I* bis *III* auch die Nummern *IV* und *V* zur Verfügung, wodurch 60 verschiedene Lagen möglich sind. Das bedeutet für allfällige Entschlüsselungsversuche immerhin eine Verzehnfachung des Aufwands. Zugunsten höherer Funksicherheit bedient sich die Marine überdies einer weitaus komplizierteren Verfahrensweise beim Verschlüsseln, genannt *„Schlüssel M"*, der sich den Entschlüsselungsversuchen der Polen weitgehend entzieht.
Im Hinblick auf einen Kriegsfall bildet aber vor allem auch die zu erwartende Zunahme des Funkaufkommens ein erhebliches Geheimhaltungsproblem. Je mehr Funksprüche der Gegner auffangen kann, die auf ein und denselben Schlüssel zurückgehen, umso leichter kann er in diesen Schlüssel einbrechen. Um die Menge an Funksprüchen eines Schlüssels möglichst gering zu halten, werden Anfang 1936 für verschiedene Institutionen wie Behörden, Führungsstäbe, das Heer oder SS-Einheiten unterschiedliche Schlüsselkreise gebildet. Es entstehen horizontale Kreise etwa zum Nachrichtenaustausch zwischen einzelnen zusammengefassten Führungsstellen, sowie vertikale, die den Nachrichtenverkehr von den höchsten zu den unteren Stellen einer Einheit umfassen. Für jeden dieser Kreise werden eigene Tagesschlüssel ausgegeben – wie bisher in Form gedruckter Unterlagen und meist für einen Monat im Voraus –, doch wird die Verfahrensweise verschärft. Die Walzenlage wird ab Anfang 1936 monatlich geändert und ab Oktober 1936 wie die Ringstellungen, die Grundstellung der Walzen sowie die Steckerverbindungen (deren Zahl von sechs auf bis zu acht steigt) täglich.

Das Chiffrieren bleibt beim Alten. Der Heeres-Schlüssler wählt einen beliebigen Spruchschlüssel – drei Buchstaben, bei denen es sich um keine leicht erratbare Kombination handeln darf. Die gewählten Buchstaben werden auf der Enigma zweimal hintereinander eingetippt, die entstehenden sechs Chiffren notiert. Danach stellt der Schlüssler wie üblich die drei Walzen auf die gewählten Buchstaben ein und verschlüsselt mit dieser Einstellung die Nachricht. Die Chiffren werden auf dem dafür vorgesehenen Formular ebenfalls notiert und gehen dann an den Funker. Dieser sendet zunächst den *„Spruchkopf"*, der der eigentlichen Nachricht vorangestellt ist. Die entsprechenden Buchstaben, die unverschlüsselt abgesetzt werden, enthalten neben Datum und Uhrzeit eine Zahl, die für die Anzahl der Chiffren steht, inklusive der sechs Chiffren des Spruchschlüssels und der fünf Buchstaben der so genannten *„Kenngruppe"*. Zur Sicherheit hinsichtlich atmosphärischer Störungen wird jedes der Elemente des Spruchkopfs doppelt gefunkt, denn sie enthalten wichtige Vorabinformation für den Empfänger. Durch die mitgelieferte Anzahl der Chiffren etwa soll er sicher sein können, den Spruch zur Gänze aufgenommen und nichts versäumt zu haben. Eine ähnliche Funktion hat die *„Kenngruppe"*, die ihm auf den ersten Blick anzuzeigen hat, zu welchem Schlüsselkreis der Spruch gehört und welche Schlüsselunterlagen zu seiner Entschlüsselung nötig sind. Handelt es sich um eine fremde Kenngruppe, kann er sich jede weitere Mühe sparen, denn dann kann er ihn mit seinen Schlüsselunterlagen nicht entziffern. Damit die Kenngruppe diese Funktion erfüllen kann, steht sie an einem bestimmten Platz innerhalb des Funkspruchs, nämlich an einer in den Schlüsselunterlagen vorbestimmten, täglich wechselnden *„Kenngruppen-Einsatzstelle"*. Bei *„Einsatzstelle 1"* ist sie ans Ende des Spruchkopfs und vor die sechs Chiffren des Spruchschlüssels zu setzen, auf welche dann die Chiffren der eigentlichen Nachricht folgen, angeordnet allesamt in Fünfergruppen. Bei *„Einsatzstelle 2"* steht sie hinter den ersten fünf Chiffren des Spruchschlüssels, die sechste folgt dann nach ihr.
Um im Chiffrebild nicht herauszustechen, ist die Kenngruppe ebenfalls fünfstellig, wobei die ersten beiden Buchstaben bloße Füllbuchstaben darstellen, beliebig gewählt vom Schlüssler. Die folgenden drei stammen aus der gedruckten *„Kenngruppentafel"*, die Teil der Schlüsselunterlagen ist. Sie bietet dem Schlüssler für jeden Tag einige solcher Gruppen zur Auswahl, die jeweils aus drei Buchstaben bestehen. Zur besseren Tarnung sind diese Gruppen für verschiedene Funksprüche abwechselnd zu verwenden und deren drei Buchstaben in ihrer Reihenfolge zu variieren. Diese Vorgangsweise ist auch für die Teile eines mehrteiligen Funkspruchs anzuwenden, denn längere Mitteilungen sind grundsätzlich zu unterteilen, um der Gegenseite möglichst wenig Chiffren zu bieten, die auf denselben Schlüssel zurückge-

hen. Ein einzelner Funkspruch darf anfangs nicht mehr als 180 Buchstaben aufweisen. Für jeden neuen Spruch sowie für jeden Teil eines Spruchs ist in analoger Weise übrigens auch ein neuer Spruchschlüssel zu wählen.

Die von polnischen Funkhorchstationen in Posen, in der Nähe von Krakau, sowie in Starograd in Pommern aufgenommenen deutschen Funksprüche werden zum Entschlüsseln nach Warschau gebracht. Dort werden sie samt zusätzlichen Informationen wie den von deutschen Einheiten verwendeten Rufzeichen, mit denen sich die Stationen untereinander zu erkennen geben, sowie Zeiten und Frequenzen, zu und auf denen sie senden, katalogisiert. Vermerkt werden auch Eigenheiten einzelner Funker, an denen diese wiedererkannt werden können. Schließlich entwickeln Funker so etwas wie eine individuelle Handschrift beim Morsen, und Horcher ein geschultes Ohr für derartige Besonderheiten. Dank solcher Zusatzinformationen lassen sich mitunter militärische Verbände identifizieren und Schlussfolgerungen hinsichtlich ihrer Bewegungen ziehen.
Was die Entzifferungsarbeit betrifft, vervielfacht sich der Aufwand, muss doch jetzt jeder Schlüsselkreis für sich gebrochen werden. Außerdem wird das Eindringen umso schwieriger, je weniger Chiffren pro Schlüsselkreis für die Auswertung zur Verfügung stehen. Und durch die Erhöhung der Steckerverbindungen auf bis zu acht funktioniert Rejewskis Rastermethode zur Bestimmung der rechten Walze kaum noch. An deren Stelle tritt eine neue Methode, *„metoda zegara"* genannt, also Uhrenmethode, die sein junger Kollege Jerzy Różycki entwickelt. Sie basiert auf der statistischen Häufigkeit von Buchstabenwiederholungen in deutschen Texten, genauer auf der Tatsache, dass bei zwei beliebigen, untereinander geschriebenen Texten durchschnittlich alle 13 Stellen dieselben Buchstaben untereinander zu liegen kommen. Dies gilt auch für Enigma-Chiffren, wenn sie demselben Schlüssel entstammen, während dies bei Chiffren unterschiedlicher Schlüssel nur halb so oft vorkommt. Da ein Übertrag auf diese Statistik wie ein Schlüsselwechsel wirkt, versucht Różycki zwei Funksprüche zu finden, zwischen denen ein Übertrag erfolgt ist, um Rückschlüsse auf die Walze zu ziehen, die ihn verursacht hat und deshalb rechts liegen muss.
Er sucht dazu zunächst in aufgefangenen Funksprüchen, von denen er die Spruchschlüssel bereits entziffert hat, nach solchen, die auf Enigmas mit fast gleicher Ausgangsstellung chiffriert worden sind; Funksprüche wie etwa die mit den Spruchschlüsseln *H-X-B* und *H-X-G*. Diese beiden gehen auf identische Stellungen der linken und der mittleren Walze zurück *(H-X)*, und die Stellungen der rechten Walze liegen um gezählte fünf Drehschritte (von *B* bis *G*) auseinander. Er schreibt nun die beiden Funksprüche um die Differenz dieser fünf Drehschritte verschoben untereinander. Solcherart auf



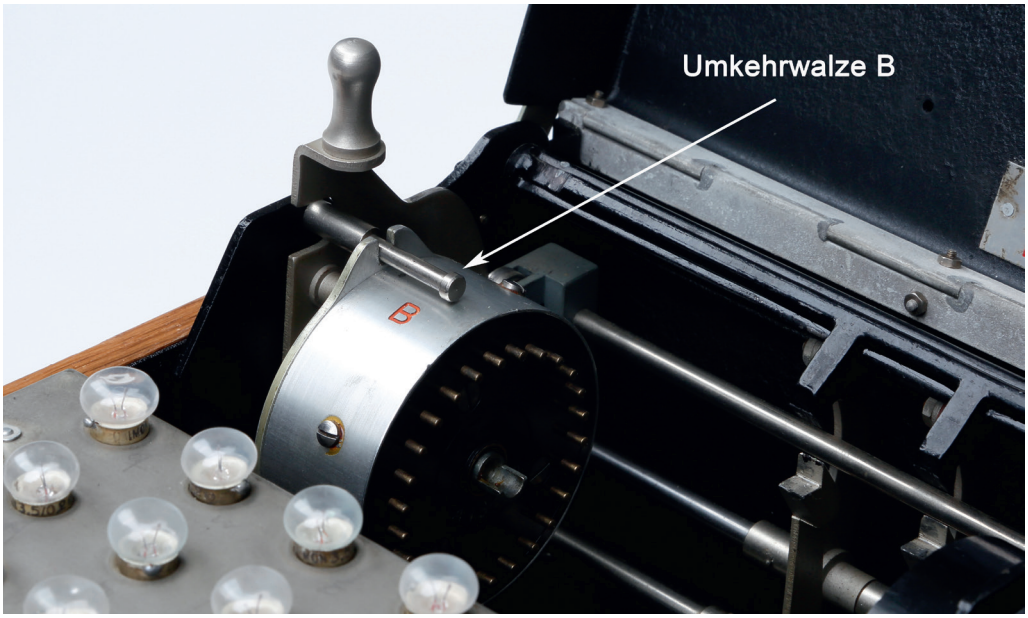
13 *Synchronisierte Funksprüche der Uhrenmethode*

dieselbe Maschinenstellung synchronisiert, lassen sich ihre Chiffren über Dutzende Stellen hinweg daraufhin untersuchen, wie oft gleiche Buchstaben untereinander zu liegen kommen. Ist die Häufigkeit geringer als im Normalfall, ist dies ein Hinweis darauf, dass zwischen den beiden untersuchten Sprüchen ein Übertrag stattgefunden hat. Ist dies der Fall, muss es zwangsläufig im Differenzbereich der beiden Maschinenzustände (also innerhalb der fünf Drehschritte) geschehen sein. Im vorliegenden Fall lässt sich die rechts liegende Walze letztlich als Walze *II* identifizieren, denn bei ihr sitzt der Übertrag bekanntermaßen zwischen *E* und *F*, was innerhalb der untersuchten fünf Drehschritte *B* bis *G* liegt.
Die neue Methode funktioniert passabel und ist für die Arbeit der polnischen Gruppe überaus bedeutsam, nachdem die Walzenlage mittlerweile täglich aufs Neue herauszufinden ist.

Angesichts drohender Verschärfungen des Enigma-Schlüsselverfahrens denkt Rejewski aber auch über eine neue, umfassende Methode zum Schlüsselbrechen nach. Es soll eine Methode sein, bei der er nicht auf das Erraten von Spruchschlüsseln angewiesen ist. Er muss schließlich damit rechnen, dass es den Deutschen irgendwann gelingen wird, diese offenkundige Schwachstelle zu beseitigen. Rejewski sucht und findet einen gänzlich anderen Zugang zu den geheimnisvollen Mechanismen der Enigma.
Nach der Analyse zahlreicher Funksprüche eines Tages erkennt er, dass die Maschine innerhalb der sechs Stellen der Spruchschlüssel richtiggehende Chiffrezyklen erzeugt.[5] Wenn etwa in einem Funkspruch ein *F* an der ersten Stelle zu einem *W* an der vierten Stelle wird, und sich an einem anderen Funkspruch zeigt, dass aus einem *W* an der ersten Stelle beispielsweise ein *Y* an der vierten wird und aus einem weiteren, dass aus dem *Y* an der ersten Stelle etwa ein *E* an der vierten wird, entsteht ein derartiger Zyklus, der sich letztlich schließt, wenn nämlich die letzte seiner Chiffren, angenommen das *E*, an der ersten Stelle eines Spruchs zu einem *F* an der vierten und damit wieder zur Ausgangschiffre wird. Der – in diesem Fall –

[5] Siehe im Abschnitt *Kryptologie* das Kapitel *Charakteristische Transformationen und Zyklen*

vierstellige Zyklus lautet dann: *F/W/Y/E*. Analysiert man die ersten und die vierten Stellen von Funksprüchen eines Tages, erhält man mehrere solcher Zyklen, die immer in geradzahliger Anzahl auftreten, eine Länge von eins bis dreizehn aufweisen und insgesamt immer alle 26 Buchstaben des Alphabets enthalten. Ein derartiger Zyklensatz könnte folgendermaßen aussehen: *(F/W/Y/E) (A/C/R/K) (V) (T) (M/H/P/U/J/D/B/O) (Z/Q/L/X/S/G/I/N)*.
Solche Zyklensätze lassen sich auch an den zweiten und fünften sowie den dritten und sechsten Spruchschlüsselstellen herleiten.
Mit diesen Zyklen hat Rejewski Charakteristika gefunden, die der Tageseinstellung der Enigma entspringen und deshalb zur Rekonstruktion des Tagesschlüssels herangezogen werden können. Er verzeichnet in weiterer Folge alle Zyklen, die an den mehr als 105.000 Maschinenstellungen entstehen, in einem umfassenden Katalog. Zur rascheren Erstellung lässt er bei der Warschauer Firma, die bereits die Nachbau-Enigmas gefertigt hat, ein aus zwei verschalteten Enigma-Walzensätzen bestehendes *„Zyklometer"* bauen, das die Arbeit beschleunigt.
Nach einjähriger Tätigkeit ist der Katalog komplett. Er enthält Anzahl und Länge der Zyklen aller auftretenden Zyklensätze und macht das alltägliche Schlüsselbrechen vergleichsweise einfach. Zunächst werden die charakteristischen Zyklen des Tages gebildet und der entstehende Zyklensatz – etwa *(F/W/Y/E) (A/C/R/K) (V) (T) (M/H/P/U/J/D/B/O) (Z/Q/L/X/S/G/I/N)* – im Katalog nachgeschlagen. Dabei wird jedoch nicht nach Ähnlichkeiten mit den darin auftretenden Chiffren gesucht, da diese durch Stecker verwürfelt sind, sondern nach Zyklensätzen, die gleich viele und gleich lange Zyklen besitzen. Im vorliegenden Beispiel müssen sie aus sechs Zyklen bestehen – nämlich zwei Vierer-, zwei Einser- und zwei Achterzyklen. Im Katalog finden sich dann zumeist mehrere Varianten mit diesen Eckdaten, deren jede zu überprüfen ist, ob sie die gesuchte Schlüsselstellung repräsentiert. Dazu werden die Stecker rekonstruiert, und zwar durch einen Abgleich der Buchstaben der aktuellen charakteristischen Zyklen, welche durch Stecker verwürfelt sind, mit den Zyklen der gerade untersuchten Variante aus dem Katalog, die dazu auf einer ungesteckten Enigma erzeugt werden. Sind die gesteckten Buchstaben erkannt, können sie in der untersuchten Variante eingesetzt werden, um zu testen, ob sie Klartext liefert. Ist dies der Fall, kann Rejewski an der Nachbau-Enigma, an der er arbeitet, Walzenlage samt Stellungen der Walzen, also die gesuchte Schlüsselstellung, ablesen. Liefert die Variante keinen Klartext, prüft er weiter, bis er die richtige gefunden hat. Rejewski und seine Kollegen haben damit das deutsche Rätsel neuerlich gelöst.
Im November 1937 erleiden sie jedoch einen schweren Rückschlag, als die deutsche Seite eine neue Umkehrwalze B einführt, die über eine andere



14 *Rückschlag für die polnischen Mathematiker: die neue Umkehrwalze B*

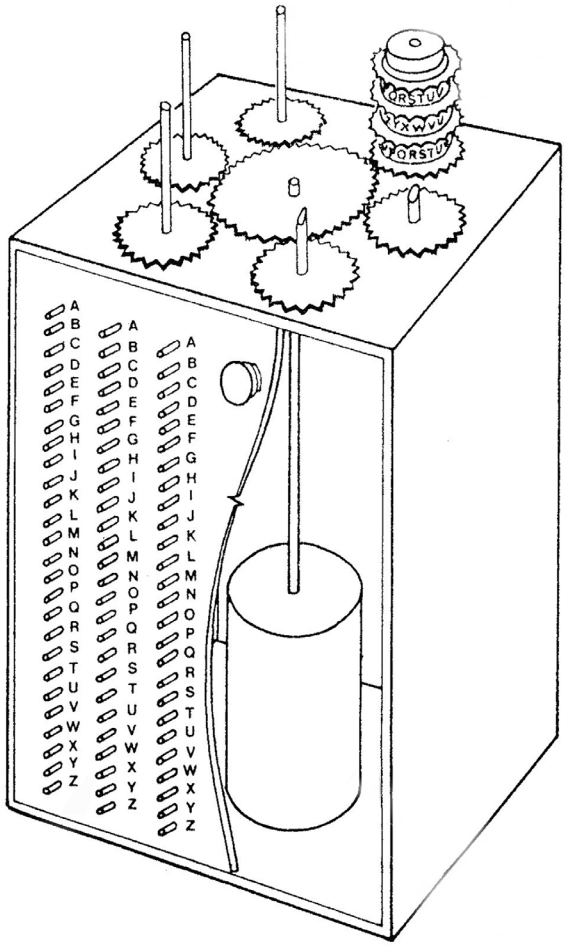
Verdrahtung verfügt als ihre Vorgängerin. Der mühsam hergestellte Zyklenkatalog ist jetzt nutzlos. Die neue Umkehrwalze muss berechnet und ein neuer Katalog erstellt werden. Dabei haben die jungen polnischen Mathematiker noch gehöriges Glück im Unglück. Dank des Umstands, dass die Verdrahtungen der drei Schlüsselwalzen unverändert bleiben, sind sie in der Lage die Umkehrwalze zu berechnen. Und ihnen kommt zugute, dass sie dezidiert wissen, dass es die Umkehrwalze ist, die sich geändert hat, nachdem sie zuvor einen deutschen Funkspruch entziffert haben, der alle Schlüssler daran erinnert, am 1. November um 00.00 Uhr die neue Umkehrwalze in ihren Enigmas zu montieren.

Mit der zunehmenden Verschärfung der außenpolitischen Lage gewinnt die Entschlüsselungsarbeit an Brisanz. Aus Furcht vor Spionage übersiedelt das Referat des polnischen Chiffrierbüros in ein eigenes Gebäude in Pyry in einem Waldgebiet außerhalb von Warschau. Hier finden Rejewski und seine Kollegen Räumlichkeiten vor, in denen sie mit ihren Zyklometern, Enigmas und Kartotheken ungestört und abgeschirmt arbeiten können. Es ist ein streng geheimes Projekt. Allen Beteiligten ist es kategorisch untersagt, außerhalb dieser Räume über ihre Arbeit zu sprechen, um zu vermeiden, dass deutsche Agenten etwas aufschnappen und Berlin

alarmieren könnten. Würde dies geschehen, würden die Deutschen mit Sicherheit ihr Verschlüsselungsverfahren grundlegend ändern und sämtliche bisherigen Anstrengungen wären vergebens. Die Geheimhaltung geht so weit, dass selbst Abteilungen des polnischen Generalstabs erst nach und nach davon erfahren, woher die Nachrichten stammen, die ihnen regelmäßig zugetragen werden. Es gilt, die vielversprechende Geheimwaffe um jeden Preis zu schützen.
Im Januar 1938 steht ein zweiwöchiger Test am Programm, der die Effizienz der Entschlüsselung unter kriegsmäßigen Bedingungen zeigen soll. Das Ergebnis fällt zufriedenstellend aus: Ein Großteil der aufgefangenen Enigma-Funksprüche kann entschlüsselt werden, obwohl manche durch atmosphärische Störungen entstellt oder unvollständig sind. Was Rejewski und seine Kollegen nicht wissen, ist, dass die Verantwortlichen des Biuro Szyfrów über zahlreiche aktuelle Schlüsselunterlagen verfügen, die der deutsche Spion Schmidt in den vergangenen Jahren geliefert hat. Man hat ihnen diese Unterlagen vorenthalten, um sie zu zwingen, funktionierende Methoden zu entwickeln, die man für den Fall eines Krieges, wenn mit Spionagematerial nicht mehr zu rechnen sei, bitter nötig haben würde.
Indessen wächst die Bedrohung durch das Deutsche Reich stetig. Im März 1938 erfolgt der *„Anschluss"* Österreichs durch den Einmarsch deutscher Truppen. Das nächste Opfer ist die Tschechoslowakei. Hitler fordert eine Angliederung der tschechischen Sudetengebiete an Deutschland. England und Frankreich stimmen zu, um einen Krieg zu vermeiden. Die Regierung in Prag muss sich fügen. Im Oktober wird das Sudetenland durch Truppen der deutschen Wehrmacht besetzt. In Warschau beobachtet man das Heranrücken des Hitlerstaates an die eigenen Grenzen mit wachsender Sorge.

Im Hinblick auf einen möglichen Kriegsausbruch verschärft die Chiffrierstelle in Berlin das Enigma-Schlüsselverfahren erneut. Man geht gänzlich davon ab, Grundstellungen in den Schlüsselunterlagen auszugeben, um zu verhindern, dass der Gegner allzu leicht in alle Funksprüche eines Tages einbrechen kann, wenn ihm ein einzelner Einbruch gelingt. Jeder Schlüssler muss nun wie den Spruchschlüssel auch die Grundstellung frei wählen, und zwar für jeden Funkspruch wie für alle Teile von mehrteiligen Funksprüchen. Grundstellung und Spruchschlüssel dürfen dabei nie identisch sein.
Die Vorgangsweise beim Chiffrieren ändert sich geringfügig. Der Schlüssler stellt die – nunmehr frei gewählte – Grundstellung auf seiner Maschine ein und chiffriert dann wie üblich den ebenfalls frei gewählten Spruchschlüssel, indem er ihn zwei Mal hintereinander eintippt. Die entstehenden

sechs Chiffren werden auf dem Funkformular notiert. Danach wird die Enigma auf den Spruchschlüssel eingestellt, um mit dieser Einstellung, wie üblich, die eigentliche Nachricht zu chiffrieren. Die entstehenden Chiffren werden ebenfalls notiert. Vorneweg am Formular steht wie bisher der Spruchkopf, der nun allerdings auch die drei Klarbuchstaben der Grundstellung enthält, die jetzt – da frei gewählt – mitgefunkt werden muss. Genau genommen, sind es sechs Buchstaben, da die Grundstellung zur Sicherheit zweimal hintereinander gefunkt wird.
Obwohl die Grundstellung klar gefunkt wird, können die polnischen Kryptologen damit nichts anfangen, solange sie die anderen Einstellungen des Tagesschlüssels nicht kennen. Damit nicht genug, können bei frei gewählten Grundstellungen auch keine Spruchschlüssel mehr erraten werden, weil die verräterischen Häufungen nicht mehr auftreten. Dadurch lassen sich auch keine Zyklensätze mehr herleiten. Mit einem Schlag sind fast alle bisherigen Methoden hinfällig. Das Einzige, worauf Rejewski noch zurückgreifen kann, sind die so genannten Ein-Buchstaben-Zyklen, kurz Einserzyklen. In diesen Fällen stehen an der ersten und vierten oder an der zweiten und fünften oder aber an der dritten und sechsten Stelle des Spruchschlüssels eines Funkspruchs dieselben Chiffren, etwa: *HYEHOQ* oder *FGELGC* oder *DKATWA*. Dieses Phänomen der Einserzyklen tritt irregulär und insgesamt bei rund 40 Prozent aller Maschinenstellungen der Enigma auf. Man könnte also versuchen, einen Funkspruch, dessen Spruchschlüssel einen Einserzyklus aufweist, anhand dieses Einserzyklus in der Maschinenperiode zu lokalisieren, um die Schlüsselstellung herauszufinden. Dazu müsste man im schlechtesten Fall jeden der 42.000 Einserzyklen auf einer Enigma daraufhin überprüfen, ob es sich um den gesuchten handelt. Das ist eine sehr große Zahl an abzuarbeitenden Fällen, wenngleich deutlich weniger als die Hälfte der über 105.000 Möglichkeiten insgesamt. Händisch würde dies dennoch viel zu lang dauern, weshalb Rejewski eine elektromechanische Maschine – die sogenannte *„Bomba"* – ersinnt, die diese Arbeit schneller erledigt. Innerhalb weniger Wochen wird die neue Maschine von der Warschauer Radiobaufirma, die schon die Enigmas und das Zyklometer hergestellt hat, gebaut.
Die Bomba soll die Maschinenperiode der Enigma auf der Suche nach Einserzyklen schnellstmöglich durchrattern. Um aber die Anzahl der zu überprüfenden Fälle von zigtausenden auf eine überschaubare Menge zu reduzieren, lässt Rejewski sie nicht bei jedem einzelnen Einserzyklus anhalten, sondern nach drei Einserzyklen gleichzeitig suchen. Er macht sich dabei den Umstand zunutze, dass Einserzyklen in der Maschinenperiode in irregulären Abständen zueinander auftreten. Die Abstände der gesuchten



15 *Die Bomba rattert alle möglichen Walzenstellungen der Enigma durch*

drei bilden also ein signifikantes Muster, doch ist wegen der nach wie vor unbekannten Ringstellungen noch unklar, wo in der Maschinenperiode es liegt. Dies herauszufinden, obliegt der Bomba. Sie soll ihren Suchlauf immer dann anhalten, wenn drei Einserzyklen in den gesuchten Abständen auftreten. Das kommt insgesamt allerdings noch gut tausendmal vor – viel zu oft, um alle Fälle auf einer Enigma händisch überprüfen zu können. Rejewski senkt deshalb die Zahl an zu überprüfenden Fällen noch weiter, indem er drei besondere Einserzyklen verwendet, nämlich solche, die aus dem gleichen Buchstaben – etwa *H* – bestehen. Dabei nimmt er an, dass *H* ungesteckt ist (was immerhin in rund der Hälfte aller Fälle zutrifft), da ansonsten die weiteren Entzifferungsschritte nicht funktionieren würden.

Zur Umsetzung eines solchen Suchlaufs verfügt die Bomba über drei Paare an Enigma-Walzensätzen, die miteinander gekoppelt sind. Am ersten Walzensatz eines Paares wird die Grundstellung des ersten der drei Funksprüche, nach deren Einserzyklen gesucht wird, eingestellt – etwa *D-N-W*. Am zweiten Satz wird dieselbe Grundstellung um drei Stellen vorgerückt eingestellt – also *D-N-Z*. Die Differenz entspricht dem Abstand zwischen erster und vierter Stelle (bzw. zweiter und fünfter oder dritter und sechster, wenn es sich um Einserzyklen des entsprechenden Typs handelt). Diese Differenz dient dazu, einen im Zuge des Suchlaufs gefundenen Einserzyklus durch gleichzeitiges Erscheinen seiner beiden gleichen Buchstaben auf den beiden Walzensätzen sichtbar werden zu lassen. In analoger Weise werden an den verbleibenden zwei Walzensatzpaaren die Grundstellungen der zwei anderen Funksprüche eingestellt. Auf diese Weise erhalten alle drei Grundstellungen einen gemeinsamen Startpunkt, wodurch auch die gesuchten drei Einserzyklen gleichzeitig auftauchen müssen.
Nach dem Start der Bomba laufen die gekoppelten Walzensatzpaare die Maschinenperiode durch, um die drei Einserzyklen zu finden. Da die beiden *Hs* in jedem der untersuchten Einserzyklen gleichen, wenn auch unbekannten, Klarbuchstaben entsprechen müssen, und umgekehrt, wird mit jedem Schritt ein *H* in die Walzensätze geschickt, bis an allen dreien Einserzyklen erscheinen. Kontrolllampen zeigen an, wenn dies der Fall ist. Ist es soweit, bleibt die Bomba stehen. Man kann dann die Stellungen der Walzen an einem der Walzensätze ablesen – angenommen *B-J-T* –, diese auf einer Enigma einstellen und testen. Dazu sucht Rejewski nach Spruchschlüsselchiffren eines aktuellen Funkspruchs, die, in die Enigma eingetippt, zwei idente Dreierbuchstabenkombinationen – also die Klarbuchstaben eines Spruchschlüssels – ergeben. Erscheinen solche, bedeutet das, dass die gefundene Stellung die gesuchte Schlüsselstellung darstellt. Die noch fehlenden Ringstellungen leitet Rejewski aus der Differenz der ursprünglich aufgefangenen Grundstellung, etwa *D-N-W,* und der auf der Bomba gefundenen, *B-J-T,* ab. Es sind zwei Drehschritte zwischen *D* und *B*, vier zwischen *N* und *J* und drei zwischen *W* und *T*. Die Ringstellungen lauten demnach: *03-05-04* (neutrale Ringstellung *01-01-01* plus zwei bzw. vier bzw. drei Drehschritte). Nun kann Rejewski den gefundenen Spruchschlüssel exakt benennen, einstellen und damit den zugehörigen Funkspruch entschlüsseln.
Beim Eintippen der Chiffren kommt mitunter noch Buchstabensalat zum Vorschein, da nach wie vor Steckerverbindungen wirksam sind. Doch da und dort – wo es sich um nicht gesteckte Buchstaben handelt – finden sich auch leidlich lesbare Fragmente. Diese Fragmente machen es zumeist möglich, den Rest des Texts durch geschicktes Austauschen von Buchstaben zu

rekonstruieren und im Zuge dessen gleich auch die Steckerverbindungen zu identifizieren. Danach liegt der Tagesschlüssel der Enigma offen.[6]
Da im November 1938 in Pyry gleich sechs Bombas in Betrieb gehen, können Rejewski und seine Kollegen die sechs möglichen Walzenlagen parallel abarbeiten und alle Maschinenstellungen innerhalb von rund zwei Stunden prüfen. Sie haben die Enigma wieder unter ihre Kontrolle gebracht.

Die Bomba-Methode funktioniert jedoch nur so lange, als die Zahl der Steckerverbindungen relativ niedrig ist. Eine allfällige Erhöhung durch die deutsche Chiffrierstelle droht auch diese Methode wirkungslos werden zu lassen. Rejewskis Kollege Henryk Zygalski arbeitet deshalb an einer Methode, die zwar ebenfalls auf Einserzyklen basiert, jedoch den Vorzug hat, von Steckerverbindungen unabhängig zu sein. Anders als die Bomba benutzt Zygalski Funksprüche mit beliebigen Einserzyklen, die entsprechend leichter zu finden sind. Er arbeitet auch nicht mit einer Maschine, sondern mit großen gelochten Kartonbögen. Er will für jede der sechs Walzenlagen einen Satz aus 26 Bögen produzieren, in die alle in der Maschinenperiode der Enigma vorkommenden Einserzyklen gelocht werden. Auf jedem Bogen befindet sich eine Tabelle mit 26 Spalten für alle Drehstellungen einer der drei Walzen und 26 Zeilen für die Drehstellungen einer zweiten Walze (bei neutraler Ringstellung *01-01-01*). Der erste Bogen eines Satzes entspricht der ersten Drehstellung der dritten Walze. Dort, wo die drei Walzen Einserzyklen erzeugen, sind in die Felder der Tabelle Löcher gestanzt. Für die weiteren Drehschritte der dritten Walze entstehen 25 analoge Lochbögen. Da ein solcher Satz an Bögen, wie erwähnt, nur eine einzige Walzenlage abbildet, bedarf es insgesamt sechs verschiedener Sätze.
Grundsätzlich beruht Zygalskis Methode auf denselben Prinzipien wie jene der Bomba. Auch hierbei werden die Grundstellungen aktueller Funksprüche aneinander ausgerichtet, um ihre Einserzyklen gemeinsam erscheinen zu lassen, allerdings durch Lochkartons auf einem Lichttisch. Nachdem aber auch Zygalski weder die Lage der Walzen noch die Ringstellungen kennt, also auch nicht sagen kann, wo die Grundstellungen der Funksprüche innerhalb der Maschinenperiode liegen, muss er seine Suche auf gut Glück beginnen. Er startet mit einem beliebigen Kartonbogen. Lautet die Grundstellung des ersten untersuchten Spruchschlüssels etwa *C-B-A,* nimmt er der Einfachheit halber den Bogen *C* eines Kartensatzes und legt ihn auf den Lichttisch. Für die Grundstellung des nächsten Spruchs – *E-F-F* – muss er dann den Bogen *E* um vier Zeilen (von *B* auf *F*) nach oben und um fünf Spalten (von *A* auf *F*) nach links verschoben darüber legen. Infolge dieser Ausrichtung kommen die gemeinsamen Einserzyklen übereinander

[6] Siehe im Abschnitt *Kryptologie* das Kapitel *Maschinenpower: Bomba*

zu liegen, erscheinen als übereinstimmendes Loch, angezeigt durch das durchscheinende Licht. Nicht übereinstimmende Löcher werden überdeckt und erlöschen. Für einen weiteren Spruch mit der Grundstellung *G-H-I* wird der Bogen G gegenüber dem ersten Bogen – *C* – um sechs Zeilen nach oben (von *B* auf *H*) und um acht Spalten (von *A* auf *I*) nach links verschoben auf die beiden bereits ausgerichteten Bögen gelegt. Wieder verschwinden Löcher.

In der Regel muss Zygalski sechs, sieben Kartons am ersten Bogen ausrichten, um die Löcher im günstigsten Fall auf ein einziges zu reduzieren, das dann die gemeinsamen Einserzyklen repräsentiert. An einem solchen gemeinsamen Loch kann die gesuchte Schlüsselstellung abgelesen werden. Die Walzenlage wird an den verwendeten Kartonbögen ersichtlich und die Stellung der Walzen an der Position des Lochs. Die Ringstellungen schließlich lassen sich folgendermaßen herleiten: Liegt das gemeinsame Loch im Verhältnis zur Grundstellung des ersten Spruchs *C-B-A* etwa am Bogen *B* an der Koordinatenstelle *A-X*, entspricht dies gemäß der Differenz zwischen *C-B-A* und *B-A-X* den Ringstellungen *02-02-04* (neutrale Ringstellung *01-01-01* plus einen Schritt bzw. einen Schritt bzw. drei Schritte). Mit diesen Ringstellungen kann dann einer der aktuellen Spruchschlüssel entschlüsselt und mit seiner Hilfe der zugehörige Funkspruch entziffert werden. Wegen der Wirkung der Stecker erscheint freilich auch hier noch Chiffrechaos, doch ist es wie schon bei der Methode mit der Bomba mitunter möglich, durch geschicktes Austauschen bestimmter Buchstaben den Text zu rekonstruieren und dabei gleich auch die Stecker zu eruieren.

Zygalskis Methode mit den Lochkartons führt aber nicht immer sofort ans Ziel. Es ist nicht unwahrscheinlich, dass beim ersten Durchgang mit den Kartonbögen gar kein Loch übrig bleibt. Dann ist der beliebig gewählte Anfangsbogen – im obigen Fall *C* – falsch und das gesamte Prozedere muss, mit dem nächstfolgenden Bogen – in diesem Fall *D* – beginnend, wiederholt werden. Dabei sind für die anderen anzulegenden Funksprüche ebenfalls um eine Stelle vorgerückte Bögen zu verwenden, also statt dem Bogen *E* der Bogen *F* und statt dem Bogen *G* der Bogen *H* usw. Führt dieser Durchgang auch nicht zum Ziel, wird mit den nächsthöheren Bögen neuerlich von vorn begonnen. Die schrittweise Erhöhung entspricht dem Durchprobieren aller möglichen Ringstellungen, nachdem diese unbekannt sind. Aber selbst wenn alle 26 Bögen abgearbeitet und alle Ringstellungen getestet sind, muss noch immer kein Ergebnis vorliegen. Es kann nämlich sein, dass es sich beim untersuchten Lochkartensatz um den falschen Satz handelt. Schließlich repräsentiert jeder nur eine von sechs Walzenlagen. In diesem Fall muss die gesamte Prozedur mit dem nächsten Satz von vorn begonnen werden. Doch die Methode funktioniert.

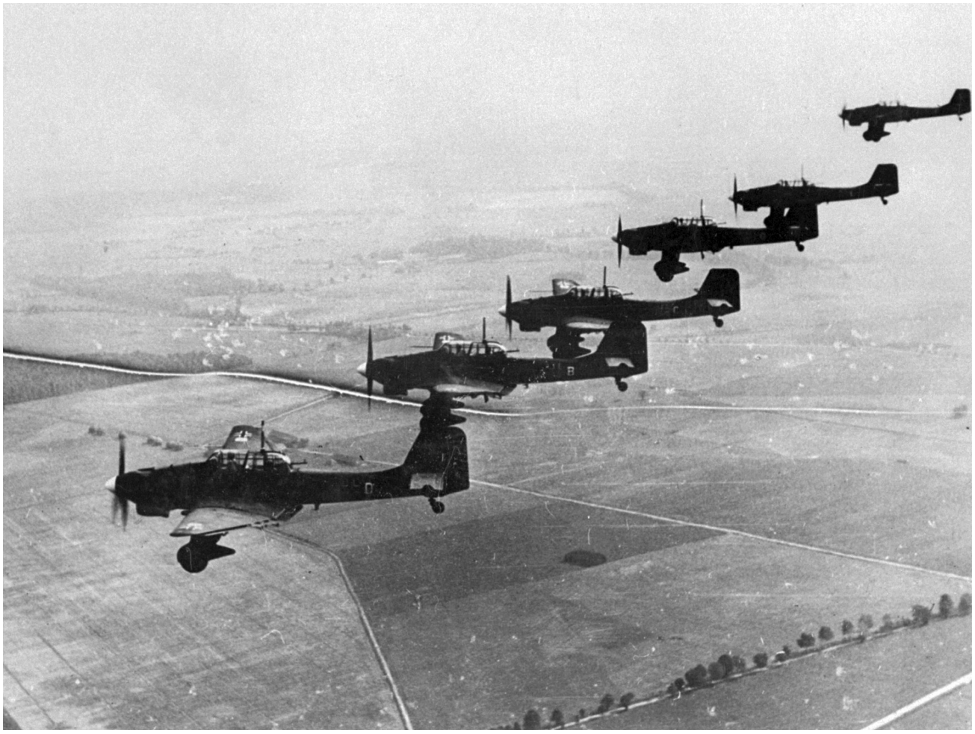
Der nächste Rückschlag folgt Ende des Jahres 1938, als die Schlüssler des deutschen Heeres und der Luftwaffe zusätzlich die Walzen *IV* und *V* einsetzen (die die Kriegsmarine schon seit geraumer Zeit in Verwendung hat). Nunmehr stehen also drei aus fünf Schlüsselwalzen zur Verfügung (während die Kriegsmarine ihren Sicherheitsvorsprung durch Verwendung zweier weiterer Walzen mit den Nummern *VI* und *VII* wahrt).
Da die Polen die Verdrahtung der beiden neuen Walzen *IV* und *V* nicht kennen, können jetzt nur noch jene Schlüssel gebrochen werden, deren Walzenlage sich aus den bekannten Walzen *I, II* und *III* zusammensetzt; alle Kombinationen mit einer der neuen Walzen bleiben vorerst unzugänglich. Abgesehen davon lassen die beiden neuen Walzen den Arbeitsaufwand enorm ansteigen. Fortan sind nicht mehr nur sechs, sondern 60 verschiedene Walzenlagen zu untersuchen. Es müssen nicht mehr sechs Bombas für sechs mögliche Lagen parallel laufen, um auf Erfolge in absehbarer Zeit hoffen zu können, sondern 60 für 60 Lagen. Für Zygalskis Methode machen die beiden zusätzlichen Walzen die Herstellung von insgesamt 60 Sätzen an Lochkartons erforderlich.
Es ist eine ernste Situation, doch kommt Rejewski wieder ein gravierender Fehler auf deutscher Seite zugute. Ausgerechnet der *„Sicherheitsdienst"*, der Geheimdienst der SS, verwendet in fahrlässiger Weise die vierte und die fünfte Walze in Verbindung mit dem alten Verschlüsselungsverfahren des doppelten Spruchschlüssels auf Basis einer gemeinsamen Grundstellung. Das ermöglicht es den Polen, nach bewährter Methode die Verdrahtung der vierten und der fünften Walze zu errechnen und damit den entstandenen Rückstand ein Stück weit aufzuholen. Theoretisch.
Praktisch sind sie letztlich nicht in der Lage, die Bombas und Enigmas in adäquater Weise aufzurüsten. Es können nur einige Exemplare der neuen Walzen hergestellt werden, und es erscheint undenkbar, kurzfristig so viele Bombas zu bauen. Die Folge ist, dass die 60 Walzenlagen auf den wenigen bestehenden Maschinen nacheinander abgearbeitet werden müssen, wodurch sich der Entschlüsselungsprozess enorm verlängert. Eine rasche Entschlüsselung, die im Ernstfall unverzichtbar ist, um umgehend militärische Gegenmaßnahmen einleiten zu können, rückt in weite Ferne.
Die Situation verschärft sich weiter, als mit 1. Januar 1939 vom deutschen Chiffrierdienst die Zahl der Steckerverbindungen an der Enigma auf zehn erhöht wird. Der Verwürfelungsgrad wird dadurch so hoch, dass die Bomba-Methode so gut wie gar nicht mehr funktioniert. Bei zehn gesteckten Kabeln, also zwanzig vertauschten Buchstaben, sind im Text kaum klare Fragmente mehr zu erkennen, die es erlauben, zu beurteilen, ob man verwürfelten Klartext oder Chiffren vor sich hat. Andererseits steht die steckerunabhängige Methode von Zygalski noch nicht zur Verfügung, weil

16 *Billiarden Möglichkeiten durch das Steckerbrett*

die benötigten 60 Sätze zu je 26 Lochkartons mit ihren unzähligen Lochungen noch nicht fertiggestellt sind. Der Aufwand wird für die kleine polnische Gruppe zu hoch. Gleichzeitig wächst die Bedrohung eines deutschen Überfalls.

In der Zwischenzeit denkt der französische Geheimdienstmann Gustave Bertrand darüber nach, was angesichts des heraufziehenden Krieges zu tun das Beste wäre. Er könnte den deutschen Geheimdienst durch Zuspielung geheimen Materials wissen lassen, dass Polen und Franzosen deutschen Funkverkehr mitlesen. Dies hätte aller Wahrscheinlichkeit nach zur Folge, dass die Deutschen gravierende Änderungen in ihrem Schlüsselverfahren vollziehen würden und man mit der Entschlüsselungsarbeit wieder von vorne beginnen müsste. Doch brächte es zweifellos Sand in Hitlers anlaufende Kriegsmaschinerie und dadurch Zeitgewinn. Die Wehrmachtführung würde wohl nicht wagen, unter Verwendung eines kompromittierten Verschlüsselungsverfahrens einen Krieg zu beginnen. Sie würde sicherlich ihr System nachjustieren, dann aber deutlich gestärkt zuschlagen.

Andererseits denkt Bertrand daran, den polnischen, französischen und britischen Nachrichtendienst zusammenzuspannen und sämtliche Kenntnisse zu teilen, um gemeinsam Gegenstrategien zu entwickeln. Er entscheidet sich für diese zweite Option, die auf lange Sicht Erfolg verspricht. Die engere Zusammenarbeit soll zudem dazu führen, dass er von polnischer wie von britischer Seite, die er beide seit Jahren mit kostspieligen Enigma-Unterlagen beliefert, endlich die versprochenen konkreten Ergebnisse erhält.
Im Januar 1939 findet in Paris ein Treffen zwischen polnischen, französischen und britischen Geheimdienstleuten und Chiffrierexperten statt. Die Polen sind vertreten durch Gwido Langer, den Leiter des Biuro Szyfrów, und seinen Stellvertreter Maksymilian Ciężki, das französische Service de Renseignements durch Gustave Bertrand und den Kryptologen Henri Braquenié, der britische Secret Intelligence Service durch Alexander *„Alastair"* Denniston, den Leiter des britischen Chiffrierbüros *„Government Code and Cypher School"*, und seinen Chefkryptologen Dillwyn Knox. Bei den Besprechungen wird deutlich, dass die Briten an der Möglichkeit zweifeln, die Enigma rechnerisch rekonstruieren zu können. Langer und Ciężki halten sich bedeckt, geben die erzielten Erfolge nicht preis. Seitens ihrer Vorgesetzten wurde ihnen untersagt, das Geheimnis um ihren Einbruch in die Enigma zu lüften, sofern nicht auch die anderen Ergebnisse vorzuweisen hätten. So verständigt man sich am Ende nur unverbindlich auf gemeinsame Forschungsarbeit und auf weitere Treffen, sobald es neue Entwicklungen gäbe.
Die neuen Entwicklungen lassen nicht lange auf sich warten. Adolf Hitler lässt deutsche Truppen in den tschechischen Landesteil der Tschechoslowakei einmarschieren, den er zum *„Reichsprotektorat Böhmen und Mähren"* erklärt. Gleichzeitig reduziert er den slowakischen Landesteil zu einem Marionettenstaat unter seinem Diktat. Durch diese Entwicklung sieht sich Polen weitgehend vom Deutschen Reich umzingelt. Es wird vollends klar, wer das nächste Opfer ist, als aus Berlin territoriale Forderungen an Warschau ergehen. Ein Krieg scheint unvermeidlich.
Der polnische Generalstabschef Wacław Stachiewicz ordnet daraufhin an, den westlichen Verbündeten nun doch Einblick in das Enigma-Geheimnis zu gewähren. Man vereinbart ein weiteres Treffen, im Zuge dessen am 24. Juli 1939 eine erste Unterredung im Warschauer Hotel Bristol stattfindet. Die Franzosen sind wieder vertreten durch Bertrand und Braquenié, die Briten durch Denniston und Knox sowie einen Verantwortlichen für den Funkabhördienst der Royal Navy. Die polnische Delegation wird vertreten durch Langer vom Biuro Szyfrów, Stefan Mayer vom polnischen Geheimdienst und den Kryptologen um Rejewski.



17 *„Stukas" beim Überfall auf Polen*

Langer unterrichtet die anwesenden Gäste darüber, dass das Geheimnis der Enigma gelüftet und die Maschine rekonstruiert sei. Tags darauf werden die Gespräche in den Anlagen des Biuro Szyfrów in Pyry fortgesetzt. Die Polen präsentieren die Früchte ihrer bisherigen Arbeit; Briten und Franzosen staunen über die Methoden und die vorgeführten Enigmas und Bombas. Am Ende werden den Gästen zwei der zahlreichen nachgebauten Enigmas, über die man mittlerweile verfügt, ausgestattet mit allen fünf Walzen, sowie die Baupläne der Bomba übergeben. Die beiden Enigmas gelangen einige Wochen nach dem Treffen mit Diplomatengepäck nach Paris. Bertrand persönlich bringt das für die Briten bestimmte Exemplar nach London. Nicht zu früh.

Die deutsche Führung plant den Krieg gegen Polen ehestmöglich zu beginnen. Nach Jahren an Übungen und Manövern, den Probeläufen beim *„Anschluss"* Österreichs und der Zerschlagung der Tschechoslowakei steht die Wehrmacht vor dem ersten echten Kriegseinsatz. Im August registriert der polnische Generalstab immer mehr Grenzverletzungen durch

18 *Deutsche Panzer während des „Polenfeldzuges“*

deutsche Aufklärungsflugzeuge. Es sind die Vorzeichen des Überfalls. In den Morgenstunden des 1. September ist es soweit. Von Westen, Norden und Süden dringen deutsche Armeen über die langen und deshalb nur schwach verteidigten Grenzen in Polen ein. Die den Truppenverbänden zugeteilten Nachrichteneinheiten verlegen während des Vormarschs Kabel, um den Anschluss an das deutsche Kabelnetz und damit Kontakt zu den rückwärtigen Kommanden zu halten. Dort, wo noch keine Kabelverbindung hinreicht, halten motorisierte Funktrupps Verbindung. Die Sprüche werden von Funkern aufgenommen, entschlüsselt, in Klartext auf Formulare geschrieben und durch Melder, oft per Motorrad, zugestellt.

In Pyry wird wie schon bisher rund um die Uhr an der Entschlüsselung solcher Funksprüche gearbeitet. Der Charakter der Tätigkeit verändert sich jedoch erheblich. Nun geht es nicht mehr um die Lösung einer abstrakten mathematischen Aufgabe, sondern ums nackte Überleben. Die deutsche Wehrmacht führt einen erbarmungslosen Krieg gegen die polnische Armee wie auch gegen Zivilisten. Hitlers Ziele weisen weit über einen

militärischen Triumph hinaus, umfassen die systematische Ermordung von Angehörigen der polnischen Gebildetenschicht sowie der jüdischen Volksgruppe. Umso tragischer ist der Umstand, dass die Erfolgssträhne der Gruppe um Rejewski jetzt abreißt. Man verfügt zwar über das nötige Wissen, doch fehlen die Instrumente zur Lösung der auf fünf Walzen basierenden Enigma-Schlüssel. Ausschlaggebend für das Versagen ist aber auch, dass die Funkhorchstellen der polnischen Armee sehr schnell von deutschen Einheiten überrannt und ausgeschaltet oder zur Verlegung nach Osten gezwungen werden und somit kaum aufgefangenes Spruchmaterial vorliegt. Die Geheimwaffe versagt.

Angesichts des katastrophalen Kriegsverlaufs wird bald klar, dass die Kryptologengruppe nicht länger in Pyry belassen werden kann. Zu hoch ist das Risiko, dass das wertvolle Personal in deutsche Hände fällt. Bereits am 6. September ergeht der Befehl, Akten zu vernichten und die Evakuierung von Gerätschaften und Personal vorzubereiten. Die Bombas und die meisten der nachgebauten Enigmas werden zerstört, um Spuren zu beseitigen. Der geheime Tross des Chiffrierbüros tritt in einem Sonderzug eine tagelange, immer wieder durch Luftangriffe unterbrochene Reise ins Ungewisse an. Im Reisegepäck befinden sich neben wichtigen Unterlagen auch die letzten beiden noch existierenden Nachbau-Enigmas, gut verpackt in hölzerne Kisten.

Nach wochenlanger abenteuerlicher Flucht gelangen Marian Rejewski und seine Kollegen nach Frankreich, wo sie Ende Oktober 1939 im Château de Vignolles in Gretz-Armainvilliers in der Nähe von Paris ihre Arbeit wieder aufnehmen. Französische Geheimdienststellen sorgen für Organisation, Sicherheit und den Funkabhördienst, der über Stationen in Metz, Strasbourg und Mulhouse verfügt. Leiter der Gruppe ist Gustave Bertrand. Es sind drei Nachbau-Enigmas vor Ort – die zwei aus Polen geretteten Exemplare und jenes, das dem französischen Geheimdienst im Juli überlassen worden ist. Eines dieser drei Exemplare wird zerlegt, um Konstruktionszeichnungen anzufertigen, mit deren Hilfe weitere Repliken gebaut werden können. Ein weiteres Exemplar dient Forschungszwecken, weshalb anfangs nur ein einziges für die Entschlüsselungsarbeit zur Verfügung steht.


52
Hut 6

Station X in Bletchley Park

Auf der Grundlage der polnischen Vorarbeiten beginnen mit Ausbruch des Krieges auch die Briten Vorkehrungen für die Entschlüsselung des Enigma-Funkverkehrs zu treffen. Unter der Regie des Geheimdiensts entsteht in einem Anwesen namens Bletchley Park in der nordwestlich von London, auf halbem Weg zwischen Oxford und Cambridge gelegenen Kleinstadt Bletchley ein streng geheimes Zentrum der *„Government Code and Cipher School"*. Geleitet wird die mit dem Tarnnamen *„Station X"* bedachte Institution von dem routinierten Kryptologen Alastair Denniston, der während des Ersten Weltkrieges schon dem *„Room 40"*, einem legendären Dechiffrierzentrum der britischen Admiralität, angehört hat.
Auf dem Anwesen entstehen Baracken – *„Huts"* genannt –, in denen ausgesuchte Mitarbeiter – unter ihnen Schachmeister und Mathematiker – ihre Arbeit aufnehmen. Viele von ihnen sind jung, kommen von renommierten Universitäten und bringen neue Denkansätze mit, die im konservativen Militärapparat bisweilen noch auf Unverständnis stoßen. Wie alle Beteiligten sind sie per Eid und bei Androhung von Gefängnis zu bedingungsloser Verschwiegenheit verpflichtet. Unter keinen Umständen darf etwas von der Enigma-Entzifferung nach außen dringen, da die deutsche Seite sonst ihr System ändern oder dieses Wissen dazu nutzen könnte, die Alliierten England und Frankreich, die Deutschland nach dem Überfall auf Polen den Krieg erklärt haben, durch Desinformation gezielt zu täuschen.
An den Frontlinien in Westeuropa herrscht indes noch die sprichwörtliche Ruhe vor dem Sturm. Deutsche und französische Truppen belauern einander an der Grenze, und auch in England harrt man in diesen spannungsgeladenen Tagen der kommenden Ereignisse.
In Chatham und Chicksands befinden sich Abhörstationen, so genannte *„Y-Stations"*, in denen Bedienstete der *„War Office Y Groups"* den Funkverkehr des deutschen Heeres und der Luftwaffe überwachen. In mehrstündigen Schichten wird der Äther belauscht, um die piepsenden Morsezeichen aufzuschnappen und niederzuschreiben. So monoton diese Tätigkeit ist, so bedeutsam ist es, die Chiffren korrekt aufzunehmen, da

19 *Hut 6 in Bletchley Park*

20 *Den Äther nach Morsezeichen durchsuchen. Funkhorchstation der Royal Air Force*

jeder kleine Fehler jeglichen Entschlüsselungsversuch zunichte macht. Sind einzelne Morsezeichen nicht genau zu verstehen, muss dies angemerkt werden, fallen Zeichen gänzlich Störungen zum Opfer, ist exakt anzugeben, wie viele versäumt wurden. Gleichzeitig gilt es zu verhindern, versehentlich ein Zeichen einer Nachbarfrequenz mitzuerwischen, was natürlich auch jeglichen Entschlüsselungsversuch zum Scheitern verurteilen würde. Ein feines Gehör und höchste Konzentration sind nötig.
In den Anfängen ist es zudem noch recht schwierig, genügend brauchbares Spruchmaterial zum Schlüsselbrechen zu sammeln. Die Heeresstellen in Deutschland kommunizieren weitgehend über sichere Telegrafenleitungen, ihr Funkverkehr fällt in diesen Tagen äußerst gering aus, und wenn sie funken, wechseln sie oft Frequenzen und Rufzeichen. Die Sprüche, die aufgefangen werden können, gelangen durch Motorradboten oder über eine Fernschreibverbindung nach Bletchley Park. In Hut Six wird jeder dieser Sprüche unter Anführung der Frequenz, auf der er empfangen wurde, sowie seines Rufzeichens registriert. Dann folgt die Auswertung.
Nachdem sich die Chiffren noch nicht entziffern lassen, widmet sich der Mathematiker Gordon Welchman dem Spruchkopf, der jedem Funkspruch vorangestellt ist. Dieser enthält unter anderem die Kenngruppe, die für den Schlüsselkreis steht, dem der Funkspruch angehört. Sie wird von deutschen

Funkern mittlerweile fix als erste Gruppe vor die Chiffren des Spruchschlüssels gesetzt. Durch Sortieren der Kenngruppen des jeweiligen Tages kann Welchman alsbald mehrere Schlüsselkreise identifizieren, die er durch Unterstreichen mit unterschiedlichen Buntstiften kennzeichnet. Die Farben, die er verwendet – rot, blau, grün –, werden diesen Schlüsseln in Bletchley Park künftig ihre Namen geben: *„Red"*, *„Blue"*, *„Green"*.
Darüber hinaus bieten sich die Rufzeichen als Untersuchungsobjekte an. Jede deutsche Funkstation verfügt über ein derartiges, aus drei Buchstaben bestehendes Rufzeichen, das sie mitsendet, um sich zu identifizieren. In analoger Weise wird der Empfänger des Spruchs in Form eines Buchstabenkürzels ausgewiesen. Über diese Kürzel versuchen die britischen Spezialisten die deutschen Funkstationen zu enttarnen. Werden mehrere von ihnen als zusammengehörig erkannt, hat man es möglicherweise mit einem größeren Truppenverband zu tun, dessen aktivste Funkstation in der Regel das Hauptquartier darstellt. Ausgehend von solchen Indizien können Schlussfolgerungen gezogen werden: Ein Ansteigen des Funkverkehrs insgesamt verweist auf erhöhte Aktivität des Verbands, durch Funkpeilung lassen sich gegebenenfalls Bewegungen nachvollziehen. Erschwerend wirkt, dass auf deutscher Seite die Rufzeichen täglich gewechselt werden, doch wiederholt sich die Zuweisung der Rufzeichen regelmäßig. Nach längerer Beobachtung dieser Kennungen ist es einfach, den Wiederholungscharakter zu durchschauen. Welchman analysiert auch die Frequenzen, auf denen Sprüche aufgefangen worden sind, sowie die Zeitpunkte, zu denen dies geschehen ist. Schließlich kann ein fixer Sendezeitpunkt eine Funkstation verraten, auch wenn sie täglich ein neues Rufzeichen benutzt; ähnliche Rückschlüsse ergeben sich aus der Nutzung von bestimmten Frequenzen.
In weiterer Folge etablieren sich in Hut Six mehrere Arbeitsräume, in denen sämtliche Schritte von der Registrierung der aufgefangenen Funksprüche bis zu ihrer Entzifferung erledigt werden. Für die Entschlüsselung greift man auf die Möglichkeiten zurück, die der doppelte Spruchschlüssel bietet und derer sich schon die Polen bedient haben: Einserzyklen, bei denen die ersten und vierten Stellen des Spruchschlüssels dieselbe Chiffre aufweisen, die zweiten und fünften oder die dritten und sechsten. In Bletchley Park nennt man diese besonderen Buchstabenpaare in Anspielung auf das weibliche Chromosomenpaar XX *„Females"*.
Zunächst gilt es, genügend Funksprüche eines Tages aufzufangen, um ausreichend viele Females zu bekommen. Darüber hinaus braucht man Lochkartons, wie sie Henryk Zygalski vor nicht allzu langer Zeit in Polen entwickelt hat. Sie entstehen unter der Obhut des 23jährigen John Jeffreys und firmieren deshalb als *„Jeffreys Sheets"*. Im Dezember 1939 sind die nötigen 60 Sätze zu je 26 Bögen fertig. Sobald genügend aufgefangene

Funksprüche eines Schlüsselkreises vorliegen, werden die entsprechenden Bögen in der obligatorischen Weise übereinandergelegt. Liefern sie ein Ergebnis, wird dieses sofort im Maschinenraum an den so genannten *„Type-X"*-Schlüsselmaschinen getestet. Bei diesen Maschinen handelt es sich um große Schreibmaschinen mit eingebautem Walzenwerk, das die Enigma zu imitieren erlaubt. Die zumeist weiblichen Bediensteten, die an diesen Maschinen sitzen, wissen freilich nichts über die Bedeutung der Sprüche, die sie tippen. Eingeweiht sind lediglich die Kryptologen, denen es im Januar 1940 erstmals gelingt, einzelne deutsche Funksprüche zu entschlüsseln und zu entziffern, wenn auch keine aktuellen.
Erweist sich das ausgetestete Ergebnis als falsch, geht die Prozedur mit den Lochkartons weiter, bis ein Ergebnis den gesuchten Schlüssel offenbart. Das Entschlüsseln dauert aber noch viel zu lang, als dass die Erkenntnisse für eine unmittelbare militärische Reaktion nutzbar wären, ganz abgesehen davon, dass sich die entzifferten Nachrichten inhaltlich oft als wenig ergiebig erweisen. Ungeachtet dessen vollzieht sich dieses Ritual fortan Tag für Tag, rund um die Uhr. Wenn die deutschen Funker um Mitternacht die Schlüssel wechseln, ist Hut Six gefordert, sie aufs Neue zu brechen.

Deutsche Marinefunksprüche werden von den *„Y-Stations"* in Flowerdown und Scarborough aufgefangen und gelangen ebenfalls per Motorrad oder Fernschreiber nach Bletchley Park, und zwar in Hut Eight. Die an ihrer charakteristischen Form erkennbaren Sprüche – die Chiffren sind in Vierergruppen angeordnet – lassen sich aber noch nicht entschlüsseln. Schuld daran ist unter anderem die von der deutschen Kriegsmarine verwendete Enigma. Sie arbeitet mit acht verschiedenen Schlüsselwalzen, nachdem knapp vor Kriegsausbruch die Walze mit der Nummer *VIII* hinzugekommen ist. Damit steigt die Anzahl an möglichen Walzenlagen von 210 (bei drei aus sieben Walzen) auf 336 (bei drei aus acht). Das bedeutet einen enormen Mehraufwand für Bletchley Park, ganz abgesehen davon, dass man die Verdrahtung der Walzen *VI, VII* und *VIII* noch gar nicht kennt. Im Unterschied zu den Walzen *I* bis *V* verfügen die Walzen *VI* bis *VIII* zudem über je zwei Übertragskerben, sodass sie, in die Enigma eingesetzt, die jeweils benachbarte Walze nicht nur einmal pro Umlauf um einen Schritt mitdrehen, sondern zwei Mal.
Außerdem bedient sich die deutsche Kriegsmarine einer deutlich komplizierteren Verfahrensweise beim Verschlüsseln: Walzenlage und Ringstellungen, genannt *„innere Einstellungen"*, werden jeden zweiten Tag durch einen Offizier geändert, die *„äußeren Einstellungen"* – die Grundstellung der Walzen und die Steckerverbindungen – täglich durch den Schlüssler.

Darüber hinaus hat der Schlüssler aus einem umfangreichen *„Kenngruppenbuch"*, das tausende dreistellige Buchstabenkombinationen systematisch auflistet, zwei Kenngruppen auszuwählen. Eine *„Zuteilungsliste für Kenngruppen"* legt fest, aus welchen Spalten er auszuwählen hat. Eine der Kenngruppen bildet die *„Schlüsselkenngruppe"*, die mitgesendet wird, um den Schlüsselkreis zu indizieren, dem der Spruch angehört. Die andere dient als *„Verfahrenkenngruppe"* zur Bildung des Spruchschlüssels. Dazu wird sie in die auf den aktuellen Tagesschlüssel eingestellte Enigma getippt. Die entstehenden Chiffren bilden den Spruchschlüssel. Damit die beiden Kenngruppen nicht wiederholt gewählt werden können und um auffällige Häufungen zu vermeiden, sind sie nach ihrer Verwendung aus dem Kenngruppenbuch zu streichen.
Für die Übermittlung an den Empfänger werden die Kenngruppen auf spezielle Weise verschlüsselt. Die Schlüsselkenngruppe wird niedergeschrieben und darunter – um eine Stelle nach links versetzt – die Verfahrenkenngruppe. In die links oben und rechts unten frei bleibenden Ecken schreibt der Schlüssler beliebige Füllbuchstaben. Er erhält dadurch zwei untereinander stehende, vierstellige Chiffregruppen. Vertikal gelesen, hat er vier Buchstabenpaare vor sich, die er durch Tauschpaare ersetzt. Jene entnimmt er einer von zehn vorgedruckten *„Doppelbuchstabentauschtafeln"*, in denen alle möglichen Varianten an Buchstabenpaaren systematisch aufgelistet sind. Aus welcher Tafel er diese zu nehmen hat, geht aus einem *„Tauschtafelplan"* hervor, der dies für jeden Tag eines Monats festlegt. Der Funker hat die neuen vier Paare hintereinander zu funken – und zwar einmal am Anfang des Funkspruchs und zur Sicherheit hinsichtlich allfälliger Übermittlungsaussetzer ein weiteres Mal am Ende.
Aus Sicherheitsgründen soll ein Funkspruch möglichst kurz sein, nicht mehr als 80 Gruppen zu je vier Chiffren umfassen. Dem gegnerischen Abhördienst soll möglichst wenig Material zuteil werden, das auf den gleichen Schlüssel zurückgeht. Die Nachricht soll überdies im Telegrammstil verfasst und die Schreibweise variiert werden. Für häufig verwendete Worte und Routinebegriffe – etwa Bezeichnungen von Dienststellen wie *„Befehlshaber der U-Boote"* – sind wechselnde Kürzel wie *„Bef. Unterseeboote"*, *„Befhbr. uuubte"* oder schlicht *„bduuu"* zu verwenden, um dem Gegner das Einbrechen zu erschweren. Längere Sprüche sind zu unterteilen. Für jeden Funkspruch wie auch für jeden Teil eines Funkspruchs ist die Kenngruppe zu ändern. Außerdem muss im hinteren Drittel eines jeden Spruchteils – mit Ausnahme des letzten – die Silbe FORT – für *„Fortsetzung"* – eingesetzt werden; im ersten Drittel aller Folgeteile ist FORT samt der Uhrzeit des ersten Teils einzusetzen, damit der Empfänger die Teile als zusammengehörig erkennt.

21 *Der Schlüssel M, das Schlüsselverfahren der Kriegsmarine*

Neben dem Marineschlüssel *„M Allgemein"* existiert für Inhalte besonderer Geheimhaltungsstufe die höherwertige Variante *„M Offizier"*. Dabei handelt es sich um eine doppelte Verschlüsselung, deren erster Teil durch einen Offizier erfolgt. Dieser benutzt zur Verschlüsselung eines Funkspruchs die Walzenlage und die Ringstellungen des aktuellen Tagesschlüssels, jedoch besondere Steckerverbindungen, die nur ihm zugänglich sind. Den Spruchschlüssel wählt er aus einer vorgedruckten Liste mit 26 Schlüsseln aus, über die nur er verfügt. Der Spruchschlüssel wird nicht mitgeschickt, sondern lediglich durch einen Namen, der für einen Buchstaben des Alphabets steht, indiziert. Jeder der 26 Spruchschlüssel auf der Liste ist einem solchen Buchstaben zugeordnet. Infolgedessen wird vor die Chiffren das Wort *„Offizier"* samt dem betreffenden Namen – etwa *„Offizier Paula"*, wenn es sich um den Buchstaben *P* handelt – unverschlüsselt geschrieben. Danach wird der gesamte Funkspruch durch den regulären Schlüssler mit dem aktuellen Tagesschlüssel ein weiteres Mal verschlüsselt. Erst dann wird er abgesetzt.

Auf der Empfängerseite erhält der Schlüssler nach dem ersten Entschlüsselungsdurchgang eine Reihe unleserlicher Chiffren, denen *„Offizier Paula"* voransteht. Diese Phrase sagt ihm, dass er die Chiffren durch einen Offizier weiter entschlüsseln lassen muss. Jener findet in seiner Liste unter *P* den verwendeten Spruchschlüssel und gelangt mit dieser Einstellung zu Klartext. Über die Variante *„M-Offizier"* hinaus verfügt der Marineschlüssel über eine noch höhere Geheimhaltungsstufe, genannt *„M-Stab"*. Und für den Fall, dass der Maschinenschlüssel ausfällt, existiert mit dem so genannten *„Reservehandverfahren"* ein rein handschriftliches Schlüsselverfahren.
Der Schlüssel *M* lässt den Schlüsslern wenig freie Wahl, gibt zahlreiche Listen vor, aus denen sie auf streng geregelte Weise auszuwählen haben. Dies ermöglicht ein hochwertiges Verschlüsselungsverfahren, minimiert den menschlichen Unsicherheitsfaktor und reduziert dadurch das Risiko verräterischer Häufungen. Allerdings erfordert diese Vorgangsweise das Mitführen einer Vielzahl an geheimen Schlüsselunterlagen auf See, was das Risiko mit sich bringt, dass diese erbeutet werden. Aus diesem Grund werden solche Unterlagen alsbald mit wasserlöslicher roter Tinte gedruckt, damit ihr brisanter Inhalt umgehend verschwindet, wenn sie bei feindlicher Bedrohung ins Meer geworfen werden.

In dieser prekären Situation haben die Briten unerwartetes Kriegsglück. In einer Februarnacht des Jahres 1940 ist ein deutsches U-Boot damit beschäftigt an der Westküste Schottlands Minen zu legen, um den Seeweg für Schiffe der Alliierten zu blockieren. Es ist ein gefährliches Unterfangen, da das seichte Gewässer im Notfall kein ausreichend tiefes Abtauchen erlaubt. Es tritt ein, was zu befürchten war. Das Boot wird vom Sonar eines britischen Minensuchschiffs erfasst und durch Wasserbomben zum Auftauchen gezwungen. Der U-Boot-Kapitän gibt der Besatzung den Befehl, das Boot zu versenken und über Bord zu gehen. Einige Besatzungsmitglieder tragen die Schlüsselwalzen der Enigma mit sich. Sie sollen sie ins Meer werfen, sobald sie draußen sind. Aber einer von ihnen vergisst bei seinem Überlebenskampf im eiskalten Wasser, dies zu tun. Als er geborgen wird, fallen den Briten drei Walzen in die Hände, darunter die unbekannten *VI* und *VII*.
Angesichts dieser Beutestücke rückt das Ziel, den Schlüssel M zu knacken, ein bedeutendes Stück näher. Mit dieser Aufgabe betraut ist der 27jährige britische Mathematiker Alan Turing, der als einer von wenigen daran glaubt, dass der deutsche Marineschlüssel brechbar ist und darin geradezu eine persönliche Herausforderung erblickt. Doch bis zum Durchbruch wird noch einige Zeit vergehen.

22 *Wasserlösliche Tinte für rasche Selbstzerstörung*

In der Zwischenzeit beschäftigt sich in Hut Four in Bletchley Park ein 20jähriger Student namens Harry Hinsley intensiv mit maritimer Funkverkehrsanalyse. Da man die Funksprüche noch nicht mitlesen kann, konzentriert er sich auf die verwendeten Frequenzen und Rufzeichen deutscher Schiffe und Boote und versucht daraus soviel Information wie möglich zu gewinnen. Anfang April 1940 erkennt er eine Versammlung von deutschen Kriegsschiffen in der Ostsee und prophezeit bevorstehende Aktionen, die er aus dem starken Anschwellen des Funkverkehrs schließt. Tage später werden die umfangreichen Militäroperationen für alle Welt erkennbar, im Zuge derer deutsche Truppen Dänemark und Norwegen besetzen.
Während der deutsche Marineschlüssel unzugänglich bleibt, gelingt Hut Six ein Einbruch in einen neuen Schlüsselkreis, der *„Yellow"* genannt wird. Yellow umfasst den Funkverkehr deutscher Verbindungsoffiziere, die die an den Kämpfen in Norwegen beteiligten Heeres- und Luftwaffen-Einheiten koordinieren. Dabei fällt für die britischen Kryptologen viel Abhörmaterial an, Mitte April gelingt ihnen schließlich der erhoffte Einbruch. Es ist das erste Mal, dass sie in der Lage sind, den Funkverkehr eines deutschen Schlüsselkreises sofort und kontinuierlich mitzulesen, doch können sie diesen Vorteil nicht nutzen. Es fehlt noch an organisatorischen Voraussetzungen für eine rasche und effiziente Verteilung der Information an die militärischen Einheiten vor Ort.

Aufgenommen von französischen Horchstationen, werden die deutschen Funksprüche aus Norwegen zur gleichen Zeit auch von Rejewski und seinen Kollegen in Frankreich untersucht. Sie haben dafür aus Bletchley Park einen Satz der neuen Lochkartons erhalten, was eine bescheidene Zusammenarbeit über den Ärmelkanal hinweg nach sich zieht. Erzielte Ergebnisse werden über eine Fernschreibverbindung ausgetauscht. Um unerwünschtem Mitlesen durch deutsche Agenten vorzubeugen – etwa durch Anzapfen der mehr als 600 Kilometer langen Leitung – verschlüsselt man die Nachrichten sinnigerweise mit einer der nachgebauten Enigmas.
Ab Mitte April registriert die polnisch-französische Gruppe Funksprüche, die von einer immer bedrohlicher werdenden Konzentration deutscher Truppen nahe der holländischen, belgischen, luxemburgischen und französischen Grenzen künden. Der erwartete Angriff in Westeuropa zeichnet sich ab, doch der französische Generalstab, der auf die Unüberwindbarkeit seiner Grenzbefestigungen vertraut, reagiert auf die Warnungen nicht.
Am 10. Mai 1940 beginnt die deutsche Wehrmacht einen Überraschungsangriff auf Belgien, Holland und Frankreich. Ihre motorisierten Truppen umgehen die Verteidigungswerke der *„Maginot-Linie"* und dringen tief ins französische Landesinnere vor. Binnen kurzer Zeit zeichnet sich für die Alliierten eine militärische Katastrophe ab. Gleichzeitig verlieren sie den Zugang zum Funkverkehr der deutschen Armeen.
Grund ist eine neue Schlüsselanleitung der Chiffrierstelle in Berlin, die eine gravierende Änderung beinhaltet. Die Spruchschlüssel werden nur noch einmal in die Enigma getippt und chiffriert und somit auch nur noch einfach gefunkt (was übrigens auch für die Grundstellung gilt). Damit wird die Schwachstelle des doppelten Spruchschlüssels eliminiert, was britische wie polnische Kryptologen, die ihre Arbeit weitgehend auf dieser Schwachstelle aufgebaut haben, hart trifft. Die bisherigen Entschlüsselungsmethoden sind nun hinfällig, auch die Lochkartons haben ausgedient, nachdem jetzt keine Females mehr auftreten. Ausgenommen den deutschen Funkverkehr in Norwegen, wo noch für kurze Zeit das alte Verfahren beibehalten wird, findet man sich weitgehend ausgesperrt wieder.
Der schwere Rückschlag kommt nicht ganz unerwartet. Seit Langem ist klar, dass die Entschlüsselung mittels Lochkartons nur so lange funktioniert, wie die deutsche Seite an der leichtsinnigen Praxis festhält, die Spruchschlüssel doppelt zu senden. Deshalb haben die Verantwortlichen in Bletchley Park für den Fall, dass dies irgendwann nicht mehr geschehen würde, Alan Turing beauftragt, gänzlich neue Strategien zu entwickeln. Turing wendet sich von den Spruchschlüsseln ab und konzentriert sich auf die chiffrierten Nachrichten selbst. Durch das Studium entzifferter deutscher Funksprüche erkennt er, dass sie nach einer strengen Ord-

nung aufgebaut sind. Die Nachrichten enthalten im Allgemeinen formal korrekte Angaben über Sender und Empfänger samt Titeln und Grußfloskeln. Dank dieser strengen Ordnung kann Turing auch bei aktuellen Funksprüchen das Vorkommen bestimmter Klartextworte mit einer gewissen Wahrscheinlichkeit vermuten. Nachdem zahlreiche Stationen in der Regel kurz nach sechs Uhr morgens routinemäßig Wetterberichte senden, kann Turing etwa davon ausgehen, dass das deutsche Wort *„Wetter"* in so manchem Spruch, der zu dieser Zeit aufgefangen wird, vorkommt. Hat er einen solchen Spruch in Händen, versucht er herauszufinden, hinter welchen Chiffren sich das vermutete Wort verbirgt. Dazu lässt sich der Umstand nutzen, dass die Enigma keinen Buchstaben in sich selbst chiffriert. Er kann also versuchen, die Position des Wortes *„Wetter"* dadurch zu finden, dass er es entlang der Chiffren verschiebt, bis kein Buchstabe auf seinesgleichen zu liegen kommt. Lässt sich auf diese Weise ein Abschnitt exakt lokalisieren, kennt er die Chiffren, die den Klarbuchstaben zugewiesen werden. Theoretisch muss er jetzt nur noch an jeder einzelnen der Maschinenstellungen der Enigma das Wort *„Wetter"* eintippen, bis diese Chiffren erscheinen. Die Stelle, an der das geschieht, ist die gesuchte Schlüsselstellung.
Es ist, wie gesagt, eine bloß theoretische Option, denn händisch ist sie wegen der vielen Maschinenstellungen in der kurzen zur Verfügung stehenden Zeit kaum durchführbar; ganz zu schweigen davon, dass sich das Vorhandensein des Wortes *„Wetter"* nur vermuten lässt, was sich am Ende auch als falsch erweisen kann. In diesem Fall beginnt alles von vorn. Seit Anfang 1940 plant Turing jedoch eine *„Bombe"*, die viel leistungsfähiger als ihr polnisches Vorgängermodell sein und die zahlreichen Möglichkeiten mit hoher Geschwindigkeit abarbeiten können soll. Anders als die polnische Bomba, die hauptsächlich nach Beziehungsmustern gesucht hat, welche dem doppelten Spruchschlüssel entspringen, soll Turings Bombe in den Chiffren nach so genannten *„Cribs"* suchen, also nach Worten wie eben *„Wetter"*, von denen man aus guten Gründen annehmen kann, dass sie in den Chiffren vorkommen.
Die Herstellung einer komplexen Maschine wie der Bombe ist aber sehr kostspielig und schwer durchzusetzen, zumal es anfangs alles andere als sicher ist, dass sie die Enigma-Schlüssel irgendwann tatsächlich wird brechen können. Trotzdem nimmt Turings Vision im Frühjahr 1940 Gestalt an. Eine erste Bombe, bestehend aus drei Dutzend miteinander verschalteten Enigma-Walzensätzen, geht in Betrieb. Sie wird optimistisch *„Victory"* genannt.

Indessen nehmen die Ereignisse auf dem Schlachtfeld einen dramatischen Verlauf. Rasch vormarschierende deutsche Panzerverbände kesseln bei

Dünkirchen an der Kanalküste einen großen Teil der Truppen der Alliierten ein, darunter belgische Einheiten, drei französische Armeen und das ganze britische Expeditionskorps. Es droht eine vernichtende Niederlage.
Hinter den militärischen Erfolgen der Deutschen stehen kryptografische. Die Chiffrierstelle in Berlin liest französische Funkchiffren mit, wodurch die deutsche Führung über alle maßgeblichen Vorgänge und Zustände in der französischen Armee im Bilde ist, über Gliederung und Bewaffnung, über Schwachstellen der Maginotlinie, über die Stimmung unter den Soldaten und in der Bevölkerung, aber auch über Bewegungen der britischen Truppen am Kontinent.
Im Gegensatz zu den deutschen Kryptologen, die wertvolle Information über den Gegner liefern, verfügt Bletchley Park in diesen Tagen über keine Möglichkeit deutsche Funksprüche zu entschlüsseln. Die Bombe arbeitet nicht schnell genug und es fehlt zumeist an brauchbaren Cribs, weshalb fieberhaft nach anderen Methoden gesucht wird. Immerhin kann man sich eine altbekannte Nachlässigkeit deutscher Funker zunutze machen. Obwohl es ihnen ausdrücklich untersagt ist, verwenden manche von ihnen gelegentlich noch immer gleiche Schlüsseleinstellungen für mehrere Funksprüche, oder aber wählen der Einfachheit halber Kurzworte als Spruchschlüssel oder drei auf der Tastatur nebeneinander oder untereinander liegende Buchstaben. Solche simplen Kombinationen, die sich mit etwas Glück – bzw. durch systematisches Durchprobieren – erraten lassen, werden in Bletchley Park *„Cillis"* genannt. Sie treten umso häufiger auf, je größer das deutsche Funkverkehrsaufkommen insgesamt wird.
Einem genialen Einfall des 21jährigen Studenten John Herivel ist der neuerliche Einbruch in die Enigma zu verdanken. Herivel denkt schon seit geraumer Zeit darüber nach, wie deutsche Funker ihre Maschinen wohl in Betrieb nähmen. Stellen sie zuerst die Ringe an den Walzen ein, um die Walzen danach in die Maschine einzusetzen? Oder justieren sie die Ringe erst auf den bereits eingesetzten Walzen? In letzterem Fall bestünde eine gewisse Wahrscheinlichkeit, dass Schlüssler nach dem Einstellen der Ringe durch nur geringfügiges Verdrehen der Walzen zur ersten Grundstellung des betreffenden Tages gelangen würden. Dies würde bedeuten, dass bei frühen, kurz nach dem mitternächtlichen Schlüsselwechsel aufgefangenen Funksprüchen die Ringstellungen in der Nähe der Grundstellungen liegen müssten, und da die Grundstellungen bei jedem Funkspruch in Klarbuchstaben aufscheinen, ließe sich dieser Bereich verorten.
Herivels Theorie stößt bei den Verantwortlichen auf Zustimmung. Die Funkhorcher in den Horchstationen werden angewiesen, sich besonders der ersten Funksprüche nach Mitternacht anzunehmen. Und tatsächlich

23 *Enigma-Nachrichten für den deutschen Panzergeneral Guderian*

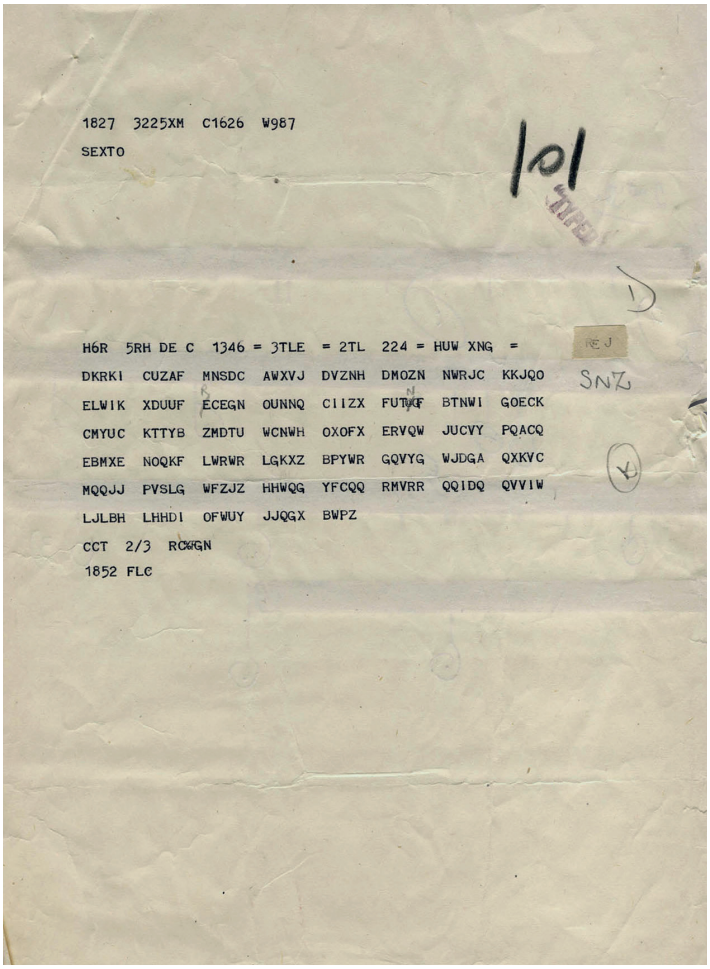
lassen aufgefangene Sprüche Häufungen dahingehend erkennen, dass die jeweils ersten, zweiten und dritten Buchstaben ihrer Grundstellungen im Alphabet relativ nahe beieinander liegen. Die Grundstellungen *S-W-E, T-V-G, S-X-F* und *R-X-G* mögen dies verdeutlichen. Die linke Walze steht immer im Bereich *R, S, T*, die mittlere bei *V, W, X* und die rechte bei *E, F, G*, was ein Anzeichen dafür ist, dass die Ringstellungen der drei Walzen in der Nähe liegen. Die Kryptologen in Bletchley Park können sich in einem derartigen Fall auf die Untersuchung der Maschinenstellungen in diesem Walzensektor konzentrieren. Der Arbeitsaufwand reduziert sich dadurch enorm, ist aber natürlich immer noch hoch. So muss Stellung für Stellung dieses fortan *„Herivel-Quarter"* genannten Sektors daraufhin getestet werden, ob sie die Schlüsselstellung darstellt – und dies selbstverständlich bei allen möglichen Walzenlagen.

Das Einstellen der Ringe auf den bereits eingesetzten Walzen, wie es Herivels Hypothese zugrunde liegt, wird übrigens von der deutschen Dienstvorschrift ausdrücklich verlangt. Damit hat sie einen nicht unerheblichen Anteil daran, dass die Briten diese recht verlässliche Entschlüsselungsmethode entwickeln können.

Ab dem 20. Mai 1940 ist man in Hut Six wieder in der Lage, den Luftwaffenschlüssel Red zu entziffern, zumeist sogar täglich. Das hat auch damit zu tun, dass die Einheiten der deutschen Luftwaffe, die während der militärischen Operationen in Frankreich laufend zur Unterstützung von Panzereinheiten gerufen werden, einen umfangreichen Funkverkehr verursachen und viel Material zur Analyse produzieren.

Gelingt es, Schlüssel zu brechen, werden die Sprüche entziffert und in Hut Three übersetzt und ausgewertet. Hut Three wird von Frederick Winterbotham geleitet, einem Angehörigen des Militärgeheimdienstes MI6. Auf seine Initiative hin werden die Sprüche von Offizieren der einzelnen Truppengattungen in militärisch korrekter Weise interpretiert. Dies scheint geboten, da es manchmal neben der Übersetzung auch der Rekonstruktion lückenhafter Passagen bedarf, was neben der Kenntnis der deutschen Sprache auch spezielles Wissen über die deutsche Armee, über Strategie, militärische Begrifflichkeiten und Verfahrensweisen voraussetzt. Darüber hinaus müssen sie natürlich über den Inhalt aller bislang entzifferten Sprüche Bescheid wissen, um neue Erkenntnisse in einen Gesamtkontext einbetten zu können.

Zu Winterbothams Aufgaben gehört auch, dafür zu sorgen, dass das Informationsmaterial, das aus der Enigma-Entzifferung gewonnen wird, möglichst rasch und unter Wahrung strengster Geheimhaltung zu den britischen Befehlshabern an die Kriegsschauplätze gelangt.


1827 3225XM C1626 W987
SEXTO

H6R 5RH DE C 1346 = 3TLE = 2TL 224 = HUW XNG =
DKRKI CUZAF MNSDC AWXVJ DVZNH DMOZN NWRJC KKJQO
ELWIK XDUUF ECEGN OUNNQ CIIZX FUTWF BTNWI GOECK
CMYUC KTTYB ZMDTU WCNWH OXOFX ERVQW JUCVY PQACQ
EBMXE NOQKF LWRWR LQKXZ BPYWR GQVYG WJDGA QXKVC
MQQJJ PVSLG WFZJZ HHWQG YFCQQ RMVRR QQIDQ QVVIW
LJLBH LHHDI OFWUY JJQGX BWPZ
CCT 2/3 RCHGN
1852 FLC

24 *Aufgefangene deutsche Chiffren*

In Frankreich werden infolge der dramatischen Ereignisse die polnischen Kryptologen von Vignolles nach Paris evakuiert, wo ihre Arbeit im Hauptquartier des französischen Geheimdienstes eine Fortsetzung findet. Tag und Nacht wird gearbeitet, und nachdem das geänderte deutsche Verschlüsselungsverfahren während der ersten zehn Tage der Kampfhandlungen jegliches Eindringen in deutsche Funksprüche verhindert hat, stellen sich jetzt allmählich wieder Erfolge ein. Mithilfe methodischer Ansätze aus Bletchley Park wie Cillis und Herivel Tip können zahlreiche Funksprüche der deutschen Luftwaffe entziffert und Erkenntnisse aus mehrmals täglich übermittelten Lagemeldungen, aus Einsatzbefehlen, Sonderaufträgen für

Bombardierungen, Einsatzberichten oder Wettermeldungen gezogen werden. Andere Funksprüche berichten von Kraftstoffbedarf oder liefern Versorgungs- und Verlustmeldungen. Es gilt, aus solchen Informationssplittern ein möglichst umfassendes Gesamtbild zusammenzufügen.
Der unglückliche Kriegsverlauf lässt sich aber nicht mehr wenden. Im Gegenteil, ein entzifferter Funkspruch, in dem ein deutscher General ankündigt, die britischen Truppen von den französischen abschneiden zu wollen, führt zu einer groß angelegten Rückzugsaktion der Briten.
Im Zuge derer gelingt es, hunderttausende Soldaten des bedrängten Expeditionsheeres auf die Britischen Inseln in Sicherheit zu bringen und vor der Gefangenschaft zu bewahren. Das rettet wichtige Reserven zur Verteidigung Großbritanniens, auch wenn fast die gesamte Ausrüstung am französischen Strand zurückbleibt und viele der eingesetzten Schiffe im Ärmelkanal versinken, was tausenden Soldaten das Leben kostet.
Nebel hält jedoch unzählige Bomber am Boden und verhindert ein weitaus größeres Massaker.
Danach nehmen die Dinge ihren Lauf. Für die polnische Gruppe in Paris muss es besonders zermürbend sein, Triumphmeldungen der heranrückenden deutschen Armeen zu entziffern. Wie schon in Polen scheint letztlich aller Aufwand vergebens, erweist sich die aggressive Blitzkriegsstrategie der deutschen Wehrmacht als überlegen. Die französische Führung kapituliert. Als am 14. Juni deutsche Soldaten in der Metropole Paris einmarschieren, werden die polnischen Kryptologen samt ihrem Gerät in den unbesetzten Teil Frankreichs in Sicherheit gebracht. Kurz danach bringt man sie nach Algier, von wo sie nach einigen Wochen nach Uzés in Südfrankreich zurückkehren, um im Chateau des Fouzes ihre Arbeit wieder aufzunehmen.

Nach der Niederlage Frankreichs droht der deutsche Angriff auf Großbritannien – vor allem aus der Luft. Im Hauptquartier des *„Fighter Command Centre“* in Bentley Priory in Stanmore bereitet man sich auf die deutschen Bomberflotten vor. Auf einer großen Lagekarte werden alle verfügbaren Informationen zusammengeführt. Frauen in Uniform verschieben färbige Holzmarken mit Höhen- und Richtungsangaben, die die gemeldeten feindlichen Flugzeuge darstellen. Dadurch können angeflogene Ziele frühzeitig erkannt, gewarnt und verteidigt werden. Von einer erhöhten Galerie aus überblickt der Kommandant Hugh Dowding das gesamte Lagebild. Von hier aus gibt er seine Befehle an die regionalen Jagdflieger-Gruppen, die auf Flugplätzen im ganzen Land stationiert sind.
Dank einer sicheren Fernschreibleitung mit Hut Three kann sich Dowding auch auf Erkenntnisse aus Bletchley Park stützen, die auf entschlüsselte

25 *Ein Lagezentrum des Fighter Command der Royal Air Force*

deutsche Funksprüche zurückgehen. Ein solcher Entzifferungserfolg betrifft einen Befehl Hitlers an die Oberbefehlshaber von Heer, Luftwaffe und Kriegsmarine, eine Landung deutscher Truppen auf den Britischen Inseln vorzubereiten. Die Briten haben zwar nicht das Originalfernschreiben aus dem Führerhauptquartier abgefangen, jedoch einen Funkspruch, mit dem der Oberbefehlshaber der Luftwaffe, Hermann Göring, die Kommandanten seiner Luftflotten über diesen Befehl Hitlers instruiert.

Anfang August 1940 ist ein Anschwellen des deutschen Funkverkehrs auf einige hundert Sprüche täglich zu bemerken. Es ist ein untrügliches Zeichen dafür, dass Vorbereitungen auf größere Operationen in Gang sind. Der umfangreiche Funkverkehr erleichtert den britischen Kryptologen die Arbeit. Aus entzifferten Funkspüchen kennen sie bald die Aufstellung von Görings Luftflotten, die Einsatzbereitschaft ihrer Flugzeuge und anstehende Pläne. Am 8. August wird der Tagesbefehl Görings entziffert, der die so genannte *„Operation Adlertag"* ankündigt, eine große Luftoffensive gegen die Britischen Inseln zur Vorbereitung einer Landung. Großspurig prophezeit Göring darin, die feindlichen Flugzeuge innerhalb kürzester Zeit vom Himmel zu fegen. Der Klartext des Funkspruchs, der sich an die Befehlshaber der drei deutschen Luftflotten in Norwegen, Belgien und Frankreich richtet, liegt kurze Zeit später allerdings auch Hugh Dowding und Premierminister Winston Churchill in London vor.
Nach einer Verschiebung wegen Schlechtwetters wird der Adlertag seitens der deutschen Führung für den 15. August neuerlich angesetzt. Bomberflugzeuge sollen in mehreren Angriffswellen neben britischen Flughäfen und Radarstationen so viele Jagdflugzeuge wie möglich zerstören und die Royal Air Force dermaßen schwächen, dass sie späteren deutschen Angriffen nichts mehr entgegenzusetzen hätte. Doch ist den Briten aus entzifferten deutschen Funksprüchen Görings Absicht bekannt, ihre Jagdflugzeuge in aufreibende Kämpfe zu verwickeln, deren Verluste sich die hochgerüstete Luftwaffe eher leisten könne als die Air Force. Dowding unterläuft wohlweislich diese Strategie, hält seine Flugzeuge zurück, setzt sie ganz gezielt ein. Bletchley Park liefert ihm dafür mögliche Angriffstermine, Ziele, mitunter auch Angaben zur Zahl der vorgesehenen Angreifer. Durch den entstehenden Wissensvorsprung können sich die Verteidiger vorbereiten. Den Deutschen hingegen erwächst Bletchley Park zu einem unsichtbaren Gegner; ein Gegner, der zudem erst am Beginn seiner Entwicklung steht. Bezeichnend dafür ist eine neue Bombe – genannt *„Agnes"* –, die Mitte August in Betrieb genommen wird. Sie verfügt über einige technische Verbesserungen, vor

26 *Luftschlacht über England*

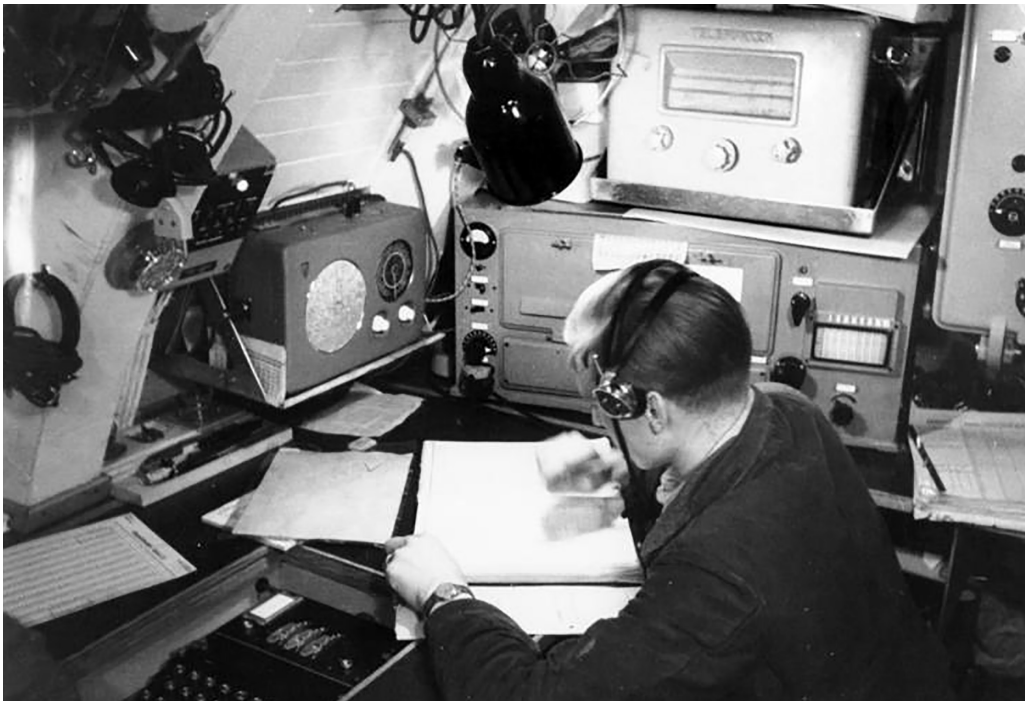
allem über ein von Gordon Welchman entwickeltes, schachbrettartiges *„Diagonal Board"*, das die Dauer der Suchläufe deutlich verkürzt. Trotz der zahlenmäßigen Überlegenheit der Luftwaffe bleibt die von Göring erhoffte Wirkung aus, die britische Verteidigung bricht nicht zusammen. Am 15. September kommt es zu einer entscheidenden Luftschlacht. In zwei großen Angriffswellen nehmen mehr als 1.000 deutsche Bomber und Jagdflugzeuge Kurs auf die Britischen Inseln. Vorgewarnt durch Bletchley Park, formiert Dowding eine Armada aus 300 Jagdflugzeugen, die sich den Angreifern der ersten Welle entgegenstellen. Überrascht von der massiven Gegenwehr, laden manche Bomber ihre tödliche Fracht überhastet ab und kehren um. Die britischen Jagdflugzeuge drehen ab, fassen auf ihren Flugplätzen Treibstoff und Munition und fliegen der nächsten Welle entgegen. Alleine an diesem Sonntag verliert die deutsche Luftwaffe rund 100 Flugzeuge und am Ende des Tages erweist sich ihre Angriffsstrategie als gescheitert. Zwei Tage danach entschlüsselt

Bletchley Park Hitlers Befehl, angesichts der verlustreichen Luftschlacht über England die Vorbereitungen auf eine Landung einzustellen. Es ist ein vorentscheidender Sieg der Briten. Da der Einbruch in die Enigma nach wie vor streng geheim ist, weiß aber kaum jemand, dass der Erfolg nicht zuletzt auf entzifferten Funksprüchen beruht.

Top Secret Ultra – der streng geheime Gegner

Neben den Angriffen aus der Luft entfaltet Deutschland einen *„uneingeschränkten U-Boot-Krieg"*. Karl Dönitz, Oberbefehlshaber der deutschen U-Boot-Flotte, will Großbritannien, das zu seiner Versorgung in hohem Maße von Importen abhängig ist, durch Versenkung seiner Frachtschiffe von überseeischen Handelsstützpunkten abschneiden und buchstäblich aushungern. In der ersten Phase des Krieges ist die deutsche U-Boot-Waffe aber noch vergleichsweise schwach. Dönitz ist weit davon entfernt, die Zahl an Booten zu haben, die er glaubt haben zu müssen, um Großbritannien in die Knie zu zwingen. Die im Einsatz befindlichen Boote verfügen zudem noch über keine allzu große Reichweite. Allerdings kann er sich bei seinen Angriffsplanungen auf die Entschlüsselungen seines Funkhorchdienstes, des so genannten *„Beobachtungsdienstes"*, stützen. Dem gelingt es, in Funkschlüssel der britischen Marine einzubrechen und den Funkverkehr von Schiffen, die Nachschub aus Nordamerika, Australien, Afrika sowie dem Mittleren und Nahen Osten auf die Britischen Inseln transportieren, zu lesen.
Geführt wird der Krieg der U-Boote von Dönitz aus großer Entfernung, von Land aus, zunächst aus Wilhelmshaven, dann, nach der Besetzung Frankreichs, von Paris, später vom Atlantikhafen Lorient aus. Dazu versammelt er seinen Mitarbeiterstab vor großen, in Planquadrate unterteilten Karten. Darauf zeigen Markierungen die Standorte von deutschen U-Booten und Schiffen der Alliierten an, deren Position durch entschlüsselten Funkverkehr in Erfahrung gebracht werden konnte. Man berät anhand der Gesamtlage die Angriffsoperationen für die nächste Zeit und funkt die entsprechenden Befehle an die auf See befindlichen U-Boote. Dass kein Spruch verloren geht, dafür sorgen Frequenzpläne, die festlegen, zu welchen Tageszeiten welche Frequenzen benutzt werden, fixe Programmzeiten sowie eine Nummerierung, um kontrollieren zu können, ob jedes Boot alle Funksprüche auch aufgenommen hat bzw. wann ein versäumter Spruch von der Leitstelle wiederholt wird, damit er noch aufgenommen werden kann.

27 *Alan Mathison Turing, Jg. 1912*



28 *Funker in einem deutschen U-Boot*

Funken ist jedoch nicht ungefährlich. U-Boote müssen zum Funken auftauchen. Tun sie dies, geraten sie in Gefahr, entdeckt zu werden. Möglichst rascher Funkverkehr ist geboten, um diese Gefahr klein zu halten, vor allem dann, wenn sie unmittelbar in militärische Aktionen involviert sind. Mit dem *„Funksignaldienst"* existiert ein Verfahren zur Übermittlung von Standardphrasen aus einem *„Signalbuch"*. Der Kürze wegen werden nicht die Phrasen selbst, sondern ihnen zugeordnete vierstellige Buchstabengruppen gefunkt. In der Regel bestehen derartige Sprüche aus 5 bis 30 solcher Gruppen. Vor dem Funken werden sie mit einer Enigma mit den aktuellen Einstellungen des Tagesschlüssels – Walzenlage, Ringstellungen und Steckerverbindungen – sowie unter Verwendung eines gewählten Spruchschlüssels chiffriert. Letzteren wählt der Schlüssler aus einer von 15 Tafeln aus, deren jede 999 verschiedene Dreierbuchstabenkombinationen verzeichnet. Aus welcher der Tafeln er ihn auszuwählen hat, geht aus einem zu den Schlüsselunterlagen gehörenden *„Verteilungsplan"* hervor, der jedem Kalendertag eine der Tafeln zuweist. Übermittelt wird der Spruchschlüssel in Form einer dreistelligen Kennzahl, die ihm auf der Tafel zugeordnet ist. Der letzten Endes vom Funker abgesetzte Funkspruch ent-

hält vorneweg diese dreistellige Kennzahl, die unverschlüsselt gesendet wird, damit der Empfänger mit ihrer Hilfe auf der entsprechenden Tafel den Spruchschlüssel identifizieren, die Chiffren der Buchstabengruppen entziffern und mit diesen im Signalbuch die eigentliche Nachricht rekonstruieren kann.

Funk ist zentraler Bestandteil des U-Boot-Krieges. Er erlaubt es, Verbindung zu den Booten auf See zu halten, um sie im Rahmen der so genannten *„Rudeltaktik"* für den Angriff auf ganze Schiffskonvois zu koordinieren. Das U-Boot, das zuerst auf einen Konvoi trifft, soll ihn zunächst unbemerkt verfolgen. Der Kommandant meldet die Sichtung an die U-Bootführung an Land, etwa mittels der Phrase *„Gustav Gelb"*, die für *„Feindlichen Konvoi gesichtet"* steht. Aufgrund der gemeldeten Position erfolgt seitens der U-Bootführung die Entscheidung, welche der in der Nähe befindlichen Boote für den Angriff abkommandiert werden. Erst wenn sich vor Ort eine größere Gruppe versammelt hat, wird der Konvoi angegriffen – gemeinsam, um so viele Frachtschiffe wie möglich zu versenken.
Aufgrund dieser zentralen Rolle des Funks besteht allerdings immer auch die Gefahr, dass es dem Gegner gelingt, den Funkverkehr der U-Boote abzuhören, zu entziffern und deren Position in Erfahrung zu bringen. Diese Gefahr ist allgegenwärtig, auch weil dem Gegner im Zuge der Aufbringung eines Boots jederzeit geheime Schlüsselunterlagen in die Hände fallen können. Der Funk bildet insofern nicht nur das Nervensystem der U-Boot-Flotte, sondern auch ihre Achillesferse.
Die Gegenspieler sitzen in London im *„Operational Intelligence Centre"* der Royal Navy. Eine seiner Sektionen ist der von dem Zivilisten Rodger Winn geleitete *„Submarine Tracking Room"*. Hier werden ebenfalls emsig Informationen gesammelt, um auf ähnlichen Karten wie jenen der Deutschen die Bewegungen der gefährlichen U-Boote verfolgen und bedrohte Frachtschiffe rechtzeitig umleiten zu können. Aus Bletchley Park kommen für dieses Lagebild anfangs aber noch kaum verwertbare Entzifferungserkenntnisse. Noch hält der deutsche Marineschlüssel. Man muss sich bezüglich der Standorte deutscher U-Boote mit Erkenntnissen der Funkpeilung begnügen. Dazu werden unmittelbar nach Erfassung eines deutschen Funkspruchs mehrere Stationen alarmiert, die das sendende Boot aus unterschiedlichen Richtungen einzupeilen versuchen. Dies bedarf entsprechender Koordination und vor allem schnellen Handelns, denn mit Ende des Funkspruchs ist die Gelegenheit vorüber. Gelingt die Peilung, lässt sich aus dem Schnittpunkt der Peillinien der Standort des erfassten Bootes errechnen. Das Ergebnis wird an den Befehlshaber der Region weitergeleitet, damit er das geortete Boot bekämpfen kann.

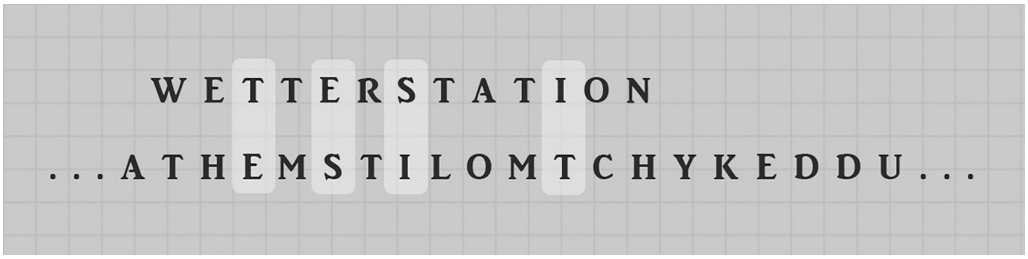
Aus Mangel an Funkpeilstationen außerhalb Großbritanniens verlaufen die Peilstrahlen jedoch oft in sehr spitzem Winkel, weswegen sie vor allem bei Peilungen auf große Distanz ungenaue Ergebnisse liefern. Solche Ungenauigkeiten auf der Karte bedeuten auf hoher See bisweilen riesige Entfernungen, und dies wiederum kann zur Folge haben, dass das winzige Ziel in den Weiten des Ozeans nicht gefunden wird. Die Briten beginnen deshalb, für exaktere Peilungen an allen möglichen Küsten der Welt Stationen einzurichten. Darüber hinaus werden die eingesetzten Peilgeräte immer empfindlicher und erlauben das Einpeilen von immer kürzeren Sprüchen.
Im Gegenzug wird auf deutscher Seite ein Kurzsignalverfahren forciert, das die Funkdauer auf einige Sekunden senken und dem Gegner möglichst wenig Zeit zum Peilen lassen soll. Dem liegt ein zehnseitiges *„U-Boot-Kurzsignalheft"* zugrunde, das die Boote auf See mitführen. Es stellt eine Auflistung der wichtigsten Standardphrasen des Seekrieges dar – seien es Feindlagemeldungen oder Operationsabsichten. Jeder der Phrasen ist eine Gruppe aus drei Buchstaben zugeordnet, die stellvertretend gefunkt zu werden hat. Ein derartiger Funkspruch soll aus höchstens zwei solcher Gruppen bestehen, zuzüglich eines Buchstabenkürzels, das die Identität des sendenden Bootes ausweist. Bei Bedarf werden mit diesem Kurzsignalverfahren auch Standortmeldungen übermittelt.
Vor dem Absetzen des Kurzsignals werden die Buchstaben auf der Enigma mit einem Spruchschlüssel chiffriert, den der Schlüssler einer von zwei vorgedruckten Schlüsseltafeln (für gerade und ungerade Monate) entnimmt. Darauf befinden sich je 26 Spruchschlüsselvorschläge, denen jeweils ein Buchstabe des Alphabets zugewiesen ist. Der Einzelbuchstabe des gewählten Spruchschlüssels wird am Beginn des Funkspruchs gesendet, um den Empfänger zum richtigen Spruchschlüssel zu führen und ihm so das Entschlüsseln zu ermöglichen.
Ähnliches gilt für die Übermittlung regelmäßiger Wetterfunksprüche, die für großräumige taktische Planungen der U-Boot-Führung ebenso unverzichtbar sind wie Meldungen zu Feindlage und Konvoisichtungen. Die Boote führen gedruckte *„Wetterkurzschlüssel"* mit, worin unterschiedliche meteorologische Informationen bestimmten Buchstaben zugeordnet werden. Ein Wetterfunkspruch eines U-Bootes enthält demzufolge einzelne Buchstaben für geografische Länge und Breite der aktuellen Position des Boots, für Luftdruck, Temperatur, Windrichtung und –stärke, Wetter, Wolken und Sichtverhältnisse sowie ein Buchstabenkürzel des Absenders. Die zusammengestellten Buchstaben werden vor dem Absenden auf der Enigma chiffriert, und zwar mit einem Spruchschlüssel, ausgewählt aus einer Schlüsseltafel mit 26 Vorschlägen.

Anfangs sind die nur schwach geschützten Schiffskonvois der Alliierten leichte Beute. Die Zahl an Versenkungen durch deutsche U-Boote steigt rasch an. Neben dem Verlust von Nahrungsmitteln und Kriegsgerät macht sich der an Schiffen selbst schmerzlich bemerkbar. Überdies sterben zivile Matrosen in großer Zahl.
Angesichts der dramatischen Lage wächst in Bletchley Park die Überzeugung, dass man mit Kryptologie alleine nicht ans Ziel kommt, zumindest nicht rechtzeitig. Einen Ausweg erkennt man in der Erbeutung aktueller Schlüsselunterlagen, weshalb bald regelrechte Beutezüge vonstatten gehen.
Nachdem im August 1940 auf einem deutschen Schiff die letzte noch unbekannte Walze *VIII* erbeutet werden kann, erfolgt im Februar 1941 ein geheimes Kommandounternehmen mit ähnlichem Auftrag. Mehrere Kriegsschiffe laufen in Richtung Norwegen aus und stellen ein deutsches Vorpostenschiff. An Bord können Schlüsselunterlagen sichergestellt werden. Teil der Beute sind unter anderem die Februar-Einstellungen des wichtigsten Marineschlüsselkreises *„Heimische Gewässer"*, der in Hut Eight als *„Dolphin"* firmiert. Die lang ersehnten Unterlagen zu Walzenlage und Ringstellungen sowie Grundstellung und Steckerverbindungen ermöglichen, dass noch am 12. März, dem Tag, an dem Alan Turing die Dokumente in die Hände bekommt, einige alte deutsche Marinefunksprüche entziffert werden können. Der zutage tretende Inhalt ist von mäßigem Interesse, doch immerhin erbringen die Dechiffrierungen einige Mosaiksteine für die Rekonstruktion der aktuellen Doppelbuchstabentauschtafeln. Ende März sind diese ziemlich komplett, was eine unverzichtbare Voraussetzung für das Schlüsselbrechen darstellt.
Die Jagd nach Schlüsselunterlagen geht indes weiter. In Hut Four folgert Harry Hinsley aus seinen Funkverkehrsanalysen, dass deutsche Wetterschiffe an entfernteste Punkte entsandt werden, um Wetterbeobachtungen zu machen und nach Deutschland zu funken. Er empfiehlt in einem Bericht an die Admiralität, ein solches Schiff zu kapern, das auf seinen langen Fahrten Schlüsselunterlagen für Monate auf See mitführen würde. Die Admiralität stimmt dem zu. In weiterer Folge wird Anfang Mai 1941 ein deutsches Wetterbeobachtungsschiff über Einpeilung seiner Funksprüche geortet und von sieben britischen Kriegsschiffen gestellt. Erneut werden wichtige Schlüsselunterlagen erbeutet.
Noch reichere Beute machen die Briten nur zwei Tage danach, als es gelingt, das deutsche U-Boot U 110, das in einen Schiffskonvoi eingedrungen ist und Schiffe torpediert, so schwer zu beschädigen, dass es nicht mehr entkommen kann. Der Kommandant des U-Boots befiehlt der Besatzung, das angeschlagene Boot zu verlassen. Da er meint, es werde ohnehin bald

sinken, verzichtet er darauf, die geheimen Schlüsselunterlagen über Bord zu werfen. Die Besatzung wird von den Briten gefangen genommen. Der Kommandant, der im letzten Moment bemerkt, dass sein Boot nicht sinkt, findet beim Versuch zurückzuschwimmen den Tod.
Letztlich geht ein britisches Enterkommando an Bord und stellt neben der Enigma Planquadratkarten für den Nordatlantik und das Mittelmeer sicher sowie das Kenngruppenbuch, Doppelbuchstabentauschtafeln, das Kurzsignalheft und das Wetterkurzsignalbuch, weiters Tagesschlüssel für die Monate April bis Juni, Schlüsseltafeln für den Offiziersschlüssel, Unterlagen für das Reservehandverfahren und die Funkkladde. Die umfangreichen Unterlagen versprechen tiefe Einblicke in den Marineschlüssel, und – was entscheidend ist – es gelingt, die Erbeutung gegenüber der deutschen Seite geheim zu halten, sodass das Schlüsselverfahren nicht grundlegend geändert wird.
Auf der anderen Seite ist Karl Dönitz zwar misstrauisch und um die Schlüsselsicherheit seiner U-Boote besorgt. Seine Bedenken werden aber durch die zuständige Marineabteilung zerstreut. Erbeutete Unterlagen seien für den Gegner nur dann von Wert, wenn er gleichzeitig über eine Enigma verfügen und das Schlüsselverfahren im Detail kennen würde, und selbst dann würde sein Einbruch auf die Geltungsdauer der Schlüsselunterlagen begrenzt bleiben, heißt es beschwichtigend. Zudem könne der Beobachtungsdienst keinerlei Veränderung der Sicherheitsvorkehrungen im britischen Funkverkehr erkennen, welche die Briten zweifellos veranlasst haben würden, hätten sie Kenntnis des Enigma-Schlüssels. Schließlich könnten sie dann dem deutschen Funkverkehr entnehmen, dass auch ihr Funk mitgelesen wird.
Diese Beschwichtigung entspringt einer groben Fehleinschätzung der Situation. Denn in Wahrheit verhelfen die zahlreichen erbeuteten Unterlagen den Kryptologen um Turing in Hut Eight, wo fortan im Schichtbetrieb rund um die Uhr gearbeitet wird, zu einem Durchbruch. Man kann den Marineschlüsselkreis Dolphin brechen und bis auf Weiteres den Funkverkehr der deutschen U-Boote im Atlantik mitlesen. Selbst Befehle von Dönitz liegen nun offen.
Wann immer es gelingt, einen Schlüssel zu brechen, wird der betreffende Spruch in Hut Four übersetzt und danach umgehend nach London an den Submarine Tracking Room geleitet, wo alle Informationen zusammenlaufen. Anfang Juni 1941 ist man in der Lage, Bewegungen deutscher U-Boote mitzuverfolgen. Und es gelingt, deutsche Versorgungsschiffe zu versenken, die an bestimmten Treffpunkten für die auf See befindlichen U-Boote und Kriegsschiffe bereitstehen.
Auf der anderen Seite des Ärmelkanals erregen die gehäuften Versenkungen neuerlich Misstrauen. Dönitz fürchtet erneut um die Sicherheit des

Enigma-Schlüssels, wenngleich eine eingeleitete interne Untersuchung wieder keinerlei Anzeichen dafür erbringt, dass dieser kompromittiert sei. Auf Drängen der Verantwortlichen in Bletchley Park laufen bald darauf wieder britische Kriegsschiffe aus, deren Kommandanten den Auftrag haben, aktuelle Schlüsselunterlagen zu erbeuten. Sie begeben sich auf die Suche nach einem deutschen Wetterbeobachtungsschiff, das nördlich von Island vermutet wird. Nachdem sie es gefunden und aufgebracht haben, erbeuten sie Schlüsselunterlagen für den Monat Juli. Anfang Juli gelangen die Unterlagen zu Turing in Hut Eight, wo man mit ihrer Hilfe für den Rest des Monats binnen weniger Stunden deutsche Marinefunksprüche entziffern kann.
Solche Entzifferungserfolge sind jedoch nur Erfolge auf Zeit; dessen ist man sich bewusst. Irgendwann treten wieder neue Schlüsselunterlagen in Kraft, die die Möglichkeit des Mitlesens beenden. Außerdem steht die britische Admiralität Kaperfahrten zunehmend skeptischer gegenüber. Sie will das Misstrauen auf deutscher Seite nicht noch weiter schüren.

Liegen keine erbeuteten Dokumente vor, müssen die Spezialisten in Hut Eight den beschwerlichen Weg gehen und mit Hilfe eines *„Crib"* genannten Textfragments und entsprechend aufwändiger Bombe-Suchläufe in aktuelle Tagesschlüssel einbrechen. Es ist ein steiniger Weg, denn schon die Suche nach Cribs gestaltet sich in der Anfangsphase schwierig. Um zu einem Erfolg versprechenden Crib zu kommen, muss man viel deutschen Funk mitlesen können und die Gewohnheiten der Funker sowie die geltenden Verfahrensweisen kennen; umgekehrt bedarf es guter Cribs, um mitlesen und Erfahrungen gewinnen zu können. Um diesen Teufelskreis zu durchbrechen, beginnt man damit, regelmäßig abgesetzte Funksprüche zu sammeln und deren Rufzeichen, Uhrzeit und Länge sowie die Frequenzen zu registrieren, auf denen sie gesendet bzw. wiederholt werden. Dahinter steht die Hoffnung, Routinemeldungen zu entdecken, in denen tagtäglich identische Wörter benützt werden. Mit der Zeit wird man fündig, und zwar vor allem bei Wettermeldungen, die von deutschen Stationen in Kanalhäfen wie Boulogne und Cherbourg routinemäßig gesendet werden. Aus ihnen lassen sich Cribs gewinnen, die Einbrüche in den deutschen Funkverkehr ermöglichen; eine Methode, die Alan Turing perfektioniert.
Turing versucht zunächst ein im Funkspruch vermutlich enthaltenes Wort – beispielsweise *„Wetterstation"* – in den Chiffren zu lokalisieren. An der vermuteten Stelle sucht er dann nach Beziehungsschleifen, so genannten *„Closures"*, wie sie zwischen Klartextbuchstaben und den darunter geschriebenen Chiffren auftreten: Wenn etwa das erste *T* des Wortes



29 *Closure zur Programmierung auf einer Bombe*

Wetterstation etwa in die Chiffre *E* übergeht, zwei Stellen später das *E* von Wetterstation in die Chiffre *S*, zwei weitere Stellen später das *S* in *I* und weitere vier Stellen später das *I* schließlich wieder in ein *T*, schließt sich die Schleife *T/E/S/I/T*. Nunmehr gilt es herauszufinden, wo in der Maschinenperiode diese Schleife liegt. Dazu wird die Bombe folgendermaßen eingestellt: Ein erster der miteinander gekoppelten Enigma-Walzensätze wird als Ausgangspunkt festgelegt und auf *03* eingestellt, für die dritte Stelle des Cribs, an der *T* in *E* übergeht. Ein zweiter Walzensatz wird um zwei Stellen vorgedreht, also auf *05* für die fünfte Stelle, an der *E* in *S* übergeht, ein dritter um weitere zwei Stellen auf *07* für die siebente Stelle, an der *S* in *I* übergeht, und ein letzter um vier Stellen auf *11* für die elfte Stelle, an der *I* schließlich wieder in *T* übergeht.
Nach dem Einstellen erfolgt der Start und die gekoppelten Walzensätze laufen synchron sämtliche Stellungen der Maschinenperiode durch. Wenn eine Stellung erreicht ist, an der Eingangs- und Ausgangsbuchstabe gleich sind, hält die Bombe automatisch an. Das muss nicht unbedingt bei einem *T* sein, nachdem Stecker wirksam sind, könnte es auch bei irgendeinem anderen Buchstaben, der mit *T* gesteckt ist, geschehen. Es muss nur derselbe Buchstabe am Ausgang stehen wie am Eingang.
Jede der Stellungen, an der die Bombe anhält, wird daraufhin analysiert, ob es sich um die gesuchte Schlüsselstellung handelt. Nur dort hat man es mit Klarbuchstaben bzw. ihren Steckerverbindungen zu tun; überall sonst lediglich mit Chiffren. Nur dort gilt, dass wenn am Haltepunkt nicht Ts, sondern beispielsweise Ks stehen, T mit K gesteckt ist. In diesem Fall hat man neben der Schlüsselstellung auch eine erste Steckerverbindung gefunden. Darüber hinaus lassen sich für alle anderen Buchstaben des Cribs und die für sie von der Bombe ausgewiesenen Chiffren Steckerannahmen treffen. Auf diese Weise werden so viele Steckerverbindungen wie möglich hergeleitet. Fehlende Stecker können auf einer nachgebauten Enigma rekonstruiert werden. Dazu werden die Walzenstellungen, die die Bombe beim Anhalten aufweist, als Schlüsselstellung eingestellt und die bereits

30 *Bombes laufen rund um die Uhr*

gefundenen Stecker gesteckt. Nach Eintippen der Chiffren des betreffenden Funkspruchs erscheinen klare Textfragmente neben verwürfelten. Durch gezieltes Austauschen von Buchstaben kann man den Text nach und nach in Klarform bringen und dabei die letzten unbekannten Stecker rekonstruieren.[7]

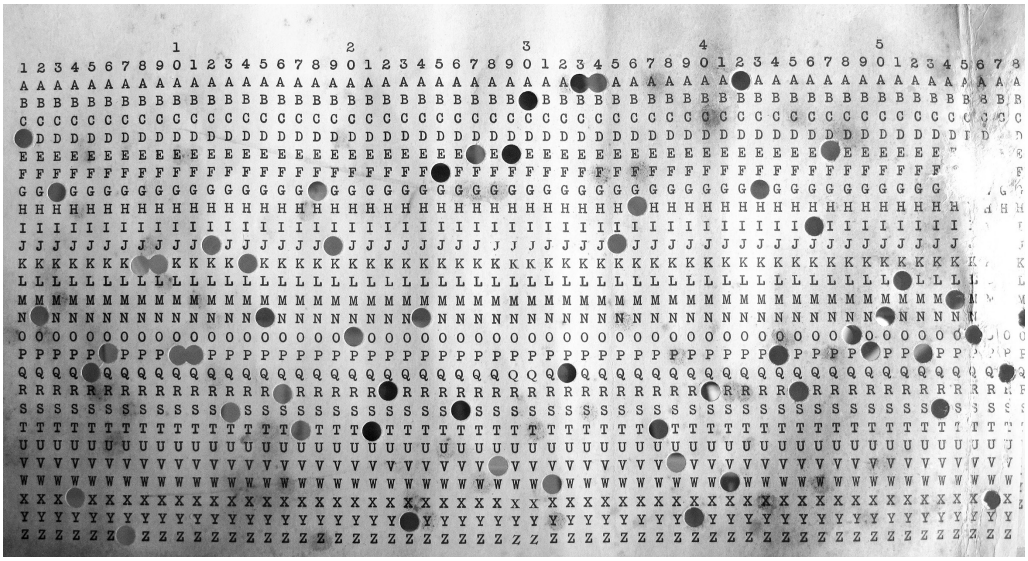
Liefert die Bombe bis zum Ende des Durchlaufs kein gültiges Ergebnis, ist möglicherweise die untersuchte Walzenlage falsch und das Schleifenmenü muss mit der nächstmöglichen Lage durchgespielt werden. Sind alle Walzenlagen getestet – im schlimmsten Fall sind dies 336! – und die Bombe hat noch immer kein Ergebnis erbracht, ist höchstwahrscheinlich das untersuchte Crib eine Fehlannahme und es muss ein neues gefunden werden, mit dem alles wieder von vorn beginnt.

Die Schwierigkeit, funktionierende Cribs zu finden, entschärft sich ab Mai 1941 mit der Erbeutung eines Wetterkurzsignalbuchs, aus dem fortan die dringend benötigten Textfragmente abgeleitet werden können. Im Laufe der Zeit kristallisieren sich ganze Kategorien an Begriffen heraus, die sich als Cribs eignen. Es entsteht ein eigener *„Crib Room"*, in dem eine vielfältige Sammlung an solchen Begrifflichkeiten systematisch verwahrt wird –

[7] Siehe im Abschnitt *Kryptologie* das Kapitel Turing: *Cribs und Closures*

von Wettermeldungen über standardisierte Anreden bis hin zu Listen von Schiffsnamen. Vor diesem Hintergrund entwickelt sich das Cribbing zu einer vielversprechenden Methode.
Eine Schwäche der Methode bilden angesichts der 336 möglichen Walzenlagen, über die die Marine-Enigma verfügt, die hohen Bombe-Laufzeiten. Bei einer Durchlaufzeit von rund zwanzig Minuten für eine Walzenlage bedeutet das für alle Lagen 112 Stunden Dauerbetrieb einer Bombe, also knapp fünf Tage Laufzeit. Zwar steigt die Zahl an Bombes allmählich auf ein halbes Dutzend, was aber den Kapazitätsengpass nicht nachhaltig beseitigt. Die verfügbaren Bombes laufen zumeist Tag und Nacht, sieben Tage in der Woche. Sie werden nur für die regelmäßigen Servicearbeiten abgeschaltet. Da immer mehr Männer zum Frontdienst eingezogen werden, sind es zunehmend Frauen, die sie bedienen – Angehörige des *„Women´s Royal Navy Service"*, kurz *„Wrens"*. Sie laden die Maschinen unablässig mit Walzen, ohne den Zweck ihrer Tätigkeit zu kennen.
Ist eine der gesuchten Einstellungen gefunden und die Maschine hält an, muss ein Analytiker gerufen werden. Jener muss dann mitunter feststellen, dass das Ergebnis, das die Bombe nach vielen Stunden anzeigt, nicht das gesuchte ist. Dann rattert die Maschine weiter. Liegt nach Stunden oder Tagen endlich ein Ergebnis vor, ist am Atlantik so manches bedrohte Schiff bereits gesunken. Es erscheint unumgänglich, das Analyseverfahren zu beschleunigen, will man die gewonnenen Erkenntnisse auch militärisch effektiv nutzen können.

Zur Beschleunigung des Verfahrens wird eine Methode forciert, die auf die polnische Uhrenmethode zurückgeht. Sie soll durch Identifizierung der rechten Walze die große Zahl an zu untersuchenden Walzenlagen senken. In ihrer einfachsten Erscheinungsform bedient sie sich zweier Funksprüche, die nahezu derselben Schlüsselstellung entstammen. Linke und mittlere Walze sollen identisch stehen, was sich an ihren Spruchschlüsseln ersehen lässt, wenn sie in klarer Form vorliegen. Bei *H-D-O* und *H-D-V* beispielsweise befinden sich linke und mittlere Walze in der gleichen Stellung. An den Stellungen der rechten Walze lässt sich eine Differenz von sieben Maschinenschritten (von *O* bis *V*) ablesen. Die Chiffren der beiden Sprüche werden nun um diese Differenz verschoben untereinander geschrieben, sodass sie synchronen Maschinenstellungen entsprechen. Nun kann die Häufigkeit ermittelt werden, wie oft gleiche Chiffren untereinander zu liegen kommen. Normalerweise sollte dies durchschnittlich alle dreizehn Stellen der Fall sein. Sinkt aber die Häufigkeit auf den halben Wert, verweist dies darauf, dass die Sprüche unterschiedlichen Schlüsseln entstammen, dass also die rechte Walze zwischen *O* und *V* einen Übertrag ausge-



31 *Banbury Sheet*

löst hat. Die Drehstellung, an der er geschehen ist, lässt darauf schließen, welche Walze ihn ausgelöst hat und somit an der rechten Position liegt. Hat man ein Ergebnis, braucht man zum Schlüsselbrechen nur noch jene Walzenlagen zu untersuchen, bei denen besagte Walze rechts liegt. Das sind nur noch 42!

Die Methode wird in Bletchley Park mit so genannten *„Banbury Sheets"* praktiziert, benannt nach der Stadt Banbury, wo die Papierstreifen hergestellt werden. Dabei handelt es sich um rund 25 Zentimeter hohe und mehrere Meter breite Streifen, bedruckt mit bis zu 200 senkrecht geschriebenen Alphabeten nebeneinander. In diese vorgedruckten Alphabete werden die Chiffren eines Funkspruchs gelocht: die erste Chiffre – etwa *D* – in das erste Alphabet an der D-Position, die zweite Chiffre ins zweite Alphabet an der entsprechenden Position usw. In gleicher Weise sind die Chiffren anderer Funksprüche auf Streifen zu lochen. Zur Analyse werden die Streifen zweier Funksprüche auf einem Lichttisch übereinander gelegt, ausgerichtet entsprechend der Differenz der Stellungen ihrer rechten Walzen. Wegen des durchscheinenden Lichts lässt sich auf einen Blick feststellen, wieviele übereinstimmende Chiffren es gibt. Aus der Häufigkeit der Übereinstimmungen kann man ableiten, ob zwischen den beiden untersuchten Sprüchen (genauer: im Differenzbereich ihrer geringfügig unterschiedlichen Spruchschlüssel) ein Übertrag passiert ist. Daran lässt sich erkennen, welche Walze ihn verursacht hat – zumindest, wenn es sich um

eine der Walzen *I* bis *V* handelt. Für die Nummern *VI* bis *VIII* ist dies nicht möglich, denn diese drei Walzen verfügen bereits über je zwei Übertragskerben, welche noch dazu bei allen dreien an denselben Positionen sitzen, sodass sie daran nicht unterscheidbar sind.
Es können jedoch auch aus Fällen, wo im untersuchten Abschnitt kein Übertrag passiert, verwertbare Erkenntnisse gewonnen werden. Man kann schließlich jede Walze kategorisch ausschließen, deren Übertragskerbe eben dort sitzt, also einen Übertrag hätte auslösen müssen.
Darüber hinaus kommt den Briten zugute, dass die deutsche Seite einmal mehr schwere Fehler begeht. Sie lässt geradezu gesetzmäßig an jedem Tag eine der drei sichereren Walzen *VI, VII* und *VIII* verwenden. Das bedeutet umgekehrt, dass Walzenkombinationen, die keine der drei beinhalten, in Hut Eight nicht untersucht werden müssen, und das sind immerhin 60.
Darüber hinaus wird im Lauf der Zeit erkennbar, dass nach dem Walzenwechsel keine der Walzen an der Stelle liegt, an der sie zuvor gelegen ist. Solche Lagen kann man ebenfalls ausschließen. Alleine dadurch reduziert sich die Zahl von 336 auf 210. Durch Anwendung solcher Erkenntnisse werden so viele Walzenlagen wie möglich von vornherein ausgeschlossen, um die zu untersuchenden im günstigsten Fall auf einige wenige zu reduzieren, die auf den Bombes mithilfe von Cribs in einer überschaubaren Zeit geprüft werden können.
Trotzdem bleibt der Aufwand beträchtlich. Es dauert ein, zwei Tage oder länger, bis Ergebnisse vorliegen, und alle zwei Tage, wenn auf den U-Booten routinemäßig die inneren Einstellungen geändert werden, beginnt die gesamte Prozedur aufs Neue.
In ihrer Durchführung erweist sich die Banbury-Methode zudem deutlich aufwändiger als zu Zeiten ihrer Erfindung in Polen. Wegen der großen Zahl an Walzenlagen, die jetzt möglich sind, müssen im Vorfeld hunderte aktuelle Funksprüche aufgefangen werden, um zwei zu finden, die bei identischer Stellung von mittlerer und linker Walze chiffriert worden sind. Um aber die Stellungen von mittlerer und linker Walze überhaupt erkennen zu können, bedarf es vorher der Entschlüsselung der Spruchschlüssel, die bekanntlich mittels Buchstabenpaaren aus den Doppelbuchstabentauschtafeln verschlüsselt sind. Die britischen Kryptologen müssen deshalb nebenher immer auch an der Rekonstruktion dieser Doppelbuchstabentauschtafeln arbeiten, die von deutscher Seite alle paar Monate erneuert werden. Dazu bedarf es der Entzifferung möglichst vieler Funksprüche, um die darin verwendeten Doppelbuchstaben zu identifizieren. Dafür wiederum braucht es die Einstellungen des aktuellen Tagesschlüssels, die mithilfe langer Bombe-Suchläufe gefunden werden müssen. Liegen diese vor, werden mithilfe einer Methode, die *„EINSING“* genannt wird, Spruchschlüssel

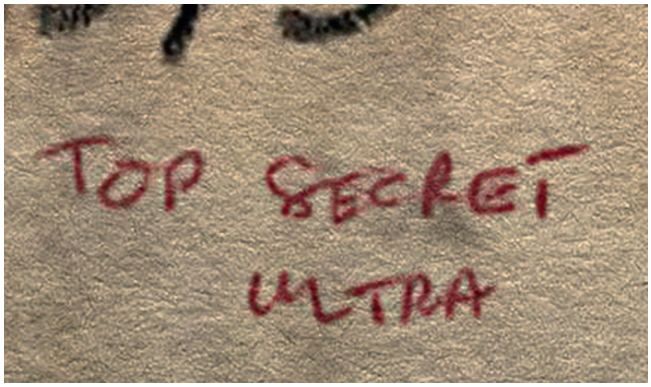
32 *Geleitzug auf hoher See*

aufgefangener Sprüche geknackt, um zu den verwendeten Doppelbuchstaben zu kommen.
Bei seiner Beschäftigung mit dem deutschen Marinefunkverkehr hat Turing erkannt, dass an die 90 Prozent der deutschen Sprüche das Wort *„eins"* enthalten, was nicht zuletzt darauf zurückgeht, dass Zahlen laut deutscher Dienstvorschrift ausgeschrieben werden müssen. Das Wörtchen *„eins"* scheint ein ideales Crib. Mit diesem Wissen erstellt er nun einen aktuellen *„EINS catalogue"*, worin er alle Viererchiffren in alphabetischer Reihenfolge verzeichnet, die das Wort *„eins"*, an jeder Maschinenstellung bei aktuellem Tagesschlüssel chiffriert, ergibt. Danach werden aufgefangene Sprüche daraufhin untersucht, ob eine der im Katalog verzeichneten Viererchiffren enthalten ist. Ein allfälliger Treffer wird an einer nachgebauten Enigma getestet: Man stellt dazu die Maschineneinstellungen laut besagtem Katalogeintrag ein und tippt weitere Chiffren des Funkspruchs. Erscheint Klartext, hat man den Spruchschlüssel gefunden. Mit seiner Hilfe können die im Funkspruch ausgewiesenen Doppelbuchstabenpaare rekonstruiert werden – zumindest einmal zwei davon, da man die vom Schlüssler frei gewählten Füllbuchstaben nicht kennt. Jedenfalls lassen sich auf diese Weise Schritt für Schritt die Doppelbuchstabentauschtafeln

33 *Ein sinkender Tanker der Alliierten*

komplettieren. Am Ende können Spruchschlüssel aufgefangener Sprüche einfach nachgeschlagen werden – so lange, bis neue Tauschtafeln in Kraft treten.

Im Sommer 1941 präsentiert sich die Lage am Atlantik dramatisch wie nie zuvor. Es versinken doppelt so viele Schiffe der Alliierten wie zur gleichen Zeit in britischen und amerikanischen Werften gebaut werden können. Der Nachschub an Kriegsgerät stockt, Lebensmittel für die britische Bevölkerung werden rar und rationiert. Die Lebensader nach Nordamerika droht zu reißen. Doch es gelingt, die Katastrophe abzuwenden.
Eine Ursache dafür ist neben den Informationen, die die Briten aus Funkpeilungen, der Luftaufklärung sowie von telegrafischen und telefonischen Nachrichten von Agenten aus Häfen in aller Welt beziehen, das Eindringen in den deutschen Marineschlüssel. Dank der Cribs aus den Wetterkurzsignalen ist es Hut Eight in der zweiten Hälfte des Jahres 1941 möglich, die meisten Tagesschlüssel von Dolphin mit ein- oder zweitägiger Verzögerung zu brechen. Das entzifferte Material gelangt über eine sichere Fern-



34 *Enigma-Nachrichten – Top Secret Ultra*

schreibleitung nach London, wo der Submarine Tracking Room infolge des Sprudelns der geheimen Nachrichtenquelle immer effizienter funktioniert. Die einlangenden Funksprüche geben laufend neue Hinweise auf deutsche U-Boote, welche auf der stetig aktualisierten Lagekarte neben britischen Kriegsschiffen, diversen Schiffskonvois wie auch einzeln fahrenden Frachtschiffen verzeichnet werden. Wie auf einem magischen Schirm gibt die Karte das Geschehen fast in Echtzeit wieder. Dadurch lassen sich gezielte Maßnahmen in die Wege leiten, die zu einem deutlichen Rückgang an Schiffsverlusten führen: Manchmal werden bedrohte Konvois umgeleitet, sodass die lauernden U-Boote ins Leere laufen. Mitunter werden Gegenangriffe geführt, wobei man sich dabei immer um Tarnung bemüht. Hat man die Position eines U-Bootes ausgemacht, schickt man zuerst ein Aufklärungsflugzeug an die Stelle, um den Schein zu wahren und nach außen hin den Eindruck zu vermitteln, man habe das Boot zufällig aus der Luft entdeckt. Erst dann wird es bekämpft. Die deutsche Seite soll auf keinen Fall Rückschlüsse darauf ziehen können, dass man ihre Funksprüche mitliest; zu wichtig ist die erschlossene Quelle, als dass man ihr Versiegen riskieren dürfte. Aus diesem Grund unterliegt alles, was mit der Enigma zu tun hat, nach wie vor allerstrengster Geheimhaltung. Für Berichte aus Bletchley Park wird der höchsten Geheimhaltungsstufe *„Top Secret"* noch das Wort *„Ultra"* angefügt. Die Enigma ist *„Top Secret Ultra"*.
Gleichzeitig macht der Kriegsverlauf klar, dass in Bletchley Park Kapazitäten fehlen, um den Arbeitsaufwand bewältigen zu können. Das gilt für Bombes wie für Personal. Da offizielle Stellen wenig Bereitschaft zeigen, Personal abzustellen und Unterstützung zu leisten für eine Organisation, deren Zweck nicht bekannt ist und auch nicht bekannt werden darf, wenden sich die Kryptologen um Turing mit der Bitte um Mittel direkt an den britischen Premierminister Winston Churchill. Churchill, der große

Stücke auf seine Ultra-Geheimnachrichten hält, gibt daraufhin Anweisung, Bletchley Park jegliche Unterstützung zukommen zu lassen. In weiterer Folge fließen Gelder, neue Abhörstationen werden eingerichtet, weitere Bombes gebaut, Personal wird rekrutiert. Eine eigene Schule für Kryptoanalytiker soll helfen, den steigenden Bedarf an Spezialisten zu decken.

Ende August 1941 können die Briten am Atlantik das nach einem Flugzeugangriff beschädigte U-Boot U 570 aufbringen und die Besatzung gefangen nehmen. Der U-Boot-Kommandant kann zuvor noch einen Funkspruch absetzen, in dem er berichtet, er werde angegriffen und sei nicht mehr in der Lage zu tauchen. Dadurch ist die deutsche U-Boot-Führung gewarnt und muss sich wieder die unangenehme Frage stellen, ob der Gegner Schlüsselunterlagen erbeutet haben könnte. Dönitz lässt einmal mehr die Sicherheit der Enigma prüfen, doch bringt die Überprüfung wenig Überraschendes zutage. Es heißt, sofern die Briten das Boot samt Unterlagen erbeutet hätten, wäre der Schlüssel bedroht – zumal dann, wenn die gefangen genommenen Offiziere das ausgegebene Kennwort verraten würden, das dazu dient, im Notfall einen alternativen Schlüssel in Kraft zu setzen. Es sei jedoch unwahrscheinlich, dass die Briten sowohl über die Unterlagen verfügen als auch Kenntnis vom Kennwort haben würden. Im November 1941 träten aber ohnehin neue Schlüssel in Kraft und spätestens dann sei die Sicherheit wieder voll hergestellt.
Das angesprochene Kennwort ist Teil des *„Stichwort-Verfahrens"*, das es erlaubt, sämtliche Funkstationen eines Schlüsselkreises mit einem Schlag auf einen neuen, sicheren Schlüssel umzustellen, sollte der Gegner Schlüsselunterlagen erbeutet haben. Dazu wird den Kommandanten auf See beispielsweise die Anordnung *„Stichwortbefehl Perseus"* gefunkt, die ihnen befiehlt, einen mitgeführten, im vorliegenden Fall mit *„Perseus"* beschrifteten Umschlag zu öffnen. Darin enthalten ist ein Kennwort, das in die Schlüsseleinstellungen einzurechnen ist. Lautet das Kennwort etwa *„Danzig"*, beginnend also mit *D*, dem vierten Buchstaben im Alphabet, ist die aktuelle Walzenlage um den Wert vier nach oben zu korrigieren: beispielsweise ist dann statt Walze *II* Walze *VI* zu verwenden, statt Walze *I* Walze *V* und statt Walze *VII* Walze *III*, denn nach acht (Walzen) wird wieder bei eins zu zählen begonnen. Die folgenden drei Buchstaben des Stichworts – *A, N* und *Z* – weisen den Schlüssler an, gemäß den Positionen im Alphabet die Werte eins, vierzehn bzw. sechsundzwanzig zu den ursprünglichen drei Ringstellungen zu addieren. In gleicher Weise sagt ihm der nächste Buchstabe des Stichworts, das *I*, der neunte Buchstabe des Alphabets, zu den vorgegebenen Steckerverbindungen jeweils neun zu addieren.

So simpel das Stichwortverfahren erscheinen mag, es stellt ein sehr effektives Instrument dar, um Angehörigen eines Funknetzes augenblicklich einen neuen Schlüssel zu geben, wo auch immer sie sich gerade aufhalten. Doch ein derartiges Notsystem ist angesichts der zunehmenden Bedrohung nicht mehr ausreichend. Vielmehr scheint nun dringend nötig, das Enigma-Schlüsselverfahren insgesamt aufzurüsten. Die Tage seiner Unangreifbarkeit sind vorüber.

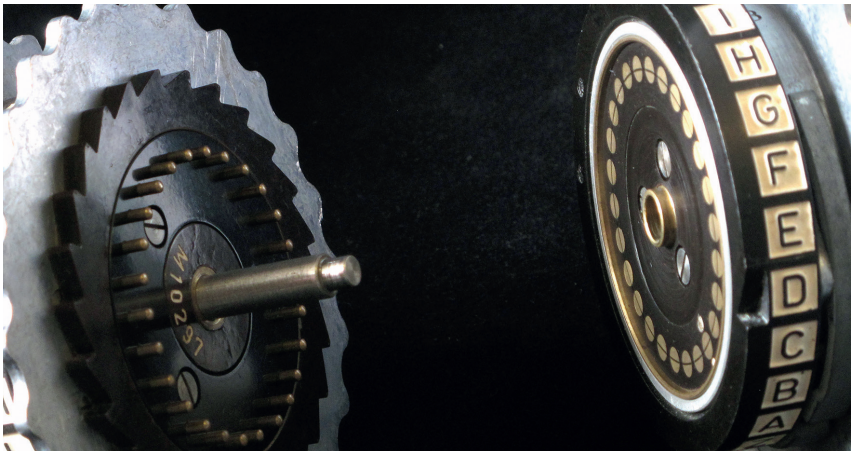
Im Januar 1942 tritt ein umfassendes Kurzsignalverfahren in Kraft, das verschiedene Vorläuferverfahren ersetzt. Auf nunmehr 120 Seiten deckt das neue *„Kurzsignalheft"* mit seinen Phrasen einen großen Bereich an Themen ab, die für den Seekrieg relevant sind – von der Feindlage über Treffen mit Versorgungsbooten bis zu Angaben zur Position gemäß Planquadraten oder zu Kurs und Geschwindigkeit. Den Phrasen sind jetzt vierstellige Buchstabengruppen (*„Signalgruppen"*) zugeordnet, die an ihrer Stelle gefunkt werden müssen, und zwar zwischen ein und sechs je Funkspruch. Vor dem Absetzen werden diese Gruppen samt zusätzlichen Gruppen für Position und Identität des Absenders auf der Enigma chiffriert. Der dabei zu verwendende dreistellige Spruchschlüssel ist – wie die ebenfalls dreistellige, zugehörige Kenngruppe – aus einem vorgedruckten *„Kenngruppenheft"* auszuwählen, das hunderte solcher Kenngruppe-Spruchschlüssel-Kombinationen bereithält.

Damit nicht genug, lässt Dönitz für die U-Boote am Atlantik anlässlich einer geplanten Offensive einen vollkommen neuen Schlüsselkreis *„Triton"* einführen. Das Besondere daran ist, dass es sich um einen vierstelligen Schlüssel handelt, der auf einer Enigma neuen Typs mit einer vierten Walze basiert. Bei dieser Maschine ist die bisher verwendete Umkehrwalze durch eine dünnere Version *B* ersetzt, die noch Platz für eine dünne vierte Schlüsselwalze *Beta* lässt. Diese vierte Walze kann zwar ebenfalls 26 Drehstellungen einnehmen, sie dreht sich jedoch nicht wie die ersten drei im Übertragsgetriebe mit, sondern verharrt in der Stellung, in der sie eingesetzt worden ist. Sie kann ihrer geringeren Dicke wegen auch nicht gegen die anderen drei Walzen getauscht werden. Wird ihr Ring auf *Z* eingestellt und sie so an die zugehörige Umkehrwalze angefügt, dass im Sichtfenster ein *A* erscheint, funktioniert sie wie die alte Umkehrwalze. In dieser Stellung kann auch mit herkömmlichen Dreiwalzen-Enigmas kommuniziert werden.

Schon seit geraumer Zeit sind die Atlantik-U-Boote mit der neuen Vierwalzenmaschine ausgestattet, doch haben sie diese bislang nur im Dreiwalzenmodus benutzt. Abgesehen davon, dass Hut Eight von deren Existenz schon vor geraumer Zeit aus Beuteunterlagen erfahren hat, ist diese Vorgangsweise nicht ohne Risiko. Durch unachtsame deutsche Schlüssler, die

35 *M4 – die Enigma der Kriegsmarine mit vier Walzen*

die vierte Walze versehentlich verwendet haben, können die Kryptologen in Hut Eight nämlich auch deren Verdrahtung herleiten. Man kann sich das so vorstellen: Ein Schlüssler hat die neue Walze nicht in der Neutralstellung *A* stehen, als er eine Nachricht verschlüsselt, die danach gefunkt wird. Vom Empfänger, der den Spruch nicht entschlüsseln kann, auf seinen Fehler aufmerksam gemacht, verschlüsselt er dieselbe Nachricht ein weiteres Mal – nun mit Neutralstellung – und lässt sie abermals funken. Dies aber ist ein kryptologischer Sündenfall. Gelingt es der Gegenseite, derartige Zwillingsversionen in entsprechender Menge aufzufangen, eröffnet ihr dies die Möglichkeit, durch Abgleich der Versionen die Verdrahtung der vierten Walze zu rekonstruieren.



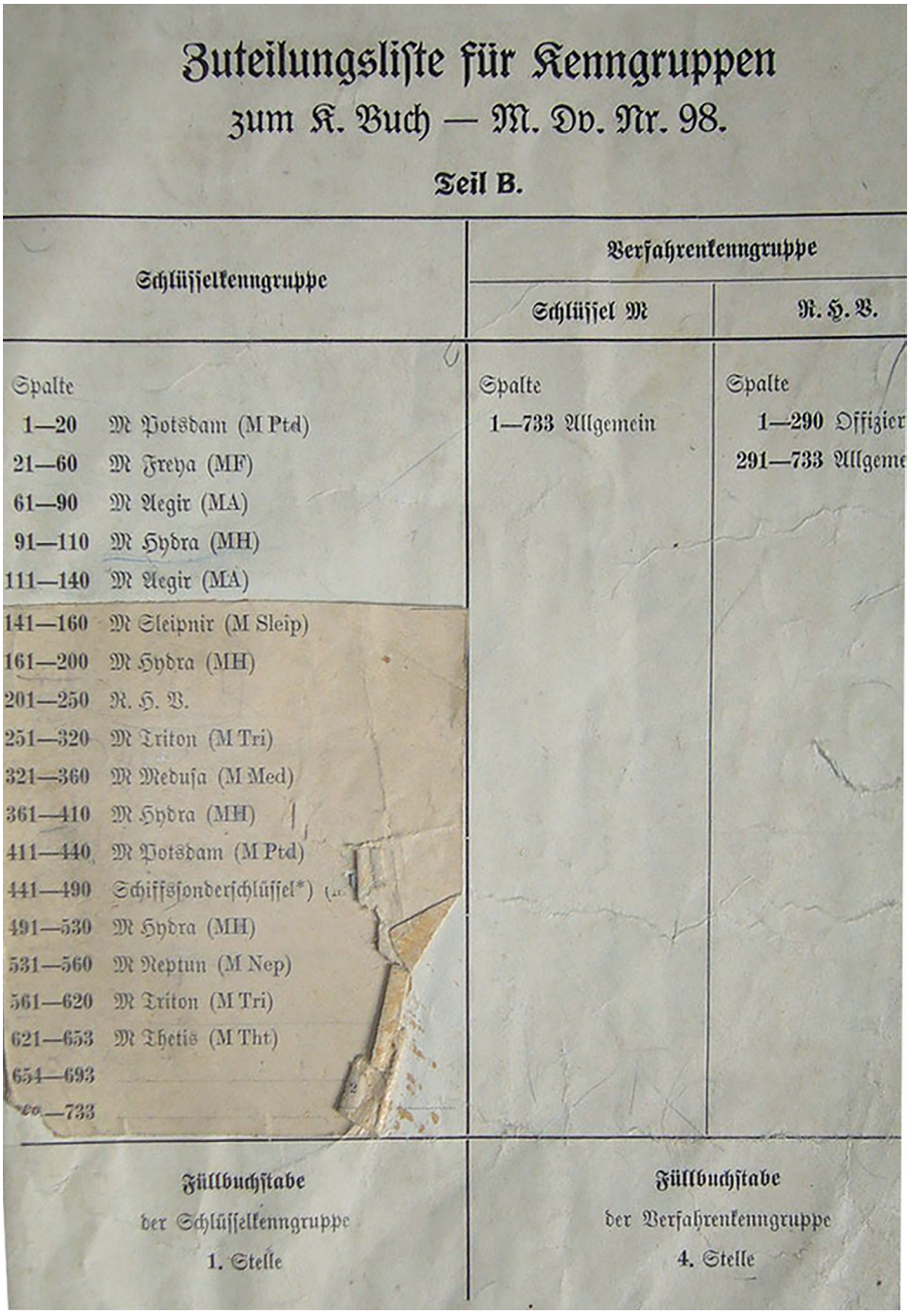
36 *Schlüsselwalzen einer Marine-Enigma mit Buchstaben-Beschriftung*

Als Dönitz am 1. Februar 1942 anordnet, die neue Walze einzusetzen, bedeutet dies für Hut Eight trotzdem einen schweren Rückschlag. Mit einem Mal tappt man wieder völlig im Dunkeln. Die Herausforderung ist groß. Die vierte Walze bietet zu jeder bisherigen Walzenstellung 26 zusätzliche Stellungen und erhöht dadurch die Zahl der Maschinenstellungen von 17.500 auf über 450.000. Das bedeutet für Hut Eight, einfach gesagt, eine Versechsundzwanzigfachung des Arbeitsaufwands. Dabei hält der Umstand, dass die vierte Walze nicht gegen die anderen austauschbar ist, die Katastrophe noch in Grenzen. Wäre sie austauschbar, würde die Zahl an möglichen Walzenlagen von 336 auf über 3.000 in die Höhe schnellen. Doch auch so wird das Kapazitätsproblem akut. Die fünfzehn Bombes, die Bletchley Park in diesen Tagen insgesamt zur Verfügung stehen – jene Exemplare mitgerechnet, die für Heeres- und Luftwaffen-Enigmas im Einsatz sind –, können schon den bisherigen Aufwand kaum bewältigen, ganz zu schweigen von einem derartigen Zuwachs. Abgesehen davon scheint die Kapazität der neuen Enigma M4 grundsätzlich zu hoch, um mit den zur Verfügung stehenden Ressourcen analysiert werden zu können. Selbst eine auf den Vierwalzen-Standard erweiterte Version der Bombe würde letzten Endes zu langsam arbeiten, um zeitgerecht Ergebnisse zu liefern. Die 336 Walzenlagen einer Dreiwalzenmaschine absolviert eine Bombe in 112 Stunden, doch für einen Durchlauf eines Schlüssels der Vierwalzenmaschine würde sie 121 Tage an Rechenzeit rund um die Uhr benötigen. Außerdem funktioniert bei der Analyse der M4 die Banbury-Methode zur Reduzierung der zu untersuchenden Walzenlagen kaum mehr. Diese Methode beruht bekanntlich auf Paaren an Funksprüchen, die mit nahezu

derselben Maschineneinstellung chiffriert wurden. Die enorm hohe Zahl an Einstellmöglichkeiten der M4 lässt aber die Chance, solche Paare zu finden, gegen Null sinken. Verschärft wird die Situation dadurch, dass dem neuen U-Boot-Schlüssel, der in Hut Eight den bedrohlich klingenden Namen *„Shark"* erhält, regelmäßig Stichworte eingerechnet werden. Die Zeit, da man den Funkverkehr der Atlantik-U-Boote mitgelesen hat, scheint vorüber.

Die Marineführung in London sieht sich auf Verfahrensweisen wie das Einpeilen funkender Boote zurückgeworfen. Immerhin sind jetzt die Peilungen genauer als zu Kriegsbeginn. Das Funkpeilnetz verfügt mittlerweile über zahlreiche Stationen in aller Welt. Der Umstand, dass so mancher deutsche U-Boot-Funker von routinierten Funkhorchern oder –horcherinnen an seinem Tastenanschlag erkannt wird, ermöglicht zudem die Bewegungen seines Bootes zu verfolgen. Jeden Morgen werden solche Funkmeldungen und Peilungen ausgewertet, um daraus Rückschlüsse auf bevorstehende Operationen der U-Boote zu ziehen. Schließlich kennt man mittlerweile die strategischen Grundlagen des deutschen U-Boot-Krieges ebenso wie die Akteure und kann entsprechende Annahmen ableiten, zumal noch weitere Informationsquellen existieren.

Die Luftaufklärung liefert regelmäßig fotografische Aufnahmen deutscher Häfen, Werften und Seegebiete, wodurch unter anderem das deutsche U-Boot-Bauprogramm mitverfolgt werden kann. Die Funkaufklärung bietet seit dem Einbruch in einen Schlüssel, der im Rahmen der U-Boot-Ausbildung in der Ostsee verwendet wird, Erkenntnisse über jedes neu in Dienst gestellte Boot. Außerdem bleibt die dreiwalzige Enigma bei diversen U-Boot-Gruppen in Meeresregionen abseits des Atlantiks weiterhin in Verwendung und deren Funkverkehr dadurch lesbar. Andererseits kommen neue unbekannte Schlüssel hinzu. Zur Erhöhung der Sicherheit untergliedert die deutsche Marineführung den Schlüssel Heimische Gewässer (alias Dolphin) in unterschiedliche Schlüsselbereiche mit eigenen Tagesschlüsseln, von denen künftig jeder für sich zu brechen ist. Es ist ein ambivalentes Bild, das sich bietet. Zwar sprudelt noch so manche Informationsquelle, doch ein so umfassendes Lagebild wie vor Einführung der Enigma M4 lässt sich nicht mehr zeichnen, zumal keines, das auch anstehende Operationsplanungen deutscher U-Boote im Atlantik beinhalten würde. Es folgen lange Monate der Ohnmacht.

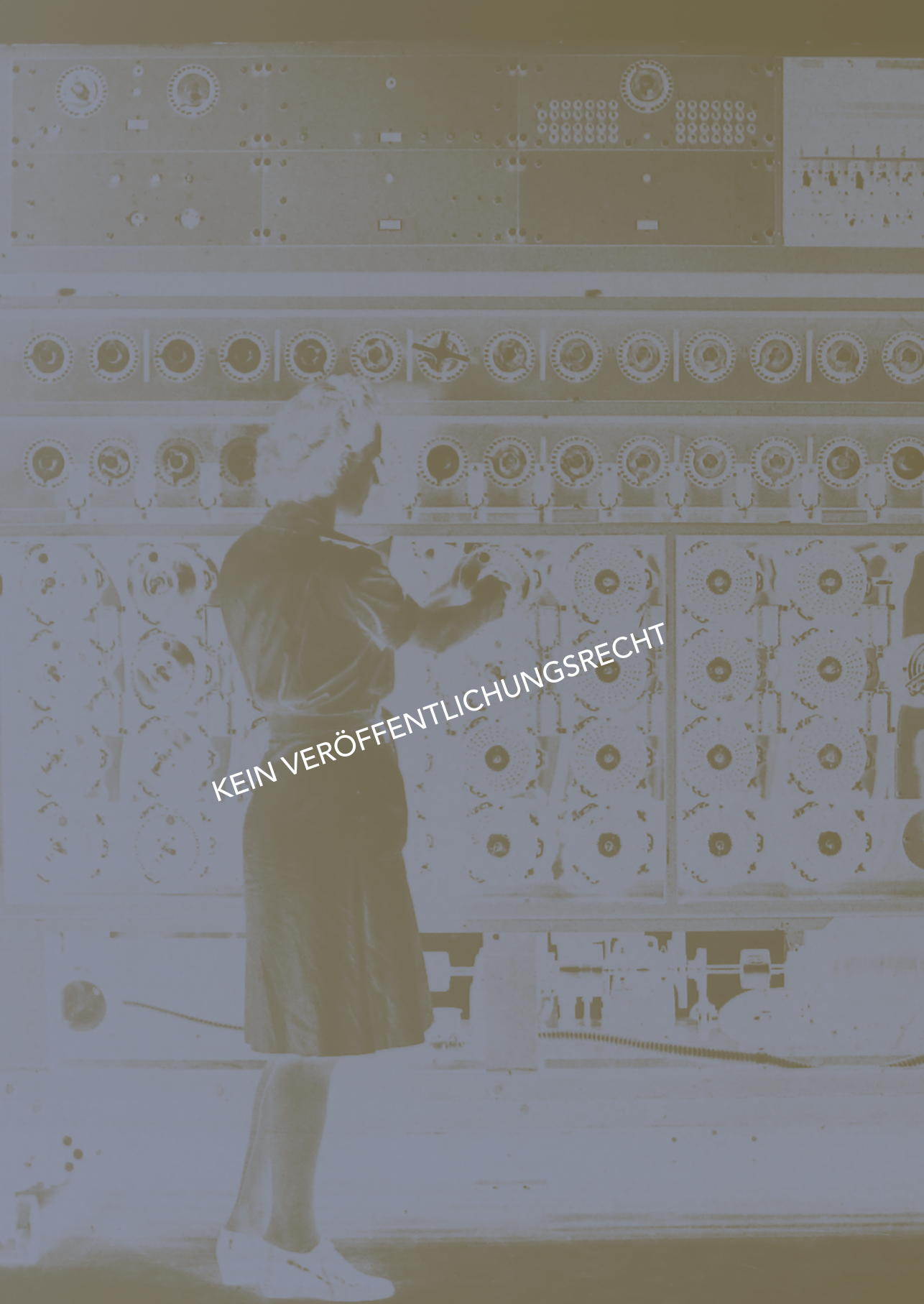


Zuteilungsliste für Kenngruppen
zum K. Buch — M. Dv. Nr. 98.

Teil B.

Schlüsselkenngruppe	Verfahrenkenngruppe	
	Schlüssel M	R. H. V.
Spalte	Spalte	Spalte
1—20 M Potsdam (M Ptd)	1—733 Allgemein	1—290 Offizier
21—60 M Freya (MF)		291—733 Allgeme
61—90 M Aegir (MA)		
91—110 M Hydra (MH)		
111—140 M Aegir (MA)		
141—160 M Sleipnir (M Sleip)		
161—200 M Hydra (MH)		
201—250 R. H. V.		
251—320 M Triton (M Tri)		
321—360 M Meduſa (M Med)		
361—410 M Hydra (MH)		
411—440 M Potsdam (M Ptd)		
441—490 Schiffsſonderſchlüſſel*)		
491—530 M Hydra (MH)		
531—560 M Neptun (M Nep)		
561—620 M Triton (M Tri)		
621—653 M Thetis (M Tht)		
654—693		
—733		
Füllbuchſtabe der Schlüſſelkenngruppe 1. Stelle	Füllbuchſtabe der Verfahrenkenngruppe 4. Stelle	

37 *Die Zahl an Schlüsselkreisen nimmt zu und damit die Zahl an Schlüsseln, die gebrochen werden müssen*



Mit Highspeed-Bombes gegen Shark

Nach dem deutschen Überfall auf die Sowjetunion gilt es im Seekrieg neben der Atlantikroute auch die Arktikroute zu sichern, über die zunehmend Panzer, Flugzeuge und Waffen von Nordamerika in die sowjetischen Häfen Murmansk und Archangelsk transportiert werden. Die großzügige Unterstützung der Sowjetunion durch Briten und Amerikaner soll Hitlers Wehrmacht an der Ostfront binden und durch einen Zweifrontenkrieg schwächen, damit mittelfristig eine Landung in Westeuropa möglich wird. Seitens der deutschen Kriegsmarine sucht man dies möglichst zu verhindern, weshalb es auch in diesen Gewässern zu erbitterten Gefechten kommt. Im März 1942 kann ein in Richtung Sowjetunion laufender Schiffskonvoi noch rechtzeitig umgeleitet und vor einem Angriff des gefürchteten deutschen Schlachtschiffs Tirpitz bewahrt werden. Einige Monate später endet ein ähnliches Ereignis in einem Desaster.

Am Anfang steht eine Warnung des britischen Marine-Attachés in Stockholm an die Admiralität in London, wonach die in Norwegen stehende Tirpitz samt Begleitschiffen einen aus Reykjavik in Richtung Archangelsk auslaufenden Konvoi angreifen könnte. Tatsächlich wird der Konvoi, der Ende Juni 1942 Island verlässt, vom deutschen Beobachtungsdienst erfasst und Tage später auch von einem Flugzeug gesichtet. Daraufhin werden U-Boote zusammengezogen.

In London erkennt man, dass deutsche U-Boote den Konvoi verfolgen und es scheint nur eine Frage der Zeit, bis auch die großen Kriegsschiffe, allen voran die Tirpitz, am Schauplatz auftauchen würden; zumal Aufklärungsfotos und aufgefangene Funksprüche belegen, dass die Tirpitz ihren Ankerplatz im norwegischen Trondheim verlassen hat. Angesichts der Möglichkeit eines bevorstehenden Angriffs entscheidet der britische Admiral Dudley Pound den Konvoi aufzulösen; jedes der Frachtschiffe solle aus eigener Kraft versuchen, einen sowjetischen Hafen zu erreichen. Die Kriegsschiffe, die als Begleitschutz fungieren, werden zurückgezogen, um sie vor der sicher scheinenden Versenkung zu bewahren. Die Folge ist eine heillose Flucht der Frachter, die die meisten geradewegs ins Verderben

38 *Für die amerikanische High-Speed-Bombe ist Shark bald kein Gegner mehr*

39 *Das deutsche Schlachtschiff Tirpitz*

führt. Im Laufe der nächsten Tage sinken mehr als zwei Drittel der ursprünglich 37 Schiffe, versenkt durch deutsche U-Boote; nur ein kleiner Teil erreicht Murmansk. Bittere Ironie der Geschichte: Die gefürchtete Tirpitz und ihre Begleitschiffe kommen gar nicht zum Einsatz.
Das erste Halbjahr 1942 erweist sich für die Alliierten als äußerst verlustreich. Monat für Monat sinken bis zu 100 Schiffe. Das Operational Intelligence Centre drängt die Verantwortlichen von Bletchley Park, den Kampf gegen den neuen U-Boot-Schlüssel Shark zu forcieren, nachdem durch eine Niederlage am Atlantik der Krieg insgesamt verloren zu gehen drohe. In dieser bedrängten Situation beteiligen die Briten die bislang auf Distanz gehaltenen US-Amerikaner, die mittlerweile auf der Seite der Alliierten in den Krieg eingetreten sind. Schließlich ist ein Großteil der versenkten Frachtschiffe amerikanischer Herkunft. Alan Turing reist über den Atlantik, um die Form der künftigen Zusammenarbeit zu klären. Im Gegenzug werden zwei Offiziere der US Navy Hut Eight in Bletchley Park zugeteilt. Außerdem bekommt die amerikanische Seite, was sie seit Langem fordert: Konstruktions- und Schaltpläne der Bombes. Die US Army beginnt mit der Planung neuartiger Modelle, die Umschaltrelais anstelle von Walzen verwenden, um eine deutlich höhere Verarbeitungsgeschwindigkeit zu erzielen. Sie sind für den Einsatz gegen die dreiwalzigen Enigmas gedacht. Gleichzeitig plant die US Navy noch schnellere Hochgeschwindigkeits-Bombes, die mit Vakuumröhren anstelle der Relais arbeiten und die vierwalzigen Enigmas ins Visier nehmen sollen.

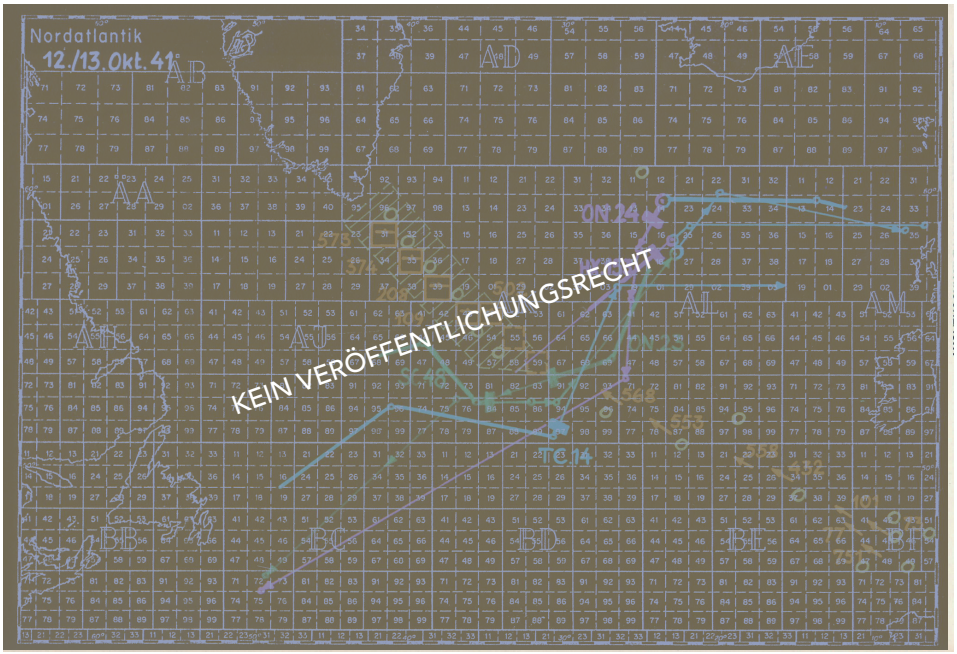
Die Briten sind auf die amerikanischen Ressourcen angewiesen. Man geht für die nahe Zukunft von einem Bedarf an deutlich über hundert Dreiwalzen-Bombes für den deutschen Heeres- und Luftwaffenfunkverkehr sowie noch mehr schnellen Vierwalzen-Bombes für den Funkverkehr der deutschen U-Boote aus, während aus eigener Produktion bislang jedoch noch keine 50 Bombes insgesamt in Betrieb gegangen sind. Hinsichtlich der Enigma M4 wird mit den Amerikanern überdies ein uneingeschränkter Wissensaustausch vereinbart und bezüglich des gemeinsamen atlantischen Kriegsschauplatzes eine enge Zusammenarbeit, die die Beobachtung deutscher U-Boote sowie Sicherung der Schiffskonvois beinhaltet. Derart gut gerüstet, nimmt man einen neuen Anlauf im Kampf gegen Shark.
Es ist aber wieder die Aufbringung eines deutschen U-Boots, die den Durchbruch bringt. Im Oktober 1942 wird U 559 durch Wasserbomben eines britischen Kriegsschiffs schwer beschädigt. Das Boot muss auftauchen, die Besatzung geht von Bord, danach beginnt es langsam zu sinken. Trotzdem versuchen britische Seeleute, daraus noch geheime Unterlagen zu bergen. Es ist ein höchst riskantes Unterfangen, bei dem zwei von ihnen ums Leben kommen. Was im Zuge dieser Aktion aber zutage gefördert wird, ist mehr als bedeutsam. Eines der Beutedokumente ist das aktuelle Wetterkurzschlüsselbuch, aus dem sich wieder Cribs für die Bombes gewinnen lassen. Darüber hinaus geht aus den Unterlagen hervor, dass deutsche U-Boot-Funker beim Senden von Kurzsignalen die vierte Walze in der neutralen Stellung *A* mit Ringstellung *Z* zu belassen haben, die Vierwalzen-Enigma also im Modus einer dreiwalzigen benutzen müssen, um auch Boote, Schiffe und vor allem Landfunkstationen, die nur über dreiwalzige Maschinen verfügen, zu erreichen.
Drei Wochen nach dem Eintreffen des brisanten Materials können die Kryptologen von Hut Eight mithilfe der neu gewonnenen Cribs auf ihren Dreiwalzen-Bombes Schlüssel brechen, Wetterfunksprüche entziffern und dabei die Positionen der funkenden U-Boote offenlegen. In weiterer Folge werden zahlreiche aktuelle Sprüche entziffert und man benötigt dafür oft nur mehr Stunden statt Tage. Shark beginnt seinen Schrecken zu verlieren. Die lange Phase der Ungewissheit scheint vorüber.

Der deutsche U-Boot-Oberbefehlshaber Dönitz befindet sich zu dieser Zeit in einer komfortablen Lage. Er verfügt mittlerweile über rund hundert U-Boote in der Region, was ihm gute Chancen einräumt, Konvois auf See aufzuspüren. Außerdem kann er die Atlantikkarte in seinem Lagezimmer seit geraumer Zeit ziemlich aktuell halten, nachdem sein Beobachtungsdienst Einblick in die *„Naval Cipher Number 3“* hat, den Chiffrierschlüssel,

40 *Offiziere halten auf der Brücke eines Kriegsschiffs Ausschau nach feindlichen U-Booten*

den die britische, die amerikanische und die kanadische Marine zur Geleitzugskoordination verwenden. Dadurch ist er in der Lage, auf Ausweichbewegungen der Schiffskonvois zu reagieren und seine Boote umzudirigieren. Da sein Beobachtungsdienst sogar den U-Boot-Lagebericht entziffert, den die Admiralität aus dem Londoner Submarine Tracking Room regelmäßig an ihre auf See befindlichen Kriegsschiffe und an die Kommandanten der Geleitzüge funken lässt, weiß er nicht nur, wo die gegnerischen Schiffe unterwegs sind, sondern auch, wo die britische Admiralität seine U-Boote vermutet. Dadurch kann er den taktischen Zügen seines Gegners frühzeitig begegnen. Allerdings werfen die britischen Funksprüche mit den Positionen seiner U-Boote einmal mehr die Frage auf, ob dieses Wissen auf Funkpeilung zurückgeführt werden kann, ob Verrat im Spiel ist, oder ob man davon ausgehen muss, dass die Briten Enigma-Funksprüche mitlesen?
Vor diesem Hintergrund gibt Dönitz Ende Jänner 1943 einen Stichwort-Befehl aus, um den U-Boot-Funkverkehr kurzfristig abzusichern. Gleichzeitig lässt er wieder die Sicherheit überprüfen. Dazu wird die von den Briten erstellte U-Boot-Lage mit einer nach eigenen Angaben gezeichneten verglichen, um zu sehen, wie groß die Übereinstimmungen sind. Am Ende

schließt der deutsche Marinenachrichtendienst aus diversen Fehlannahmen im britischen Lagebild, dass der Funkverkehr deutscher U-Boote in London nicht mitgelesen werde. Man hält eine Kompromittierung der Enigma für äußerst unwahrscheinlich. Es ist die fatale Selbsttäuschung, derer man sich immer wieder hingibt: Würden die Briten deutschen Funk mitlesen, wären sie wohl auch darüber informiert, dass die deutsche Seite ihren Funk mitliest; und in diesem Fall würden sie ihre Schlüsselverfahren geändert haben, was bislang nicht geschehen sei...
Trotzdem muss Dönitz erkennen, dass das *„Schachspiel"* mit dem Gegner auf der Atlantikkarte, das bislang passabel funktioniert hat, merklich schwieriger wird. Das liegt daran, dass die Briten nach ihrem Einbruch in den U-Bootschlüssel Shark nun entgegen aller Annahmen sehr wohl seinen Funkverkehr belauschen und sich ihrerseits bemühen, seinen Zügen zuvorzukommen. Es entsteht eine Pattsituation: Obwohl Dönitz Informationen über die Fahrpläne der Konvois erhält, gehen seine U-Boote oft leer aus, da die von der britischen Marineführung gewarnten Konvois sie umschiffen.
Nachdem der Beobachtungsdienst Ende Januar Kursanweisungen für einen Konvoi entziffert hat, lässt Dönitz Anfang Februar 1943 eine sich über hunderte Meilen erstreckende Sperrkette aus U-Booten bilden. Bei solchen Sperrketten beziehen die Boote in einem bestimmten Abstand zueinander quer zur Route des Konvois Position, um ihre Opfer wie in einem aufgespannten Treibnetz zu erwarten. Eines der U-Boote sichtet des Nachts den Konvoi und funkt die Sichtungsmeldung an die U-Boot-Führung. Dönitz formiert daraufhin aus der Ferne ein Rudel aus zwanzig U-Booten, die er an den Konvoi herandirigiert. Am Schauplatz angekommen, entwickelt sich ein tagelanger Kampf, an dessen Ende dreizehn Schiffe des Konvois, aber auch drei U-Boote gesunken sind.
Wenig später setzt Dönitz einen weiteren U-Boot-Streifen an, um einen ausgemachten Konvoi zu erwarten. Sechsunddreißig Stunden später ist sein Einsatzbefehl in Bletchley Park entziffert und der gefährdete Konvoi erhält einen Umleitungsbefehl. Dasselbe passiert mit einem anderen Konvoi, der vom Beobachtungsdienst identifiziert und von herangeführten U-Booten erwartet wird. Auch dieser Befehl wird in Bletchley Park entziffert, wieder werden Schiffe umgeleitet. Kurz danach meldet der Beobachtungsdienst neuerlich die Position eines Konvois, auf den Dönitz zwei U-Boot-Streifen ansetzt. Am nächsten Tag ist auch dieser Befehl entziffert und der bedrohte Konvoi gewarnt. Aber noch am gleichen Tag liefert der Beobachtungsdienst eine Position dieses Konvois, aus der man auf seinen aktuellen Kurs schließen kann. Die beiden angesetzten U-Boot-Gruppen werden in die vermutete Richtung dirigiert, und obwohl auch diese



41 *U-Boot-Aufstellung auf einer deutschen Planquadratkarte des Nordatlantiks*

Befehle bereits am nächsten Tag entziffert vorliegen, ist es für ein Ausweichmanöver zu spät. Der Konvoi wird von einem der U-Boote entdeckt und es folgt eine sechstägige Schlacht, im Zuge derer fünfzehn Schiffe und zwei U-Boote sinken.

Entgegen dem ersten Anschein sind Erfolge wie diese für Dönitz jedoch Pyrrhussiege. Obgleich hoch, bleibt die Versenkungsrate unter den Erwartungen und die Verluste liegen deutlich darüber. Allein im Februar verliert er fünfzehn U-Boote.

Einen kurzzeitigen Befreiungsschlag bedeutet die Einführung neuer Doppelbuchstabentauschtafeln im März 1943. In Bletchley Park kann dadurch die Banbury-Methode bis auf weiteres nicht mehr angewendet werden, was bedeutet, wieder alle möglichen Walzenlagen auf den verfügbaren Bombes durchrattern zu müssen. Darüber hinaus sehen sich die Briten auch der dringend benötigten Cribs beraubt, da auch ein neues Wetterkurzsignalbuch in Kraft tritt. Die Lage wird wieder äußerst kritisch. Man setzt die Admiralität davon in Kenntnis, möglicherweise wieder für Monate im Dunkeln zu tappen.

Gleichzeitig spielt sich am Atlantik eine erbarmungslose Schlacht ab. Vierzig deutsche U-Boote versenken in diesen Tagen mehr als zwanzig Han-

delsschiffe, bei nur einem einzigen U-Boot-Verlust. Dönitz triumphiert und die britische Admiralität sieht ihn seinem Ziel nahe, die Versorgungslinien zwischen Nordamerika und Großbritannien zu kappen.
Unter Nutzung aller verfügbaren Bombes und dank glücklicher Umstände gelingt es den Kryptologen in Hut Eight dann aber wider Erwarten innerhalb weniger Tage, die Katastrophe abzuwenden. Nach der Erbeutung entsprechender Unterlagen lassen sich die dringend benötigten Cribs anstatt aus Wetterkurzsignalen aus Kurzsignalen für Konvoisichtungen ableiten. Da auch diese im Dreiwalzen-Modus verschlüsselt werden, kann man erneut in Shark einbrechen und die Operationen der deutschen U-Boote wieder verfolgen.

Von entscheidender Bedeutung für die Wende im Kriegsverlauf ist zweifellos der Kriegseintritt der Vereinigten Staaten von Amerika. Es entsteht ein den gesamten Atlantik überziehendes Überwachungs- und Sicherungsnetz. Der zunehmende Einsatz von Flugzeugträgern und Langstreckenflugzeugen schränkt den Bewegungsraum deutscher U-Boote ein. Leistungsstarke Ortungsgeräte und modernste Torpedos erleichtern ihre Bekämpfung, zumal die Shark-Entzifferungen ihre Aufstellungen verraten. Mittlerweile arbeitet in Washington ein eigenes kryptologisches Zentrum der US Navy namens *„OP-20-G“*, das in engem Kontakt zu Bletchley Park steht und nach britischem Vorbild auch über einen Submarine Tracking Room, genannt *„Atlantic Section“*, verfügt.
Die Schiffsverluste der Alliierten gehen zurück, während gleichzeitig die Zahl versenkter U-Boote steigt. Aus den Jägern werden Gejagte. Entzifferte deutsche Funksprüche lassen erkennen, dass sich unter den U-Boot-Kommandanten Zweifel daran ausbreiten, am Atlantik weiterhin bestehen zu können. Gleichzeitig wird offenbar, dass Dönitz auf Einwände seiner Kapitäne mit brutalen Drohungen reagiert: Wer der Ansicht sei, Angriffe auf Konvois seien nicht mehr möglich, sei ein Schwächling und kein wahrer U-Boot-Kommandant!
Doch die Realität fordert ihren Tribut. Nachdem im Mai 1943 über 40 deutsche U-Boote versenkt werden, wobei 2.000 Besatzungsmitglieder ums Leben kommen, muss Dönitz die verbliebenen Boote aus der Atlantikregion zurückziehen. Er fragt sich zum wiederholten Male, ob die Alliierten den U-Boot-Funk mitlesen können. Die Antwort, die er von der zuständigen Marinedienststelle erhält, lautet wieder: *„Nein!“* Weder die Entzifferung des alliierten Funkverkehrs noch die Überprüfung der eigenen Verschlüsselungsverfahren hätten Anzeichen dafür erbracht. Zwar ist bekannt, dass die Alliierten im Besitz von mindestens einer Enigma samt den zugehörigen Schlüsselmaterialien sind, doch gibt man sich nach wie

42 *Bombardierung aufgetauchter deutscher U-Boote*

vor überzeugt, dass ihnen diese Beute nur während der Geltungsdauer besagter Schlüssel helfen würde.
Im Juni 1943 muss Dönitz einen weiteren Rückschlag hinnehmen – die völlige Umstellung des britischen Schlüsselsystems auf die neue *„Cypher No. 5"*. Nun tappt sein Beobachtungsdienst im Dunkeln, seine U-Boote verlieren vollends ihre Ziele aus den Augen, während sie selbst immer deutlicher ins Visier geraten. Die Bilanz der Sommermonate 1943 weist gegenüber 58 versenkten Frachtschiffen 74 versenkte U-Boote aus. Darüber hinaus scheinen die Angriffe der Alliierten immer zielgenauer zu erfolgen. Zwischen Juni und August versenken Flugzeuge von US-Flugzeugträgern eine Reihe deutscher Versorgungs-U-Boote, deren Aufgabe darin besteht, U-Boote in entlegenen Seegebieten aufzutanken und mit Munition und Lebensmitteln zu versorgen, um ihren Operationsradius zu erweitern. Kenneth Knowles, der Leiter des amerikanischen Tracking

Rooms, drängt seit geraumer Zeit darauf, sich entzifferter Funksprüche zu bedienen, um gezielt die deutschen Versorgungsboote zu bekämpfen, in denen er eine Schwachstelle der deutschen U-Boot-Waffe erkennt.
Dönitz ist nicht ganz ahnungslos. Laut einer Meldung eines Agenten bei der US Navy sei der Funkverkehr seiner U-Boote während der vergangenen Monate mitgelesen worden. Während die zuständigen Stellen der deutschen Kriegsmarine Derartiges nach wie vor für ausgeschlossen halten, sieht er sich in seinem Verdacht bestätigt. Denn während von den zwanzig Versorgungstreffen auf See im Juni und Juli dreizehn störungslos verlaufen sind, wurden sämtliche zehn Treffen zwischen dem 3. und 11. August gestört. Irgendwann zwischen dem 23. Juli, der Ausgabe eines neuen Stichworts, und dem 11. August, dem Datum seiner Ersetzung, müsse ein Einbruch in den aktuellen Schlüssel erfolgt sein.
Als unmittelbare Gegenmaßnahme lässt er die Art der Positionsübermittlung ändern. Um die möglicherweise enttarnten Planquadrate nicht mehr benutzen zu müssen, erhalten die Kommandanten auslaufender U-Boote versiegelte Umschläge ausgehändigt, die ausgewählte geografische Bezugspunkte mit willkürlichen Namen enthalten. Die U-Boote sollen fortan ihre Standorte durch Angabe von Entfernung und Richtung in Relation zu diesen Punkten übermitteln. Damit lässt sich das Problem jedoch nicht lösen.

Abgesehen von der Aufrüstung des kryptologischen Arsenals, die die Alliierten konsequent betreiben, sind es schwere Fehler seitens der deutschen U-Boot-Führung selbst, die den Niedergang herbeiführen. So lässt sie Befehle und Informationen allgemeiner Natur etwa zu an Bord befindlichen Dokumenten, neuen Waffensystemen der Alliierten oder speziellen Erfahrungen einzelner U-Boote in der Art von Rundbriefen in unterschiedlichen Schlüsselkreisen versenden. Solche Sprüche ergehen im Vierwalzenschlüssel Shark an U-Boote im Atlantik und werden in verschiedenen Dreiwalzenschlüsseln weitergesendet – für U-Boote in der Arktis, in der Baltischen See oder im Mittelmeer. Diese fahrlässige Praxis des Funkens wortgleicher Botschaften mit unterschiedlichen Schlüsseln – in Bletchley Park *„Reenciphering"* oder *„Reencoding"* genannt – verschafft den Briten eine verlässliche Einbruchsmethode. Sie können die Dreiwalzenschlüssel mit ihren herkömmlichen Bombes knacken und aus den entzifferten Sprüchen die nötigen Cribs zum Brechen der Vierwalzenschlüssel auf ihren ersten beiden Vierwalzen-Bombes gewinnen.
Bletchley Park verfügt mittlerweile über gut geschultes Personal, ausgefeilte Methoden und hochspezielles Gerät und damit über eine strategische Überlegenheit, die so manchen Fortschritt auf deutscher Seite umgehend

neutralisiert. Als die Deutschen mit 1. Juli 1943 für die Enigma M4 eine zusätzliche Umkehrwalze *C* samt einer neuen schmalen vierten Walze *Gamma* in Verwendung bringen, gelingt es den Briten durch Reenciphering innerhalb weniger Wochen die Verdrahtung der neuen Walzen zu rekonstruieren und damit wieder in Shark einzubrechen. Und der kryptografische Mehrwert, der darin liegt, dass die Walzen *B* und *Beta* sowie *C* und *Gamma* auch wechselweise miteinander kombiniert werden können, ist dahin, als die Briten erkennen, dass die deutsche Seite die vierte Walze immer einen ganzen Monat lang in Betrieb lässt. Gelingt es, in den aktuellen Schlüssel einzubrechen, haben sie für den Rest des Monats vergleichsweise leichtes Spiel.

Gewisse Probleme bereitet Hut Eight der phasenweise Rückzug der U-Boote aus dem Nordatlantik, denn mit den Booten verschwinden die gefunkten Kurzsignale, die die Cribs liefern. Man versucht deshalb gelegentlich, Cribs selbst zu erzeugen, etwa, indem man ein Flugzeug beordert, an einem bestimmten Ort vor der gegnerischen Küste Seeminen zu legen. Hinter dieser Methode, die *„Gardening"* genannt wird, steht die Erwartung, dass in dem deutschen Funkspruch, der dieses Geschehnis der vorgesetzten Dienststelle meldet, das Wort *„Seemine"* vorkommt. Fängt man besagten Funkspruch auf, verfügt man über ein Crib.

Derartige Tricks werden indes verzichtbar, als man entdeckt, dass eine deutsche Wetterstation in der Bucht von Biskaya an den Anfang ihrer regelmäßigen Funksprüche stereotyp die Phrase *„Wetter Vorhersage Biskaya"* setzt und damit Tag für Tag und über Monate hinweg ein ideales Crib liefert.

Die Entzifferungserfolge basieren natürlich auch darauf, dass die Briten mittlerweile über Dutzende Bombes verfügen, was die Lösung der gestellten Aufgaben, verglichen mit früheren Phasen des Krieges, deutlich erleichtert. Man hat eine umfassende Maschinerie zur Verfügung, wenngleich die wertvollen Maschinen nicht mehr in Bletchley Park arbeiten. Um das Risiko der Zerstörung durch deutsche Luftangriffe zu minimieren, sind sie samt den hunderten Frauen vom Women´s Royal Navy Service, die zu ihrer Bedienung nötig sind, in diversen Orten in der Umgebung wie Stanmore, Eastcote oder Gayhurst untergebracht worden. Zu Bletchley Park wird über Telefon- und Telegrafenverbindungen Kontakt gehalten.

Was die Bombe-Kapazitäten angeht, bietet vor allem auch die Entwicklung in den USA Grund zur Zuversicht. Mittlerweile sind die ersten beiden Hochgeschwindigkeits-Bombes, die die Namen *„Adam"* und *„Eve"* tragen, in Betrieb gegangen. Sie bestehen jeweils aus 400 Vakuumröhren, 16 Walzensätzen mit 64 verdrahteten Bakelitwalzen und

43 *Verfolgung deutscher U-Boote in einem amerikanischen Tracking Room*

einer Unmenge an Drähten. Die hohe Betriebstemperatur, die bei 2.000 Umdrehungen pro Minute entsteht, führt anfangs noch zu Verformungen der großen Walzen und zu schlecht schließenden Kontakten. Nach der Beseitigung solcher Anlaufschwierigkeiten arbeiten *„Adam"* und *„Eve"* jedoch anstandslos.

Mit anlaufender Serienproduktion nimmt in Washington eine erste Tranche von zehn Hochgeschwindigkeits-Bombes den Betrieb auf und stetig kommen neue hinzu. Ende 1943 sind es bereits 75. Sie laufen rund um die Uhr, bedient im Schichtbetrieb von Frauen, die dem *„Women Appointed for Volunteer Emergency Service"* angehören und kurz *„WAVES"*genannt werden.

Vor diesem Hintergrund wird die Analyse von Shark-Schlüsseln zur Gänze nach Washington verlegt. Ein in England aufgefangener Funkspruch wird zwar weiterhin in Bletchley Park aufbereitet, weil man hier auf Jahre an Erfahrung zurückblicken kann. Danach werden die Chiffren samt den zuge-

hörigen Suchmenüs aber per Telegraf zum Entschlüsseln über den Atlantik gesandt. Aus gutem Grund. Die amerikanische Vierwalzenbombe arbeitet zwanzig Mal schneller als die britische und verspricht nahezu jede Aufgabenstellung zeitgerecht zu lösen. Ein Durchlauf durch eine Walzenlage einer Enigma M4 mit durchschnittlich vier Stopps dauert nicht länger als 15 bis 20 Minuten. Damit ist Shark kein ernstzunehmender Gegner mehr. Ab Anfang 1944 kann in Washington und London fast der gesamte Funkverkehr der deutschen Kriegsmarine mitgelesen werden. Man kontrolliert so gut wie alle Marineschlüssel. Mitunter sind die Standorte deutscher U-Boote den Befehlshabern der Alliierten eher bekannt als den deutschen, was oft deren Schicksal besiegelt. In den ersten drei Monaten des Jahres 1944 gehen 36 U-Boote verloren, während im gleichen Zeitraum nur drei von 3.300 Schiffen aus den Konvois der Alliierten versenkt werden.
Nach einer Reihe weiterer Versenkungen deutscher Versorgungsschiffe im März 1944 lässt Dönitz erneut die Schlüsselsicherheit überprüfen und das Verfahren verschärfen. Zur Absicherung der ihm noch verbliebenen Versorgungsboote lässt er an die Kommandanten von U-Booten bezüglich ihres Treffpunkts zum Nachtanken funken, dass sie demnächst einen Offiziersfunkspruch samt dem Stichwort *„Maske"* erhalten würden, der nach nur ihnen bekannten Kriterien verschlüsselt sei. Einer der U-Boot-Kommandanten etwa hat zur Entschlüsselung dieses Texts einen neuen Spruchschlüssel aus den Initialen der Vornamen seines Sanitätsoffiziers, seines Zweiten Offiziers und seines Steuermanns sowie aus dem ersten Buchstaben des Nachnamens des Sanitätsoffiziers zu bilden. Um zu Steckerverbindungen zu kommen, sollen die des ursprünglichen Offiziersschlüssels mit der Hausnummer eines bestimmten Matrosen addiert werden. Erst dann offenbart die Enigma den vorgesehenen Treffpunkt mit dem Versorgungsboot. Ähnliche Anweisungen erhalten andere U-Boot-Kommandanten.
Es ist ein Versuch, den Kreis der Mitwisser einzuschränken, um jedwede Art von Spionage – wohl nicht zuletzt in den eigenen Reihen – auszuschließen. Eine Erhöhung der Schlüsselsicherheit gegenüber den Alliierten lässt sich durch das Verkomplizieren des Additionsmodus aber kaum erzielen. Schließlich suchen die schnellen Bombes nicht mehr nach gefinkelten Schlüsseln, sondern attackieren die Enigma in ihrer vollen Breite. Sie haben genug Verarbeitungskapazität, um sämtliche Stellungen in kürzester Zeit zu prüfen. Die Buchstabenrätsel, die zur Aufwertung der Schlüssel ersonnen werden, erzeugen in Bletchley Park und Washington insofern nur wenig Irritation. Schon bald liegen alle neuen Einstellungen vor und weitere deutsche U-Boote werden versenkt.
Die Zeit der großen kryptologischen Herausforderungen ist vorüber; jetzt geht es um die rasche Verarbeitung großer Datenmengen. Am Horizont

zieht das Computerzeitalter auf, in dem die Enigma zur Technologie einer vergangenen Ära verblasst.

Unter den gegebenen Umständen stehen die Erfolgsaussichten der geplanten Landung der Alliierten in Frankreich gut. Auf See droht vergleichsweise geringe Gefahr, nachdem die Erkenntnisse aus Hut Eight den Londoner Submarine Tracking Room in die Lage versetzen, die deutschen U-Boote, die an verschiedenen Orten lauern, zu überwachen und bei Bedarf geradezu zu verfolgen. Außerdem legen die stetigen Entzifferungen offen, wie Dönitz eine allfällige Invasionsflotte zu bekämpfen gedenkt. Aber auch für die zu erwartenden Kämpfe an Land sind Vorbereitungen getroffen. Die US Army unterhält eine eigene Einheit in Bletchley Park, deren Angehörige in Hut Three und in Hut Six arbeiten. Die Einheit ist im Umgang mit Enigma-Entschlüsselung geschult und mit Bombes ausgerüstet und betreibt auch eine eigene Abhörstation. Geleitet wird sie von dem Militärgeheimdienstmann Telford Taylor, der als Verbindungsoffizier und Angehöriger der *„US Army Intelligence Special Branch"* seit geraumer Zeit in England tätig ist. Taylors Aufgabe ist es, die wichtigsten Erkenntnisse aus der Entzifferung der Heeres- und Luftwaffen-Enigma unter Wahrung der gebotenen Geheimhaltung zum Sitz der Special Branch nach Washington und zu den US-amerikanischen Befehlshabern am europäischen Kriegsschauplatz zu übermitteln.
Dank der Entzifferung der Enigma (sowie manch anderer deutscher Chiffriermaschinen) verfügen Briten und Amerikaner über unschätzbar wertvolle Informationen. So etwa hilft Bletchley Park maßgeblich bei der Entscheidung, wo an der französischen Küste die Landeoperation vor sich gehen soll. Für die Alliierten wäre es einfacher, in der Gegend von Calais zu landen, wo die Meerenge am schmalsten ist und es entsprechend leichter fiele, die Landungstruppen gegen deutsche Angriffe zu verteidigen. Außerdem wäre man dem Zielgebiet Deutschland näher als bei anderen in Frage kommenden Plätzen weiter im Süden. Dagegen spricht, dass die deutsche Seite die Landung an eben dieser Stelle erwartet. Aus dem entzifferten Funkverkehr weiß man, dass der deutsche Oberbefehlshaber an der Kanalküste wie auch Hitler selbst dieser Meinung sind. Deswegen disponiert man um. Die Landung soll in der Normandie erfolgen. Die ist zwar deutlich weiter entfernt vom eigentlichen Ziel, doch kommen ihr strategische Vorteile zu, sofern es gelingt, die Deutschen in dem Glauben zu wiegen, der Hauptstoß des Landeunternehmens würde bei Calais erfolgen. Im Zuge der Vorbereitungen laufen deshalb Täuschungsmanöver an, die diesen Irrglauben an Calais erhärten sollen. Man bedient sich deutscher Agenten, die Bletchley Park enttarnt hat und nun unter

44 *Landetruppen der Alliierten in der Normandie*

Androhung ihrer Hinrichtung ihren ursprünglichen Auftraggebern in Deutschland über Funk gezinkte Informationen liefern. Der deutschen Führung wird vorgegaukelt, dass im Südosten Englands ein großer amerikanischer Truppenverband aufgestellt werde für eine Landung bei Calais. Damit das Ganze möglichst echt aussieht, werden vor Ort aufblasbare Attrappen von Panzern und Landungsbooten für die Kameras deutscher Aufklärungsflugzeuge drapiert. Ausgemusterte Soldaten spielen die Besatzungen, hervorragende Persönlichkeiten wie die Generäle Eisenhower und Montgomery besuchen Werften, Docks und Schiffe, die gar nicht existieren. Im Äther wird der deutschen Funkaufklärung der Funkverkehr dieser *„Geisterarmee"* offeriert. Bletchley Park spielt dabei eine zentrale Rolle. Da man den Funkverkehr des deutschen Geheimdienstes mitliest, hat man die Möglichkeit, zu verfolgen, wie die deutsche Seite auf die Inszenierung reagiert und wie sie der Täuschung mehr und mehr erliegt. In der Nacht auf den 6. Juni 1944 beginnt der lang vorbereitete Tag der Entscheidung – *„D-Day"*. Die riesige Kriegsmaschinerie der Alliierten

läuft an. Zu Beginn fliegt ein Bomberverband einen Scheinangriff in Richtung Calais. Die Täuschung gelingt. Deutsche Jagdflugzeuge steigen auf und kreisen über Calais, um den Gegner zu erwarten, der nicht kommt. Sie fehlen jetzt in den Gebieten, in denen die Landung tatsächlich erfolgt. Auch Marineeinheiten der Alliierten führen Scheinangriffe durch. Falschinformationen über eine bevorstehende Landung in der Seine-Bucht veranlassen Dönitz, zahlreiche U-Boote dorthin zu beordern. Die echten Landungsvorbereitungen hingegen entgehen der deutschen Funkaufklärung aufgrund einer strikt gehaltenen Funkstille. Diese erfolgen an den Küsten der Normandie, wo kurz nach Mitternacht Fallschirm- und Luftlandetruppen der Alliierten auf französischem Boden niedergehen. Sie sind die Vorhut eines riesigen Unternehmens mit 5.000 Schiffen und Booten aller Größen.

Bletchley Park liefert auch dafür wertvolle Geheiminformationen. Aus einem entzifferten Funkspruch des deutschen *„Oberbefehlshabers West"* geht hervor, dass er die Armee, die bei Calais liegt, nicht aber die in der Normandie in Alarmbereitschaft versetzt. In den frühen Morgenstunden unterrichtet er das Führerhauptquartier über die Ankunft der Fallschirm- und Luftlandetruppen. Hitler gibt sich überzeugt, bei den Aktivitäten in der Normandie handle es sich um ein Ablenkungsmanöver. Gegen 11 Uhr vormittags hält er eine Lagebesprechung ab, in der er ausführt, der richtige Angriff werde bei Calais erfolgen – an der schmalsten Stelle des Ärmelkanals!

Die Informationen aus Bletchley Park ermöglichen den Befehlshabern der Alliierten ihre Planungen an denen ihres Gegners auszurichten. Auch in den folgenden Wochen und Monaten, beim Vormarsch in Richtung Deutschland, liegen ihnen detaillierte Informationen über Aufstellung und Aktivitäten deutscher Armeen vor. Es ist fast so, als hätten sie einen Spion direkt an Hitlers Lagetisch sitzen.

Die deutsche Wehrmacht führt in Frankreich wie in Italien bald nur noch Rückzugsgefechte. Und auch an der Front im Osten gibt es kein Halten mehr. Die Verbände der Roten Armee rücken unaufhaltsam vor, angetrieben von ihren Generälen und Stalins Auftrag, das faschistische Deutschland zu erobern. Demgegenüber geht es für Briten und Amerikaner nicht mehr nur um den Sieg über Hitlerdeutschland, sondern auch darum, den sowjetischen Einflussbereich in Europa nicht zu sehr anwachsen zu lassen. Bletchley Park arbeitet so gesehen auch schon für den Kalten Krieg.

A
S
D
F
G
B
N
X
C
V
P

Das letzte Geheimnis der Enigma

Die schweren Rückschläge nähren auf deutscher Seite seit geraumer Zeit Zweifel an der Schlüsselsicherheit. Ein 1942 in der *„Chiffrierabteilung des Oberkommandos der Wehrmacht"* ins Leben gerufenes Referat zur *„Sicherheit der eigenen Chiffrierverfahren"*, geleitet von dem Mathematiker Karl Stein, führt eine umfassende Überprüfung durch. An deren Ende zieht Stein eine nüchterne Bilanz. Nicht alle zum Einsatz kommenden Verfahren seien sicher, zumal man fehlerfreie Anwendung nicht voraussetzen dürfe. Mit Schlüsselfehlern und Verstößen gegen Vorschriften sei immer zu rechnen. Unterlagen, Vorschriften und Gerätschaften seien nicht dauerhaft geheimzuhalten, könnten dem Gegner durch Erbeutung, Verrat oder Rekonstruktion aus dem chiffrierten Funkverkehr jederzeit zufallen. Man müsse deshalb immer vom schlimmsten Fall ausgehen, wonach der Gegner über eine gute Kenntnis des Schlüsselverfahrens und über Hilfsmittel zu dessen Kompromittierung verfüge. Stein plädiert für eine Art Grundmisstrauen im Gegensatz zum weit verbreiteten Grundvertrauen in die Enigma und ihre Möglichkeiten.

Tatsächlich haben Anwendungsfehler und Nachlässigkeiten deutscher Schlüssler und Funker den Alliierten in den vergangenen Jahren wichtige Ansatzpunkte für ihre Entschlüsselungsmethoden geliefert. Den Verantwortlichen auf deutscher Seite ist es nicht gelungen, die Schwachstellen zu beseitigen. Das hat auch damit zu tun, dass die Organisation des Chiffrierwesens lange Zeit zwischen diversen Behörden und den drei Wehrmachtteilen zersplittert gewesen ist und nicht einmal eine gemeinsame Kontrollinstanz existiert hat. Daneben sind aber auch systemische Fehlleistungen aufgetreten, so etwa der doppelt gesendete Spruchschlüssel oder die Weiterübermittlung desselben Spruchtexts in anderen Schlüsselkreisen sowie vor allem die Wiederholung stereotyper Phrasen und Begriffe über längere Zeiträume hinweg, die den alliierten Kryptologen immer wieder zu Einbrüchen in aktuelle Schlüssel verholfen haben. Verstöße gegen die Schlüsselsicherheit resultieren sowohl aus Kompetenzdefiziten der Schlüssler im Einsatz an den Kriegsschauplätzen, als auch des für die

Schlüsselverfahren zuständigen kryptologischen Personals in den Chiffrierstellen im Hinterland. Es ist bezeichnend, dass es in Deutschland am Ende des Krieges keine vergleichbaren Ausbildungsmöglichkeiten gibt, wie sie die Westalliierten eingerichtet haben. Das deutsche Chiffrierwesen hat sich in den Kriegsjahren zwar erweitert, nicht aber substanziell verbessert, ganz im Gegensatz zu den Institutionen von Briten und Amerikanern, die enorme Fortschritte erzielt haben. Mit ein Grund mag sein, dass sie zivilen Experten verantwortliche Positionen in ihrem Militärapparat zugestanden haben. Was die wenigen versierten Kryptologen in Deutschland betrifft, so sind diese militärischen Behörden nachgeordnet und in viele Entscheidungsprozesse bezüglich der Beschaffung des Geräts nicht eingebunden. Manch einer mag die Schwächen der Enigma längst erkannt, aber nicht die Möglichkeit gehabt haben, sich Gehör zu verschaffen, vielleicht auch nicht den Mut. In einem diktatorischen Herrschaftssystem, in dem Kritik als *„Defätismus"* gebrandmarkt und als Hochverrat geahndet wird, verwundert es nicht, wenn sich Verantwortliche aus Angst vor Konsequenzen scheuen, Fehler und Unzulänglichkeiten in ihren Zuständigkeitsbereichen einzugestehen.

Was das Problem vollends unlösbar macht, ist der Umstand, dass es um grundlegende Unzulänglichkeiten der Enigma geht, die mitten im Krieg kaum zu beseitigen sind: Die rechte Walze bewegt sich regelmäßig und dadurch in berechenbarer Weise. Die mittlere und vor allem die linke Walze bewegen sich hingegen viel zu wenig, um maßgeblichen Einfluss auf die Verschlüsselung zu nehmen. Die Periode scheint insgesamt zu kurz. Die Umkehrwalze erweist sich in ihrer fixen Verdrahtung als zu starr und angreifbar. Dies gilt im Grunde für die Verdrahtungen aller Walzen, die jahrelang unverändert in Verwendung bleiben. Diese Kritikpunkte stellen die Enigma an sich in Frage. Angesichts solcher Erkenntnisse gibt es in den Jahren 1943 und 1944 Überlegungen bezüglich ihrer Ersetzung – zumindest für den Nachrichtenverkehr der höheren Kommanden. Dort soll eine sicherere Verschlüsselungsmaschine namens *„Schlüsselgerät 39"* eingeführt werden, ein Abkömmling der Enigma, dessen Schlüsselwalzen durch separate Antriebswalzen Drehschritte in irregulärer Weise absolvieren. Diese Planungen verlaufen jedoch im Sand – wohl nicht zuletzt wegen des enorm hohen Aufwands eines solchen Austauschs.

1944 konstituiert sich ein *„interministerieller Sonderausschuß zur Überprüfung der Sicherheit der eigenen Geheimschriften"*, beschickt von allen Stellen und Ministerien, die Chiffrierverfahren verwenden. Er formuliert Antworten auf die Frage, ob die Enigma den an sie gestellten Anforderungen noch genüge. Dabei kommen unterschiedliche Einschätzungen für die verschiedenen Modelle zum Ausdruck. Das Modell ohne

Stecker, wie es der Geheimdienst benutzt, genüge zeitgemäßen Sicherheitsansprüchen nicht mehr, weil es mit maschinellen Hilfsmitteln in kurzer Zeit gebrochen werden könne. Eine mechanische Aufrüstung, die dies verhindert, scheint nicht durchführbar. Deshalb sollen Nachrichten fortan vor dem Chiffrieren mit der Maschine mithilfe eines anderen Verfahrens vorchiffriert werden, um die Sicherheit wiederherzustellen. Die Stecker-Enigma des Heeres könne zwar auch gebrochen werden, aber nur mit erheblichem maschinellen Aufwand. Am sichersten erscheint die Marineausführung mit ihrem komplexeren Schlüsselverfahren, obgleich auch sie theoretisch angreifbar sei.
Man hat die Notwendigkeit erkannt, grundlegende Änderungen durchzuführen. Dabei setzt man zunächst auf der Ebene der Schlüssel an. Es treten neue *„Allgemeine Schlüsselregeln für die Wehrmacht"* in Kraft, in die so manche Erfahrung der vergangenen Jahre eingeflossen sind. So solle eine fundierte Ausbildung des Schlüsslerpersonals vermeiden helfen, dass Flüchtigkeitsfehler den Nachrichtenverkehr verzögern oder dem Gegner erlauben, in die Schlüssel einzubrechen. Darüber hinaus gibt es konkrete Anweisungen, die der Vermeidung früherer Fehler gelten. Beim Verfassen von Nachrichten seien Regelmäßigkeiten sowie gleichlautende Redewendungen und Wiederholungen im Text zu vermeiden. Die Nachricht müsse gänzlich neu formuliert werden, wenn sie in unterschiedlichen Schlüsselkreisen versendet werden solle, wenn derselbe Spruch nach einem Fehler neu verschlüsselt werden müsse, aber auch, wenn ein Spruch an einen Empfänger mit einem anderen Schlüssel weiterzuvermitteln sei. Besondere Aufmerksamkeit wird der Geheimhaltung von Schlüsselmaschinen und Unterlagen gewidmet sowie der Überwachung und Einschwörung des Personals samt eindringlichem Verweis auf die bei Verstößen anzuwendenden Gesetze und drohenden Strafen.
Beim Heer tritt eine Regel in Kraft, wonach der Funkverantwortliche aus einem beliebigen Buch einen Text auswählen und ihn auf der Enigma bei Walzenlage *I, II, III* und *Ringstellung 01, 01, 01* bei willkürlichen zehn Steckerverbindungen chiffrieren soll. Die entstehenden Chiffren sind in Sechsergruppen in eine Spruchschlüsselliste einzutragen und nacheinander zu verwenden. Dabei dienen die ersten drei Buchstaben als Grundstellung und die letzten drei als Spruchschlüssel. Solche willkürlich erzeugten Schlüssel sollen Einbruchsversuchen seitens Außenstehender besser widerstehen als frei gewählte, weil sie Häufungen besonderer Buchstabenkombinationen vermeiden.
Für lange Funksprüche werden Unterbrechungen angeordnet. Zwischen dem 70. und dem 130. Buchstaben eines Spruchs ist die linke Walze um eine variable Zahl an Schritten zu verdrehen, bevor der Verschlüsselungs-

prozess fortgeführt werden darf. Damit der Spruch beim Empfänger dann auch vollständig entziffert werden kann, ist der Buchstabe, auf den die Walze dabei gedreht wird, in den Chiffren des Spruchs mitzufunken, und zwar genau an der Stelle, an der der Wechsel stattfindet. Auf diese Weise kann der Empfänger auch die folgenden Chiffren entziffern. Heer und Luftwaffe erhalten zudem Anleitungen zur Bildung von *„Notschlüsseln"* für die Enigma. Aus den Buchstaben ausgegebener Schlüssel- und Kennwörter bzw. ihren Positionen im Alphabet werden ähnlich wie beim Stichwortverfahren die Schlüsseleinstellungen errechnet. Um Verrat vorzubeugen, dürfen dieserart Notschlüssel dem Schlüssler nur mündlich gegeben werden, die Wörter sind auswendig zu lernen und nicht aufzuschreiben.
Angesichts der allgemeinen Lage muss sich auch die um Schlüsselsicherheit besonders besorgte Kriegsmarine mit vergleichsweise leicht realisierbaren Maßnahmen bescheiden. Es werden weitere U-Boot-Schlüssel auf den M4-Standard umgestellt und einzelne U-Boote erhalten individuelle *„Sonderschlüssel"*. Außerdem wird das Kurzsignalverfahren, das für dringende Funksprüche an die Führungsstellen an Land, zur Übermittlung der Feindlage sowie zur Koordination gemeinsamer Operationen mit anderen U-Booten und Kriegsschiffen oder der Übernahme von Nachschub von Versorgungsschiffen dient, komplizierter. Das Kurzsignalheft aus dem Jahr 1944 besteht aus zwei Teilen. Heft I enthält das *„Satzbuch"*, welches zahlreiche geläufige Phrasen aus dem Bereich des Seekrieges auflistet und ihnen vierstellige Zahlen zuweist. Die entsprechenden vierstelligen Zahlen werden dann mit der aktuellen Schlüsselzahl addiert, welche der *„Schlüsselzahlentafel"*, ebenfalls in Heft I, zu entnehmen ist. Im Heft II, dem *„Buchgruppenheft"*, werden den vierstelligen Zahlen vierstellige Buchstabengruppen zugewiesen. Diese werden samt dem Kürzel zur Identifizierung des sendenden Bootes mit dem aktuellen Tagesschlüssel und unter Verwendung des Spruchschlüssels aus dem zugehörigen Kenngruppenheft chiffriert. Gefunkt wird vorneweg die Kenngruppe in Klarbuchstaben, die – zur Sicherheit am Spruchende wiederholt – den Empfänger zum richtigen Spruchschlüssel, der ihr im Kenngruppenhaft fix zugewiesen ist, führt. Damit kann er entziffern, rückrechnen und rücktauschen, bis am Ende wieder die Phrasen vorliegen.
Für die Übermittlung von Kurzsignalen – auch Wetterkurzsignalen – wird ein System namens *„Kurier"* getestet. Dabei wird die händisch bediente Morsetaste durch einen Pulsgenerator ersetzt, der die Morsezeichen in Form schneller elektrischer Impulse abgibt, sodass der gesamte Funkspruch kaum eine halbe Sekunde lang dauert. Das maschinelle Übermittlungsverfahren soll ein Einpeilen durch die Gegenseite völlig unmöglich machen, kommt jedoch nicht mehr zum Einsatz. Es sind wohl vorrangig

46 *Verbesserungen, die zu spät kommen: die Enigma-Uhr...*

produktionstechnische und logistische Schwierigkeiten, die solcherart umfassende Änderungen auf der Ebene der verwendeten Gerätschaft unmöglich machen.

Vereinzelt findet bei der Luftwaffe noch die so genannte *„Enigma-Uhr"* Verwendung. Diese elektrische Schaltvorrichtung wird mithilfe von zwanzig Kabeln gemäß den Steckerverbindungen des Tagesschlüssels mit dem Steckerbrett verbunden. Die Kabel laufen in die Schaltung hinein, welche im Kern aus einem Drehschalter besteht, der die Steckerpaare noch einmal verwürfelt. Er kann in vierzig Drehstellungen gebracht werden, deren jede ein eigenes Verdrahtungsmuster erzeugt. Dem Empfänger muss die verwendete Schalterstellung natürlich als zusätzliches Element des Schlüssels mitgeteilt werden.

47 *… und die Lückenfüllerwalze*

Das Besondere an der Enigma-Uhr ist, dass sie sich der Inversität der Enigma, auf der die meisten Entschlüsselungsmethoden aufbauen, entzieht. Ein *B* kann mit einem *E* gesteckt sein, das *E* aber mit einem anderen Buchstaben. Dies bedeutet die Eliminierung einer alten Schwachstelle. Allerdings gelingt es den Briten schon bald mithilfe eines Reencipherings die Verdrahtung der Enigma-Uhr zu rekonstruieren, und mit den Bombes der neuen Generation können sie solche Schlüssel grundsätzlich brechen, wenngleich erheblich längere Cribs und Laufzeiten nötig sind.
Die Luftwaffe führt zudem eine neue Umkehrwalze *D* ein, deren Verdrahtung beliebig gesteckt werden kann. Die in Bletchley Park *„Uncle D"* genannte Walze bereitet den britischen Kryptologen gewisse Schwierigkeiten. Sie kommt aber auch nicht mehr allgemein zum Einsatz. Darüber hinaus wird eine Schlüsselwalze neuen Typs geprüft, die so genannte *„Lückenfüllerwalze"*, bei der mithilfe von Plastikstöpseln bis zu 26 Überträge an gewünschten Positionen aktiviert werden können. Auch sie wird nicht mehr eingesetzt, obwohl ihre Produktion anläuft.

Nicht einmal bis zur Produktion gelangt eine visionäre Variante der Enigma, das Modell M5, gedacht zur Verwendung für alle Wehrmachtteile. Basierend auf der M4 hätte es mit vier aus zwölf Schlüsselwalzen gearbeitet und damit tausende Walzenlagen ermöglicht. Darüber hinaus hätte es über die neuen Lückenfüllerwalzen mit zahlreichen variablen Überträgen verfügt und über einen irregulären Walzenvortrieb durch separate, unterschiedlich steckbare Antriebsräder des nicht realisierten Schlüsselgeräts 39. Damit wäre die Schwäche des regelmäßigen Schrittwerks der Enigma restlos beseitigt gewesen. Aber die M5 bleibt bloße Vision.
Ungeachtet ihrer Qualität, gilt für alle angedachten Veränderungen, dass sie zu spät kommen, um den Kriegsverlauf zu ändern. Patrick Mahon, der letzte Leiter von Hut Eight, meint rückblickend jedenfalls, es sei ein schwerer Fehler der deutschen Seite gewesen, Verschärfungen ihres Verschlüsselungssystems jeweils nur in Einzelschritten durchzuführen. Dies habe britischen Kryptologen immer wieder die Möglichkeit eröffnet, sie zu überwinden. Hätte man aber beispielsweise die Innovationen des Jahres 1944 frühzeitig und auf einmal umgesetzt, wäre Bletchley Park wohl paralysiert gewesen.

Am 8. Mai 1945 gibt das Oberkommando der Wehrmacht über den Rundfunk bekannt, dass auf allen Kriegsschauplätzen die Kämpfe einzustellen seien. Fortan dürfe nur noch offen – also nur noch unverschlüsselt – gefunkt werden. Viele der in Geheimhaltung geschulten Nachrichtensoldaten verbrennen daraufhin ihre Schlüsselunterlagen, zerstören oder versenken ihre Enigmas im nächsten See oder Sumpf oder vergraben sie irgendwo im Wald. Dem Gegner soll keinerlei Geheimmaterial in die Hände fallen. Demgegenüber ziehen einige Teams einer britisch-amerikanischen Spezialeinheit namens *„Target Intelligence Committee"* durch die befreiten Gebiete, mit dem Auftrag, Funkanlagen, Enigmas und sonstige Schlüsselmaschinen samt den zugehörigen Papieren zu suchen und zu sichern. Im letzten Moment scheitert in Flensburg ein Versuch deutscher Soldaten, geheime Unterlagen der Marine-Funkaufklärung zu vergraben und so dem Zugriff der Sieger zu entziehen. Dadurch fallen den Alliierten Belege für weit reichende Einbrüche des deutschen Beobachtungsdienstes in ihren Funkverkehr in die Hände. Auf einer Burg in Sachsen finden sie deutsche Dechiffrierexperten sowie tonnenweise Geheimunterlagen vor, die kurz vor dem Eintreffen sowjetischer Truppen abtransportiert werden können. Südlich von München sind deutsche Kryptologen in Gefangenschaft geraten, die Maschinen offerieren, mit denen sie angeblich Funkschlüssel der Roten Armee gebrochen haben. Die Maschinen werden samt den Mathematikern verladen und nach England gebracht. Es ist kein Einzel-

fall, dass die Siegermächte Kriegsbeute in Form von Spezialisten aus Hitlers Armee machen, um sie für sich weiterarbeiten zu lassen. Ob es sich dabei um überzeugte Nationalsozialisten handelt oder nicht, ist nicht entscheidend. Für moralische Überlegungen bleibt wenig Raum in diesen Tagen. Der verheerende Zweite Weltkrieg ist kaum zu Ende, steht bereits der Kalte Krieg bevor, die drohende Auseinandersetzung der westlichen Welt mit der mächtigen, nunmehr mitten in Europa stehenden Streitmacht Stalins.

Vor diesem Hintergrund wird die in Bletchley Park entwickelte Geheimwaffe mit dem Codenamen *„Ultra"* nicht außer Dienst gestellt. Man richtet sie zunächst verstärkt gegen den japanischen Funkverkehr, der auf einer Weiterentwicklung der Enigma basiert, und nach der Kapitulation Japans im August 1945 gegen den sowjetischen, zumal die Rote Armee auch erbeutete Enigmas für ihren Funkverkehr einsetzt. Darüber hinaus geben Briten und Amerikaner die eingesammelten Enigmas an andere Staaten weiter (die das vermeintlich sichere Chiffriersystem gerne übernehmen) und können deshalb in der Folge deren geheimen Nachrichtenverkehr bequem mitlesen.

Angesichts dessen wird die Geschichte von Bletchley Park weit über das Kriegsende hinaus als Staatsgeheimnis behandelt. Tausende Mitarbeiterinnen und Mitarbeiter sind per Eid verpflichtet, auch nach ihrer Entlassung ins Zivilleben über das Ultra-Geheimnis Stillschweigen zu bewahren. Sogar gegenüber der eigenen Familie muss verheimlicht werden, womit man während des Krieges beschäftigt war.

Bletchley Park wird zu einem Tabu. Das hat zur Folge, dass sich der Irrglaube von der Unangreifbarkeit der Enigma verfestigen kann. Karl Dönitz, der bei den Nürnberger Kriegsverbrecherprozessen der Todesstrafe entgeht, weil dem Gericht manches Beweisstück nicht vorliegt, weiß lange Zeit nichts über seinen einstigen geheimen Gegner. Ähnliches gilt für Heinz Bonatz, den vormaligen Leiter des Beobachtungsdienstes, der die Enigma bis zuletzt für unangreifbar hält. Es ist das letzte Geheimnis der Enigma, das allmählich ans Licht der Öffentlichkeit drängt.

1967 beschreibt der Warschauer Militärhistoriker Władysław Kozaczuk die Entzauberung der Enigma durch die polnischen Kryptologen in den 1930er Jahren, doch wird dem hinter dem Eisernen Vorhang erschienenen Buch im Westen kaum Beachtung geschenkt. Polen gehört mittlerweile zu den Staaten des Warschauer Pakts, dem Todfeind der westlichen Welt im Kalten Krieg. 1973 aber publiziert Gustave Bertrand in Paris *„Énigma ou la plus grande énigme de la guerre 1939–1945"*, worin er die polnisch-französische Zusammenarbeit schildert. Das provoziert eine britische Reaktion, die auch prompt erfolgt. 1974 erscheint Frederick Winterbothams Buch

mit dem Titel *„The Ultra Secret"*, das die Geschichte von Bletchley Park erzählt und die Enigma-Geschichte um das britische Kapitel ergänzt. In den nächsten Jahren folgen weitere Berichte von Zeitzeugen, nach und nach tritt die ganze Geschichte zutage.
Es ist freilich von bitterer Ironie, dass die beiden Hauptdarsteller der Geschichte nicht zu Wort kommen. Alan Turing, der geniale Mathematiker, der die Mittel entwickelt hat, um die Enigma endgültig zu besiegen, erlebt den Tag nicht, an dem die Öffentlichkeit von seinen bahnbrechenden Leistungen erfährt. Man hat ihn im England der 1950er Jahre seiner Homosexualität wegen vor Gericht gestellt, vollkommen diskreditiert, zu einer Hormontherapie gezwungen und letztlich in den Selbstmord getrieben.
Und Marian Rejewski, der nach dem Krieg zu seiner Familie nach Polen zurückgekehrt ist, erfährt überhaupt erst aus Winterbothams Buch von den umfangreichen Aktivitäten in Bletchley Park, obwohl er die letzten beiden Kriegsjahre im nahe gelegenen Boxmoor als Kryptologe verbracht hat. Man hat ihn ferngehalten vom streng geheimen Zentrum der Enigma-Entschlüsselung, obgleich doch er es war, der einst im polnischen Pyry die Saat dafür gelegt hat.

Kryptologie


hell Batterie dkl.
aus
R
T
Z
U
I
F
G
H
J
K
V
B
N
M
L
T
Z
U
G
I

Die Möglichkeiten der Enigma

Die ursprüngliche Ausstattung der Enigma sind drei Walzen. Da die Walzen in beliebiger Reihenfolge in die Maschine eingelegt werden können, ergeben sich sechs unterschiedliche Möglichkeiten für die Walzenlage, z.B. III-II-I oder I-II-III usw.:

$$3! = 3 \cdot 2 \cdot 1 = 6 \text{ Walzenlagen}$$

Jede der drei Walzen kann 26 verschiedene Stellungen einnehmen, d.h. insgesamt gibt es 17.576 unterschiedliche Einstellungsmöglichkeiten für die drei Walzen, z.B. 01-01-01 oder 01-01-02 usw.:

$$26^3 = 26 \cdot 26 \cdot 26 = 17.576 \text{ Stellungen}$$

Eine Steckerverbindung kann zwischen zwei beliebigen Buchstaben des Alphabets gesteckt werden, wofür 325 verschiedene Möglichkeiten existieren, z.B. (AB) oder (AC) usw.:

$$\binom{26}{2} = \frac{26!}{2!(26-2)!} = \frac{26!}{2!(24)!} = \frac{26 \cdot 25}{2!} = 325$$

Für eine zweite Steckerverbindung gibt es 276 Möglichkeiten, da hier nur mehr 24 Buchstaben zur Auswahl stehen:

$$\binom{24}{2} = \frac{24!}{2!(24-2)!} = \frac{24!}{2!(22)!} = \frac{24 \cdot 23}{2!} = 276$$

Analog ergeben sich für die weiteren Steckerverbindungen entsprechende Faktoren:

$$\binom{22}{2} = 231 \qquad \binom{20}{2} = 190 \qquad \binom{18}{2} = 153 \qquad \binom{16}{2} = 120$$

Bei sechs Steckerverbindungen erhält man über 100 Milliarden Steckmöglichkeiten unter Eliminierung der mehrfach vorkommenden Duplizierungen wie z.B. (AH) und (HA):

$$\frac{325 \cdot 276 \cdot 231 \cdot 190 \cdot 153 \cdot 120}{6!} = 100.391.791.500 \text{ Steckerverbindungen}$$

Insgesamt ergeben sich für die Enigma mit drei Walzen und sechs Steckerverbindungen (ohne Berücksichtigung der Ringe) über zehn Billiarden Einstellmöglichkeiten:

$$6 \cdot 17.576 \cdot 100.391.791.500 = 10.586.916.764.424.000 \text{ Einstellmöglichkeiten}$$

Kombinatorik

Permutation von n Objekten ohne Wiederholungen:

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$$

Ungeordnete Auswahl vom Umfang k aus einer Menge von n Objekten ohne Zurücklegen:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Geordnete Auswahl vom Umfang k aus einer Menge von n Objekten ohne Zurücklegen:

$$\frac{n!}{(n-k)!}$$


Nur Glühlampen mit
Durchmesser verwenden.
Q
W
E
R
A
S
D
X

Charakteristische
Transformationen und Zyklen

Von (rund) 60 aufgefangenen Funksprüchen eines Tages werden die doppelten Spruchschlüsselchiffren – etwa RGU IJT – in einer Tabelle untereinander aufgeschrieben und nebeneinander gestellt (wobei alle Schlüssel mit der unbekannten Tageseinstellung Walzenlage III-II-I, Ringstellung 01-01-01, Steckerverbindungen (BE)(RS)(KD)(WM)(CX)(PQ) und Grundstellung 01-01-01 verschlüsselt wurden):

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

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

49 *Die Schwachstellen der Enigma sind die Muster, die sie erzeugt.*

Nach alphabetischer Ordnung der Spruchschlüsselchiffren sind häufig auftretende Schlüssel erkennbar. Bestätigt sich die Annahme, dass sich hinter dem am häufigsten vorkommenden z.B. der trivialste Schlüssel AAA AAA verbirgt, kann dieser erraten werden:

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

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

Die invers arbeitende Enigma, die einen eingetippten Klarbuchstaben in eine Chiffre verwandelt, würde an derselben Maschinenstelle auch diese Chiffre in besagten Klarbuchstaben verwandeln. Ausgehend von dieser Überlegung, können für alle bekannten Chiffren die zugehörigen Klarbuchstaben eingesetzt werden. Danach werden alle mehrfach auftretenden Spruchschlüssel eliminiert und es verbleiben nur mehr 36 unterschiedliche Schlüssel:

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

					T
				G	
V	W	W	X	Y	Z
F	Q	U	H	C	A
T	M	H	E	W	B
K	Y	Y	N	E	U
Q	D	N	B	A	L
K	S	E	N	X	C

Ein doppelter Spruchschlüssel muss an erster und vierter Stelle immer gleiche Klarbuchstaben aufweisen, ebenso an zweiter und fünfter Stelle sowie an dritter und sechster. Noch freie Stellen solcher Paare können entsprechend ergänzt werden, wodurch weitere Beziehungen für andere Buchstaben erscheinen:

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

				G	T
				G	T
V	W	W	X	Y	Z
F	Q	U	H	C	A
T	M	H	E	W	B
K	Y	Y	N	E	U
Q	D	N	B	A	L
K	S	E	N	X	C

Am Ende der Prozedur erhält man einen kompletten Satz an Klarbuchstaben:

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

B	H	H	Q	G	T
B	H	E	Q	G	T
B	H	M	Q	G	T
B	H	H	Q	G	T
B	H	E	Q	G	T
B	H	M	Q	G	T
V	W	W	X	Y	Z
F	Q	U	H	C	A
T	M	H	E	W	B
K	Y	Y	N	E	U
Q	D	N	B	A	L
K	S	E	N	X	C

Die erste Zeile der oberen Tabellenhälfte, welche die Klarbuchstaben enthält, ergibt gemeinsam mit den Chiffren, die die Enigma ihnen zuweist, in der ersten Zeile der unteren Tabellenhälfte, die Buchstabentransformationen dieses Tages für die erste Stelle:

Stelle$_1$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T

Analog erhält man durch Klarbuchstaben und Chiffren der zweiten Stelle ein entsprechendes Buchstabentransformationsmuster:

Stelle$_2$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	T	F	G	J	U	B	C	Q	P	D	W	O	N	M	L	I	H	S	R	A	E	Z	K	Y	X	V

Gleiches gilt für die restlichen vier Stellen:

$Stelle_3$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	T	U	Y	Q	S	W	M	J	I	R	N	H	L	P	O	E	K	F	B	C	X	G	V	D	A

$Stelle_4$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	W	K	I	F	G	D	E	Y	C	R	B	X	V	Q	Z	S	N	J	P	U	T	M	A	L	H	O

$Stelle_5$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	G	Q	J	H	N	W	A	D	R	C	X	T	Y	E	Z	V	B	I	U	L	S	P	F	K	M	O

$Stelle_6$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	I	K	T	W	M	U	X	S	A	L	B	J	E	Q	P	O	N	V	H	C	F	R	D	G	Z	Y

Diese sechs Buchstabentransformationen für die sechs Stellen des Spruchschlüssels werden die charakteristischen Transformationen des Tages genannt.

Betrachtet man aufgrund der Struktur des doppelten Spruchschlüssels (der jeweils gleiche Klarbuchstaben an erster und vierter Stelle, zweiter und fünfter Stelle sowie dritter und sechster Stelle voraussetzt) die Buchstabentransformationen der ersten und vierten Stelle, erkennt man eine zyklische Struktur für einzelne Buchstabentransformationen bei der Produktbildung:

$Stelle_1$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T
$Stelle_4$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	W	K	I	F	G	D	E	Y	C	R	B	X	V	Q	Z	S	N	J	P	U	T	M	A	L	H	O
$Stelle_1 \cdot Stelle_4$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	D	M	J	Q	V	W	H	A	X	P	Z	C	G	F	B	T	L	I	R	O	S	K	Y	N	E	U

Man sieht, dass A in D übergeht, D in Q usw., bis ein Buchstabe wieder zum Ausgangsbuchstaben wird, hier H in A. Dabei entstehen mindestens zwei solcher Zyklen mit einer Länge von maximal 13 Buchstaben:

$$Stelle_1 \cdot Stelle_4 = (ADQLCJPTOBMGH)\ (EVKZUSRIXNFWY)$$

Für die anderen beiden Stellenpaare erhält man analog:

$$Stelle_2 \cdot Stelle_5 = (ALZPRUNYKFQDC)\ (BWXMESIVOTGJH)$$

$$Stelle_3 \cdot Stelle_6 = (AYWXRBCFHENJ)\ (DZILQMSUTKVG)\ (O)\ (P)$$

Die Zyklen mit ihren Buchstabenmustern ergeben sich mathematisch durch Produktbildung der Buchstabentransformationen (Permutationen) der ersten und vierten Stelle, der zweiten und fünften sowie der dritten und sechsten. Im Grunde genommen entstehen sie durch die Umkehrwalze, die die Inversität der Enigma begründet: ein Klarbuchstabe wird an einer bestimmten Maschinenstellung zu einer bestimmten Chiffre; diese Chiffre würde an derselben Maschinenstellung zu besagtem Klarbuchstaben. Daraus resultieren 13 Zyklen der Länge 2 (Zweierzyklen). In Zyklenschreibweise gilt daher für die Buchstabentransformation der ersten Stelle:

$$\text{Stelle}_1 = (AF)(BV)(CR)(DN)(EM)(GY)(HW)(IL)(JS)(KO)(PU)(QX)(TZ)$$

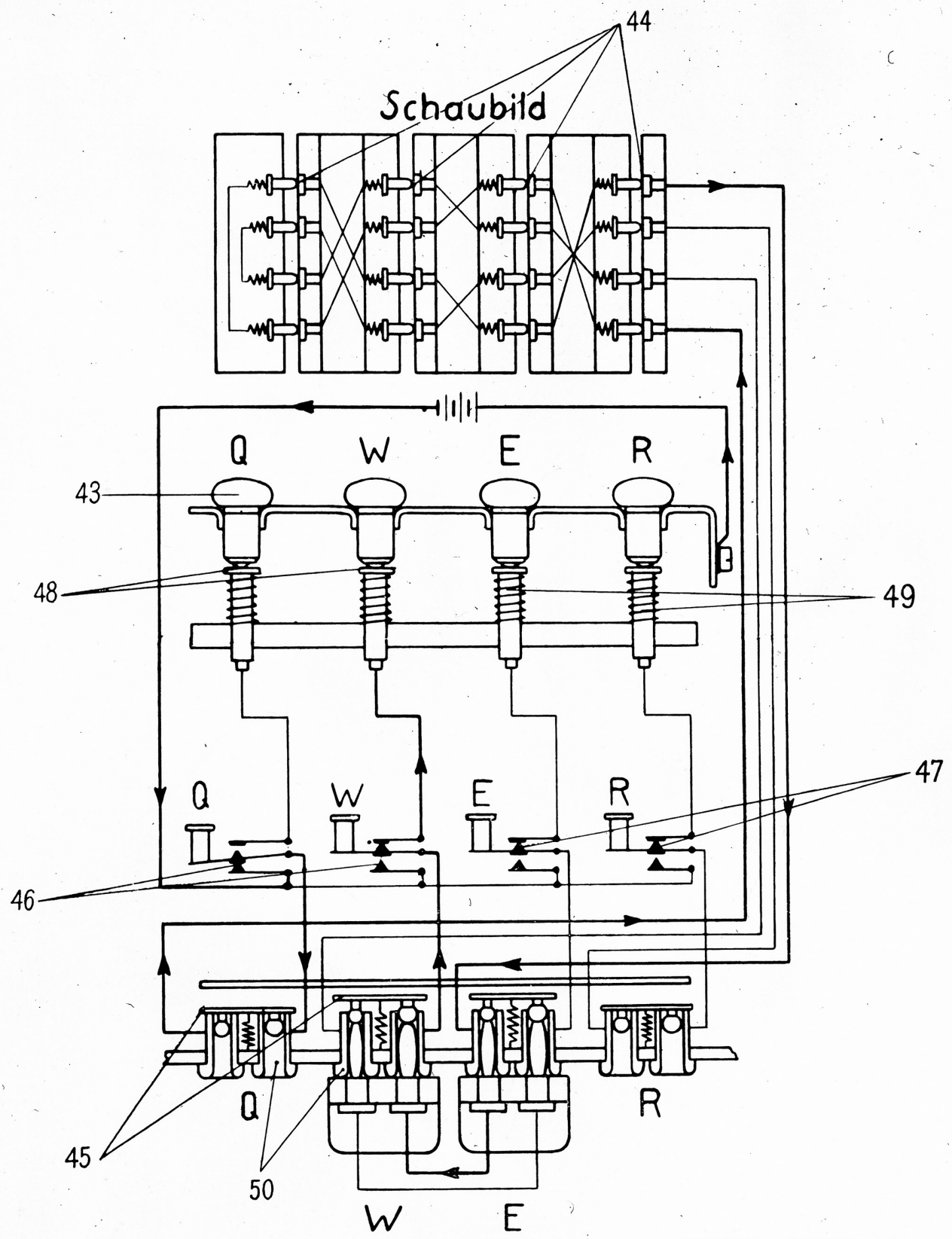
Die Paare von Zyklen im Produkt der beiden Buchstabentransformationen beinhalten nun jene Buchstabengruppen, die als Klarbuchstaben (ADQLCJPTOBMGH) in die Chiffren (EVKZUSRIXNFWY) und vice versa übergehen. Aus dem Zyklenmuster der dritten und sechsten Stelle folgt außerdem, dass durch die beiden Zyklen der Länge 1 (Einserzyklen) die entsprechende Buchstabentransformation O auf P und P auf O lauten muss, also daher eindeutig bestimmt ist.

Permutation und Zyklus

Bestehen zwei Permutationen X und Y aus n Elementen e ausschließlich aus Zyklen der Länge 2, so besteht das Produkt X·Y aus mindestens 2 und maximal n Zyklen gleicher Länge.

Daraus folgt: wenn im Produkt X·Y insgesamt nur zwei Einserzyklen (e1) und (e2) auftreten, so muss in den Permutationen X und Y jeweils der Zweierzyklus (e1e2) vorkommen.

Weiters folgt, dass beide Elemente eines Zweierzyklus in den Permutationen X und Y im Produkt X·Y immer in zwei unterschiedlichen Zyklen gleicher Länge stehen.


44
Schaubild
Q
W
E
R
43
48
49
47
46
45
50

Die Berechnung der Enigma

Bei der Enigma läuft ein eingetippter Klarbuchstabe zuerst über das Steckerfeld (S), weiter zur Eingangswalze (E), dann nacheinander über die rechte Walze (W_1), die mittlere Walze (W_2) und die linke Walze (W_3) bis hin zur Umkehrwalze (U) und anschließend den gesamten Weg zurück. Am Ende wird auf einem Leuchtfeld die zugewiesene Chiffre angezeigt. Dies lässt sich in folgender Formel abbilden:

$$\text{Enigma} = S\ E\ W_1\ W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}\ W_1^{-1}\ E^{-1}\ S^{-1}$$

Bei einem Tastendruck dreht sich zuerst die rechte Walze (W_1) um einen Drehschritt (D) weiter, bevor ein Stromkreis durch die jeweilige Verdrahtung geschlossen wird. Der Stromkreis bleibt solange geschlossen, wie eine Taste gedrückt gehalten wird, was die zugehörige Chiffre aufleuchten lässt.
Die mechanische Kraft des Tastendrucks dient zur Weiterdrehung der ersten Walze. Die zweite Walze dreht sich alle 26 Stellen und die dritte Walze nur alle 676 = 26·26 Stellen weiter, weshalb in der großen Mehrzahl der Fälle die beiden Walzen als statisch angenommen werden können. Die Buchstabentransformationen einer beliebigen Stelle können daher wie folgt geschrieben werden:

$$\text{Stelle} = S\ E\ D\ W_1\ D^{-1}\ W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}\ D\ W_1^{-1}\ D^{-1}\ E^{-1}\ S^{-1}$$

Beim zivilen Modell der Enigma ist die Eingangswalze der Reihe nach direkt mit den Tasten von links oben bis rechts unten verdrahtet, also in der Reihenfolge QWERTZUIOASDFGHJKPYXCVBNML. Rejewskis Berechnungen zeigen jedoch, dass dies bei der Heeres-Enigma nicht der Fall ist. Da die militärische Enigma im Gegensatz zur zivilen Version ein Steckerfeld besitzt, vermutet er, dass bei ihr eine triviale Verdrahtung benützt wird, da die Steckerverbindungen ohnehin alle möglichen Verdrahtungen der Eingangswalze herzustellen erlauben:

Eingang = id	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Dadurch kann nun die Eingangswalze in den Buchstabentransformationen einer Stelle einfach eliminiert werden:

$$\text{Stelle} = S\ D\ W_1\ D^{-1}\ W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}\ D\ W_1^{-1}\ D^{-1}\ S^{-1}$$

Ein Drehschritt D vorwärts bzw. ein Drehschritt D^{-1} rückwärts entspricht jeweils einer einfachen Permutation des Alphabets vorwärts bzw. rückwärts:

Drehschritt	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

$Drehschritt^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Die Buchstabentransformationen jeder der sechs Stellen, die aus den Spruchschlüsseln eines Tages abgeleitet sind, entstammen derselben Maschineneinstellung der Enigma. Der Abstand zwischen den Stellen entspricht nur einem Drehschritt bzw. mehreren Drehschritten der rechten Walze (W_1):

$$\text{Stelle}_1 = S\ D\ W_1\ D^{-1}\ W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}\ D\ W_1^{-1}\ D^{-1}\ S^{-1}$$
$$\text{Stelle}_2 = S\ D^2\ W_1\ D^{-2}\ W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}\ D^2\ W_1^{-1}\ D^{-2}\ S^{-1}$$
$$\text{Stelle}_3 = S\ D^3\ W_1\ D^{-3}\ W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}\ D^3\ W_1^{-1}\ D^{-3}\ S^{-1}$$
$$\text{Stelle}_4 = S\ D^4\ W_1\ D^{-4}\ W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}\ D^4\ W_1^{-1}\ D^{-4}\ S^{-1}$$
$$\text{Stelle}_5 = S\ D^5\ W_1\ D^{-5}\ W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}\ D^5\ W_1^{-1}\ D^{-5}\ S^{-1}$$
$$\text{Stelle}_6 = S\ D^6\ W_1\ D^{-6}\ W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}\ D^6\ W_1^{-1}\ D^{-6}\ S^{-1}$$

Mit der bereits beschriebenen Annahme, dass sich die mittlere und linke Walze für die sechs Stellen nicht drehen, können diese beiden Walzen mit der Umkehrwalze zu einer konstanten fiktiven Umkehrwalze U_C zusammengefasst werden und man erhält sechs Gleichungen mit nur mehr drei Unbekannten:

$$\text{Stelle}_1 = S\ D\ W_1\ D^{-1}\ U_C\ D\ W_1^{-1}\ D^{-1}\ S^{-1}$$
$$\text{Stelle}_2 = S\ D^2\ W_1\ D^{-2}\ U_C\ D^2\ W_1^{-1}\ D^{-2}\ S^{-1}$$
$$\text{Stelle}_3 = S\ D^3\ W_1\ D^{-3}\ U_C\ D^3\ W_1^{-1}\ D^{-3}\ S^{-1}$$
$$\text{Stelle}_4 = S\ D^4\ W_1\ D^{-4}\ U_C\ D^4\ W_1^{-1}\ D^{-4}\ S^{-1}$$
$$\text{Stelle}_5 = S\ D^5\ W_1\ D^{-5}\ U_C\ D^5\ W_1^{-1}\ D^{-5}\ S^{-1}$$
$$\text{Stelle}_6 = S\ D^6\ W_1\ D^{-6}\ U_C\ D^6\ W_1^{-1}\ D^{-6}\ S^{-1}$$

mit $U_C = W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}$

Mit den zur Verfügung stehenden Geheimunterlagen, die alle Tageseinstellungen der Enigma für die Monate September und Oktober 1932 enthalten, sind die zugehörigen Steckerverbindungen bekannt, weshalb diese neben den Buchstabentransformationen aus den erratenen Spruchschlüsseln auf die linke Seite der Gleichungen gebracht werden können:

$$S^{-1}\,\text{Stelle}_1\,S = D\,W_1\,D^{-1}\,U_C\,D\,W_1^{-1}\,D^{-1}$$
$$S^{-1}\,\text{Stelle}_2\,S = D^2\,W_1\,D^{-2}\,U_C\,D^2\,W_1^{-1}\,D^{-2}$$
$$S^{-1}\,\text{Stelle}_3\,S = D^3\,W_1\,D^{-3}\,U_C\,D^3\,W_1^{-1}\,D^{-3}$$
$$S^{-1}\,\text{Stelle}_4\,S = D^4\,W_1\,D^{-4}\,U_C\,D^4\,W_1^{-1}\,D^{-4}$$
$$S^{-1}\,\text{Stelle}_5\,S = D^5\,W_1\,D^{-5}\,U_C\,D^5\,W_1^{-1}\,D^{-5}$$
$$S^{-1}\,\text{Stelle}_6\,S = D^6\,W_1\,D^{-6}\,U_C\,D^6\,W_1^{-1}\,D^{-6}$$

Produkte von Permutationen

Für die Produkte von Permutationen X und Y gilt:

$$X^0 = X^1\,X^{-1} = \text{id}$$

$$(X\,Y)^{-1} = Y^{-1}\,X^{-1}$$

Im Allgemeinen ist das Produkt zweier Permutationen nicht kommutativ:

$$X\,Y \neq Y\,X$$

Wird die Permutation des Drehschritts auch noch auf die linke Seite gebracht, erhält man:

$$T_1 = D^{-1}\,S^{-1}\,\text{Stelle}_1\,S\,D = W_1\,D^{-1}\,U_C\,D\,W_1^{-1}$$
$$T_2 = D^{-2}\,S^{-1}\,\text{Stelle}_2\,S\,D^2 = W_1\,D^{-2}\,U_C\,D^2\,W_1^{-1}$$
$$T_3 = D^{-3}\,S^{-1}\,\text{Stelle}_3\,S\,D^3 = W_1\,D^{-3}\,U_C\,D^3\,W_1^{-1}$$
$$T_4 = D^{-4}\,S^{-1}\,\text{Stelle}_4\,S\,D^4 = W_1\,D^{-4}\,U_C\,D^4\,W_1^{-1}$$
$$T_5 = D^{-5}\,S^{-1}\,\text{Stelle}_5\,S\,D^5 = W_1\,D^{-5}\,U_C\,D^5\,W_1^{-1}$$
$$T_6 = D^{-6}\,S^{-1}\,\text{Stelle}_6\,S\,D^6 = W_1\,D^{-6}\,U_C\,D^6\,W_1^{-1}$$

Dabei entsprechen hier die Transformationen T einer Art Normierung auf die Grundstellung der Enigma, also jener Stellung, die vor dem ersten Tastendruck gegeben ist.

Das Ziel der weiteren Umformung ist es, die unbekannte, aber konstante Größe U_C aus den Gleichungen zu eliminieren, um die Verdrahtung der rechten Walze berechnen zu können. Dazu bildet man nacheinander Produkte der einzelnen Transformationen T und fasst anschließend die resultierenden Gleichungen zusammen:

$$T_1\,T_2 = W_1\,D^{-1}\,U_C\,D\,W_1^{-1}\,W_1\,D^{-2}\,U_C\,D^{2}\,W_1^{-1} = W_1\,D^{-1}\,(U_C\,D^{-1}\,U_C\,D)\,D\,W_1^{-1}$$
$$T_2\,T_3 = W_1\,D^{-2}\,U_C\,D^{2}\,W_1^{-1}\,W_1\,D^{-3}\,U_C\,D^{3}\,W_1^{-1} = W_1\,D^{-2}\,(U_C\,D^{-1}\,U_C\,D)\,D^{2}\,W_1^{-1}$$
$$T_3\,T_4 = W_1\,D^{-3}\,U_C\,D^{3}\,W_1^{-1}\,W_1\,D^{-4}\,U_C\,D^{4}\,W_1^{-1} = W_1\,D^{-3}\,(U_C\,D^{-1}\,U_C\,D)\,D^{3}\,W_1^{-1}$$

Aus der zweiten Gleichung folgt:

$$D^{2}\,W_1^{-1}\,T_2\,T_3\,W_1\,D^{-2} = U_C\,D^{-1}\,U_C\,D$$

Setzt man diesen Ausdruck in die erste Gleichung ein, erhält man einen Ausdruck ohne U_C:

$$T_1\,T_2 = W_1\,D^{-1}\,(D^{2}\,W_1^{-1}\,T_2\,T_3\,W_1\,D^{-2})\,D\,W_1^{-1} = W_1\,D\,W_1^{-1}\,T_2\,T_3\,W_1\,D^{-1}\,W_1^{-1}$$

Analog ergibt sich für die zweite Gleichung nach Umformung:

$$T_1\,T_2 = (W_1\,D\,W_1^{-1})\,T_2\,T_3\,(W_1\,D\,W_1^{-1})^{-1}$$
$$T_2\,T_3 = (W_1\,D\,W_1^{-1})\,T_3\,T_4\,(W_1\,D\,W_1^{-1})^{-1}$$

Da sich die Transformationen T und deren Produkte alle auf den gleichen Verdrahtungszustand beziehen, nämlich den der Grundstellung, müssen auch ihre resultierenden Zyklenstrukturen identisch sein. Man setzt nun die Buchstabentransformationen der sechs Stellen eines Tages und die jeweiligen Steckerverbindungen in die Gleichungen für die normierten Transformationen T ein.

Für einen Tag im September 1932 seien beispielsweise folgende Buchstabentransformationen durch Erraten von Spruchschlüssel hergeleitet worden:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_1$	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_2$	T	F	G	J	U	B	C	Q	P	D	W	O	N	M	L	I	H	S	R	A	E	Z	K	Y	X	V

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_3$	Z	T	U	Y	Q	S	W	M	J	I	R	N	H	L	P	O	E	K	F	B	C	X	G	V	D	A

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_4$	W	K	I	F	G	D	E	Y	C	R	B	X	V	Q	Z	S	N	J	P	U	T	M	A	L	H	O

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_5$	G	Q	J	H	N	W	A	D	R	C	X	T	Y	E	Z	V	B	I	U	L	S	P	F	K	M	O

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_6$	I	K	T	W	M	U	X	S	A	L	B	J	E	Q	P	O	N	V	H	C	F	R	D	G	Z	Y

In den Schlüsselunterlagen für den Monat September findet sich beispielsweise folgende Tageseinstellung: Walzenlage III-II-I, Ringstellung 01-01-01, Steckerverbindungen (BE)(RS)(KD)(WM)(CX)(PQ) und Grundstellung 01-01-01.

Daraus ergibt sich für die normierten Transformationen T:

$T_1 = D^{-1}\, S^{-1}\, Stelle_1\, S\, D$

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D^{-1}	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
S^{-1}	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
$Stelle_1$	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T
S	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
D	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
T_1	U	G	X	Q	P	W	B	Z	N	M	S	O	J	I	L	E	D	V	K	Y	A	R	F	C	T	H

$T_2 = D^{-2} S^{-1} \text{Stelle}_2 S D^2$

D^{-2}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
S^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
Stelle_2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	T	F	G	J	U	B	C	Q	P	D	W	O	N	M	L	I	H	S	R	A	E	Z	K	Y	X	V
S	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
D^2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
T_2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	E	X	V	W	A	O	H	G	Z	R	S	M	L	Q	F	Y	N	J	K	U	T	C	D	B	P	I

$T_3 = D^{-3} S^{-1} \text{Stelle}_3 S D^3$

D^{-3}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
S^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
Stelle_3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	T	U	Y	Q	S	W	M	J	I	R	N	H	L	P	O	E	K	F	B	C	X	G	V	D	A
S	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
D^3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
T_3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	X	N	D	C	S	Y	V	W	U	P	Z	M	L	B	Q	J	O	T	E	R	I	G	H	A	F	K

$T_4 = D^{-4} S^{-1} \text{Stelle}_4 S D^4$

D^{-4}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
S^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
Stelle_4	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	W	K	I	F	G	D	E	Y	C	R	B	X	V	Q	Z	S	N	J	P	U	T	M	A	L	H	O
S	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
D^4	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
T_4	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	M	L	S	Q	K	P	I	H	O	F	C	B	W	J	G	E	T	D	R	V	U	N	Y	X	A

Für das Produkt von $T_1 T_2$ ergibt sich nun:

T_1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	U	G	X	Q	P	W	B	Z	N	M	S	O	J	I	L	E	D	V	K	Y	A	R	F	C	T	H
T_2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	E	X	V	W	A	O	H	G	Z	R	S	M	L	Q	F	Y	N	J	K	U	T	C	D	B	P	I
$T_1 T_2$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	T	H	B	N	Y	D	X	I	Q	L	K	F	R	Z	M	A	W	C	S	P	E	J	O	V	U	G

Analog findet man für die restlichen Produkte:

$T_2 T_3$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	S	A	G	H	X	Q	W	V	K	T	E	L	M	O	Y	F	B	P	Z	I	R	D	C	N	J	U

$T_3 T_4$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Y	W	S	L	D	X	U	N	V	G	A	B	C	M	E	O	J	R	Q	T	H	P	I	Z	K	F

Die entsprechenden Zyklen der Produkte können nun einfach abgelesen werden:

$T_1 T_2$ = (ATP) (BHIQWOMRC) (DNZGXVJLF) (EYU) (K) (S)
$T_2 T_3$ = (ASZURPFQB) (CGW) (DHV) (EXNOYJTIK) (L) (M)
$T_3 T_4$ = (AYK) (BWIVPOEDL) (CSQJGUHNM) (FXZ) (R) (T)

Die Zyklen der Produkte haben alle die gleiche Struktur, sie bestehen aus zwei Neunerzyklen, zwei Dreierzyklen und zwei Einserzyklen. Da die normierten Transformationen aber alle dem gleichen Verdrahtungszustand entstammen, muss nicht nur ihre Zyklenstruktur dieselbe sein, sondern auch alle darin enthaltenen expliziten Buchstabentransformationen müssen identisch sein. Man versucht nun durch geschicktes Untereinanderschreiben der Zyklen – wobei eine zyklische Rotation der Buchstaben innerhalb eines Zyklus natürlich erlaubt ist – diese konsistent zueinander auszurichten. Beginnend mit den Einserzyklen (K) über (L) folgt beispielsweise:

$T_1 T_2$ = (K)
$T_2 T_3$ = (L) (K E X N O Y J T I)
$T_3 T_4$ = (L B W I V P O E D)

Nun impliziert aber E über B in der zweiten und dritten Zeile, dass auch E über B in der ersten und zweiten Zeile stehen muss:

$T_1 T_2$ = (K) (E Y U)
$T_2 T_3$ = (L) (K E X N O Y J T I) (B A S Z U R P F Q)
$T_3 T_4$ = (L B W I V P O E D)

Dies erzeugt aber einen Widerspruch, da die Buchstaben E und B nun in Zyklen unterschiedlicher Länge vorkommen. Versucht man die andere Möglichkeit mit den Einserzyklen K über M, zeigt sich, dass E über C in Folge gelten muss:

$T_1 T_2 =$	(K)										(E	Y	U)	
$T_2 T_3 =$	(M)	(K	E	X	N	O	Y	J	T	I)	(C	G	W)	
$T_3 T_4 =$		(M	C	S	Q	J	G	U	H	N)				

Mit der nächsten Bedingung X über S findet man:

$T_1 T_2 =$	(K)										(E	Y	U)	(X	V	J	L	F	D	N	Z	G)
$T_2 T_3 =$	(M)	(K	E	X	N	O	Y	J	T	I)	(C	G	W)	(S	Z	U	R	P	F	Q	B	A)
$T_3 T_4 =$		(M	C	S	Q	J	G	U	H	N)												

Für die übernächste Bedingung O über J zeigt sich:

$T_1 T_2 =$	(K)	(C	B	H	I	Q	W	O	M	R)	(E	Y	U)	(X	V	J	L	F	D	N	Z	G)
$T_2 T_3 =$	(M)	(K	E	X	N	O	Y	J	T	I)	(C	G	W)	(S	Z	U	R	P	F	Q	B	A)
$T_3 T_4 =$		(M	C	S	Q	J	G	U	H	N)												

Schließlich lassen sich so alle konsistent ausgerichteten Zyklen finden:

$T_1 T_2 =$	(K)	(C	B	H	I	Q	W	O	M	R)	(E	Y	U)	(X	V	J	L	F	D	N	Z	G)	(T	P	A)	(S)
$T_2 T_3 =$	(M)	(K	E	X	N	O	Y	J	T	I)	(C	G	W)	(S	Z	U	R	P	F	Q	B	A)	(H	V	D)	(L)
$T_3 T_4 =$	(T)	(M	C	S	Q	J	G	U	H	N)	(K	A	Y)	(L	B	W	I	V	P	O	E	D)	(X	Z	F)	(R)

Mit obiger Beziehung für das Produkt der normierten Transformationen

$$T_1 T_2 = (W_1 D W_1^{-1}) T_2 T_3 (W_1 D W_1^{-1})^{-1}$$

folgt der Zyklus für den Ausdruck mit der rechten Walze W_1, die mit den bekannten Tageseinstellungen der Schlüsselunterlagen z.B. auch als Walze I identifiziert werden kann:

$$W_1 D W_1^{-1} = (KMTHXSLRINQOJUWYGADFPVZBEC)$$

Für die Lösung von W_1 ergeben sich 26 mögliche Verdrahtungsmuster, da die Elemente im obigen Zyklus natürlich zyklisch rotiert werden dürfen. Die jeweiligen Lösungen entsprechen somit den unterschiedlichen Drehstellungen der Walze W_1:

W_{1a}	K	M	T	H	X	S	L	R	I	N	Q	O	J	U	W	Y	G	A	D	F	P	V	Z	B	E	C
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

W_{1b}	M	T	H	X	S	L	R	I	N	Q	O	J	U	W	Y	G	A	D	F	P	V	Z	B	E	C	K
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

usw.

Nach dem Ordnen der Eingänge der Walze in alphabetischer Reihenfolge ergibt sich:

W_{1a}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	R	X	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H	F	C	N	V	O	E	P	W

W_{1b}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	S	Y	A	T	Z	U	R	E	J	N	B	H	C	K	M	V	L	I	G	D	O	W	P	F	Q	X

usw.

Für W_{1a} folgt beispielsweise:

W_{1a}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	R	X	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H	F	C	N	V	O	E	P	W
D	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
W_{1a}^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	K	M	T	H	X	S	L	R	I	N	Q	O	J	U	W	Y	G	A	D	F	P	V	Z	B	E	C
$W_{1a}\ D\ W_{1a}^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	D	E	K	F	C	P	A	X	N	U	M	R	T	Q	J	V	O	I	L	H	W	Z	Y	S	G	B

In Zyklenschreibweise:

$$W_1\ D\ W_1^{-1} = (ADFPVZBECKMTHXSLRINQOJUWYG)$$

Dies ist natürlich äquivalent zum ursprünglichen Zyklus bis auf die zyklische Rotation:

$$W_1\ D\ W_1^{-1} = (KMTHXSLRINQOJUWYGADFPVZBEC)$$

Für einen Tag im Oktober 1932 – da die Walzenlage quartalsweise geändert wird, liegt nun eine andere Walze an der rechten Position – seien beispielsweise folgende Buchstabentransformationen hergeleitet worden:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_1$	S	O	J	L	W	X	H	G	Q	C	U	D	V	P	B	N	I	Z	A	Y	K	M	E	F	T	R

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_2$	B	A	G	F	U	D	C	P	X	M	R	V	J	Q	Z	H	N	K	Y	W	E	L	T	I	S	O

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_3$	D	V	R	A	Y	J	X	K	Z	F	H	W	S	P	T	N	U	C	M	O	Q	B	L	G	E	I

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_4$	M	G	I	O	H	R	B	E	C	U	Q	P	A	W	D	L	K	F	T	S	J	Y	N	Z	V	X

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_5$	B	A	N	V	W	J	R	M	S	F	U	O	H	C	L	T	Y	G	I	P	K	D	E	Z	Q	X

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_6$	W	S	U	G	I	M	D	V	E	P	Z	Y	F	O	N	J	X	T	B	R	C	H	A	Q	L	K

In den geheimen Schlüsselunterlagen für den Monat Oktober findet sich beispielsweise folgende Tageseinstellung: Walzenlage I-III-II, Ringstellung 01-01-01, Steckerverbindungen (AB)(CD)(EF)(GH)(IJ)(KL) und Grundstellung 01-01-06.

Auf analoge Weise wie bei der Berechnung für den September ergibt sich hier für die Walze W_2 im Oktober 1932:

$$W_2\, D\, W_2^{-1} = (AJPCZWRLFBDKOTYUQGENHXMIVS)$$

Ebenso gibt es für die Walze W_2 wiederum 26 Verdrahtungsmöglichkeiten, abhängig von ihrer Drehstellung. Diese Walze kann mit Hilfe der Schlüsselunterlagen beispielsweise als Walze II identifiziert werden:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W_{2a}	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W_{2b}	B	K	E	L	T	J	S	V	Y	C	M	I	X	U	N	D	R	H	A	O	Q	Z	G	W	P	F

usw.

Um aber nicht nur das Verdrahtungsmuster einer Walze zu bestimmen, sondern auch die exakte Drehstellung der Walze aus den 26 Möglichkeiten fixieren zu können, vergleicht man zwei unterschiedliche Tageseinstellungen, die z.B. im September die noch unbekannte Walze W_3 als linke Walze vorgeben und eine Grundstellung mit gleicher Position für diese dritte Walze aufweisen.

Beispielsweise sei an einem Tag X im September 1932 folgender Tagesschlüssel gegeben: Walzenlage III-II-I, Ringstellung 01-01-01, Steckerverbindungen = (BE)(RS)(KD)(WM)(CX)(PQ) und Grundstellung 01-01-01. Die zugehörige Buchstabentransformation an dieser Grundstellung ist:

$Stelle_{1\_TagX}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T

Für einen anderen Tag Y im selben Quartal sei z.B. folgender Tagesschlüssel gegeben: Walzenlage III-II-I, Ringstellung 01-01-01, Steckerverbindungen = (BE)(RS)(KD)(WM)(CX)(PQ) und Grundstellung 01-02-02. Die entsprechende Buchstabentransformation an dieser Grundstellung ist:

$Stelle_{1\_TagY}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	C	L	A	P	S	R	T	W	U	V	N	B	Z	K	X	D	Y	F	E	G	I	J	H	O	Q	M

Für den einen Tag X gilt nun:

$$Stelle_{1\_TagX} = S\ D\ W_1\ D^{-1}\ W_2\ W_3\ U\ W_3^{-1}\ W_2^{-1}\ D\ W_1^{-1}\ D^{-1}\ S^{-1}$$

Nach Umformung erhält man:

$$W_3\ U\ W_3^{-1} = (D\ W_1\ D^{-1}\ W_2)^{-1} (S^{-1}\ Stelle_{1\_TagX}\ S)\ (D\ W_1\ D^{-1}\ W_2)$$

Für den anderen Tag Y, an dem die rechte und mittlere Walze aufgrund der geänderten Grundstellung um je einen Schritt weitergedreht ist, gilt analog:

$$W_3\ U\ W_3^{-1} = (D^2\ W_1\ D^{-2}\ D\ W_2\ D^{-1})^{-1} (S^{-1}\ Stelle_{1\_TagY}\ S)\ (D^2\ W_1\ D^{-2}\ D\ W_2\ D^{-1})$$

Für beide Walzen W_1 und W_2 gibt es noch je 26 Möglichkeiten der Verdrahtungsausrichtung. Wenn man jedoch berücksichtigt, dass für beide Tage derselbe Ausdruck entstehen muss, reicht es, für die mittlere Walze W_2 eine beliebige Möglichkeit auszuwählen (jede andere würde nur einer unterschiedlichen aber ebenso gleichwertigen Grundstellung der mittleren Walze entsprechen) und anschließend für die erste Walze W_1 alle 26 Möglichkeiten durchzuprobieren. Die richtige Lösung für die erste Walze ergibt sich, wenn beide Male derselbe Ausdruck entsteht, da beide Tage dieselbe Stellung für die linke Walze W_3 vorgeben.

Für den Tag X folgt demnach:

$$W_{3a}\ U\ W_{3a}^{-1} = (D\ W_{1a}\ D^{-1}\ W_2)^{-1} (S^{-1}\ Stelle_{1\_TagX}\ S)\ (D\ W_{1a}\ D^{-1}\ W_2)$$
$$W_{3b}\ U\ W_{3b}^{-1} = (D\ W_{1b}\ D^{-1}\ W_2)^{-1} (S^{-1}\ Stelle_{1\_TagX}\ S)\ (D\ W_{1b}\ D^{-1}\ W_2)$$

usw.

Für den Tag Y folgt analog:

$$W_{3a}\ U\ W_{3a}^{-1} = (D^2\ W_{1a}\ D^{-2}\ D\ W_2\ D^{-1})^{-1} (S^{-1}\ Stelle_{1\_TagY}\ S)\ (D^2\ W_{1a}\ D^{-2}\ D\ W_2\ D^{-1})$$
$$W_{3b}\ U\ W_{3b}^{-1} = (D^2\ W_{1b}\ D^{-2}\ D\ W_2\ D^{-1})^{-1} (S^{-1}\ Stelle_{1\_TagY}\ S)\ (D^2\ W_{1b}\ D^{-2}\ D\ W_2\ D^{-1})$$

usw.

Für die Berechnung der Möglichkeiten ist es vorteilhaft, die Stecker mit den Buchstabentransformationen der ersten Stellen der beiden Tage X und Y zuerst zu berechnen, da dieser Ausdruck sich nicht ändert:

S^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
$Stelle_{1\_TagX}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T
S	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
$S^{-1}\ Stelle_{1\_TagX}\ S$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	W	P	O	V	A	Y	M	L	R	N	I	H	K	D	C	U	J	X	Z	Q	E	B	S	G	T

und

S^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
$Stelle_{1\_TagY}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	C	L	A	P	S	R	T	W	U	V	N	B	Z	K	X	D	Y	F	E	G	I	J	H	O	Q	M
S	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
$S^{-1}\ Stelle_{1\_TagY}\ S$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	X	R	O	N	L	S	T	M	U	V	Q	E	H	D	C	Y	K	B	F	G	I	J	Z	A	P	W

Weiters ergeben sich für die Varianten der Ausdrücke $D\ W_1\ D^{-1}$ folgende Buchstabentransformationen:

D	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
W_{1a}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	R	X	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H	F	C	N	V	O	E	P	W
D^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
$D\ W_{1a}\ D^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	W	Y	R	X	S	P	C	H	L	Z	F	A	I	K	T	J	G	E	B	M	U	N	D	O	V	Q

Anlog für die zweite Variante:

$D\ W_{1b}\ D^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	X	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H	F	C	N	V	O	E	P	W	R

usw.

Man erkennt, dass folgende Beziehungen zwischen den Varianten gelten:

$$D\ W_{1b}\ D^{-1} = (D\ W_{1a}\ D^{-1})\ D$$
$$D\ W_{1c}\ D^{-1} = (D\ W_{1b}\ D^{-1})\ D$$

usw.

$$W_{3a}\ U\ W_{3a}^{-1} = (D\ W_{1a}\ D^{-1}\ W_{2a})^{-1} (S^{-1}\ Stelle_{1\_TagX}\ S)\ (D\ W_{1a}\ D^{-1}\ W_{2a})$$

Für die erste Variante der ersten Walze W_{1a} ergibt sich daraus für den Tag X (für die zweite Walze W_2 wird nun eine beliebige Variante beispielsweise W_{2a} eingesetzt):

$$W_{3a}\ U\ W_{3a}^{-1} = (D\ W_{1a}\ D^{-1}\ W_{2a})^{-1} (S^{-1}\ Stelle_{1\_TagX}\ S)\ (D\ W_{1a}\ D^{-1}\ W_{2a})$$

$D\ W_{1a}\ D^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	W	Y	R	X	S	P	C	H	L	Z	F	A	I	K	T	J	G	E	B	M	U	N	D	O	V	Q
W_{2a}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
$(D\ W_{1a}\ D^{-1}\ W_{2a})$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	O	G	V	Z	C	D	U	H	E	I	A	X	L	N	B	R	S	J	W	P	T	K	M	Y	Q

Setzt man dies nun in obige Beziehung ein, ergibt sich:

$(D\,W_{1a}\,D^{-1}\,W_{2a})^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	L	P	F	G	J	A	C	I	K	S	W	N	X	O	B	U	Z	Q	R	V	H	D	T	M	Y	E
$S^{-1}\,Stelle_{1\_Tag}X\,S$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	W	P	O	V	A	Y	M	L	R	N	I	H	K	D	C	U	J	X	Z	Q	E	B	S	G	T
$(D\,W_{1a}\,D^{-1}\,W_{2a})$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	O	G	V	Z	C	D	U	H	E	I	A	X	L	N	B	R	S	J	W	P	T	K	M	Y	Q
$W_{3a}\,U\,W_{3a}^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	H	G	F	Y	S	C	B	A	L	M	O	I	J	V	K	R	W	P	E	Z	X	N	Q	U	D	T

Berechnet man analog alle weiteren 25 Drehvarianten der Verdrahtung für die erste Walze, so erhält man folgende mögliche Lösungen für den Tag X:

$W_3\,U\,W_3^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	H	G	F	Y	S	C	B	A	L	M	O	I	J	V	K	R	W	P	E	Z	X	N	Q	U	D	T
b	I	X	D	C	S	K	T	R	A	W	F	Z	N	M	P	O	V	H	E	G	Y	Q	J	B	U	L
c	I	L	P	T	Y	X	O	N	A	R	Q	B	Z	H	G	C	K	J	V	D	W	S	U	F	E	M
d	F	V	N	U	Z	A	S	L	O	R	M	H	K	C	I	W	Y	J	G	X	D	B	P	T	Q	E
e	N	M	S	U	R	G	F	W	Z	V	X	O	B	A	L	Q	P	E	C	Y	D	J	H	K	T	I
f	U	S	L	O	H	M	Y	E	Q	P	X	C	F	R	D	J	I	N	B	W	A	Z	T	K	G	V
g	W	S	V	Y	K	Z	R	Q	L	X	E	I	T	O	N	U	H	G	B	M	P	C	A	J	D	F
h	S	D	M	B	P	K	W	R	L	T	F	I	C	V	Q	E	O	H	A	J	Z	N	G	Y	X	U
i	Y	F	Q	M	G	B	E	R	J	I	L	K	D	X	P	O	C	H	V	Z	W	S	U	N	A	T
j	Z	P	K	R	Y	J	Q	S	O	F	C	V	N	M	I	B	G	D	H	X	W	L	U	T	E	A
k	F	M	P	V	R	A	Z	O	W	N	U	Y	B	J	H	C	S	E	Q	X	K	D	I	T	L	G
l	U	M	L	P	W	H	I	F	G	V	O	C	B	Z	K	D	Y	T	X	R	A	J	E	S	Q	N
m	T	I	L	O	S	G	F	Q	B	X	Y	C	U	P	D	N	H	Z	E	A	M	W	V	J	K	R
n	I	D	X	B	K	S	W	Q	A	M	E	R	J	U	T	Y	H	L	F	O	N	Z	G	C	P	V
o	S	Q	D	C	M	Y	W	U	V	R	L	K	E	O	N	X	B	J	A	Z	H	I	G	P	F	T
p	C	Y	A	U	P	V	L	S	J	I	Q	G	N	M	R	E	K	O	H	Z	D	F	X	W	B	T
q	Y	T	P	R	U	L	S	Z	W	Q	X	F	N	M	V	C	J	D	G	B	E	O	I	K	A	H
r	X	S	P	G	O	J	D	V	Z	F	U	M	L	W	E	C	Y	T	B	R	K	H	N	A	Q	I
s	E	J	H	V	A	G	F	C	L	B	Z	I	U	R	W	T	Y	N	X	P	M	D	O	S	Q	K
t	J	I	X	L	T	G	F	R	B	A	O	D	Y	S	K	U	W	H	N	E	P	Z	Q	C	M	V
u	M	Q	F	J	S	C	T	K	P	D	H	R	A	O	N	I	B	L	E	G	W	Z	U	Y	X	V
v	I	F	J	K	P	B	L	U	A	C	D	G	Z	O	N	E	V	Y	W	X	H	Q	S	T	R	M
w	Y	M	N	Q	P	U	O	Z	T	R	S	V	B	C	G	E	D	J	K	I	F	L	X	W	A	H
x	Y	T	L	U	Z	J	K	O	S	F	G	C	R	W	H	Q	P	M	I	B	D	X	N	V	A	E
y	N	O	U	V	W	J	Y	Q	R	F	X	M	L	A	B	T	H	I	Z	P	C	D	E	K	G	S
z	T	S	H	V	L	Z	W	C	N	P	O	E	Y	I	K	J	X	U	B	A	R	D	G	Q	M	F

Für den Tag Y wird für die Walze W_2 wiederum W_{2a} gewählt und man erhält analog:

$W_3 U W_3^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	U	W	V	S	L	I	K	J	F	H	G	E	Y	X	T	Q	P	Z	D	O	A	C	B	N	M	R
b	P	U	Y	E	D	T	V	I	H	S	N	Z	O	K	M	A	R	Q	J	F	B	G	X	W	C	L
c	E	I	Q	G	A	K	D	T	B	M	F	R	J	P	X	N	C	L	V	H	Z	S	Y	O	W	U
d	M	H	P	F	X	D	Y	B	N	T	U	S	A	I	R	C	W	O	L	J	K	Z	Q	E	G	V
e	T	L	D	C	U	J	N	X	S	F	O	B	V	G	K	Q	P	W	I	A	E	M	R	H	Z	Y
f	H	P	L	V	Q	T	X	A	M	Z	W	C	I	U	S	B	E	Y	O	F	N	D	K	G	R	J
g	G	J	O	N	V	P	A	M	R	B	Q	X	H	D	C	F	K	I	Z	U	T	E	Y	L	W	S
h	M	E	H	Z	B	Y	T	C	L	X	V	I	A	W	Q	R	O	P	U	G	S	K	N	J	F	D
i	D	C	B	A	R	H	S	F	Z	Q	O	N	Y	L	K	U	J	E	G	X	P	W	V	T	M	I
j	S	D	I	B	W	N	X	U	C	P	Z	V	O	F	M	J	Y	T	A	R	H	L	E	G	Q	K
k	U	S	J	Y	V	R	I	W	G	C	L	K	T	Q	X	Z	N	F	B	M	A	E	H	O	D	P
l	Q	G	V	T	X	I	B	Y	F	R	N	P	Z	K	W	L	A	J	U	D	S	C	O	E	H	M
m	X	F	Y	G	U	B	D	R	O	S	T	N	Q	L	I	V	M	H	J	K	E	P	Z	A	C	W
n	I	D	X	B	K	S	W	Q	A	M	E	R	J	U	T	Y	H	L	F	O	N	Z	G	C	P	V
o	V	H	K	N	J	M	U	B	S	E	C	Y	F	D	R	Z	T	O	I	Q	G	A	X	W	L	P
p	E	M	L	Z	A	I	J	X	F	G	S	C	B	V	Y	Q	P	U	K	W	R	N	T	H	O	D
q	W	J	Y	S	Q	T	L	N	Z	B	U	G	X	H	P	O	E	V	D	F	K	R	A	M	C	I
r	K	V	I	Q	O	X	N	S	C	M	A	Z	J	G	E	R	D	P	H	U	T	B	Y	F	W	L
s	M	I	J	V	Y	H	K	F	B	C	G	Q	A	W	R	S	L	O	P	Z	X	D	N	U	E	T
t	D	T	P	A	N	L	V	X	W	R	O	F	U	E	K	C	Y	J	Z	B	M	G	I	H	Q	S
u	C	Y	A	U	Q	J	X	R	L	F	Z	I	T	O	N	W	E	H	V	M	D	S	P	G	B	K
v	F	C	B	X	V	A	I	Q	G	K	J	S	P	Z	W	M	H	Y	L	U	T	E	O	D	R	N
w	X	L	V	I	Z	O	R	M	D	P	Y	B	H	W	F	J	T	G	U	Q	S	C	N	A	K	E
x	D	P	Z	A	K	R	M	V	U	S	E	N	G	L	Q	B	O	F	J	W	I	H	T	Y	X	C
y	W	D	N	B	M	P	U	Y	J	I	Z	R	E	C	V	F	S	L	Q	X	G	O	A	T	H	K
z	K	H	R	J	W	Y	I	B	G	D	A	T	Q	V	U	Z	M	C	X	L	O	N	E	S	F	P

Vergleicht man die beiden Tabellen für die Tage X und Y miteinander, erkennt man eine Lösung bei der Variante n, welche idente Ausdrücke für die dritte Walze liefert. Diese Lösung n entspricht der richtigen Verdrahtungsvariante der ersten Walze W_1, die nun aufgrund der Schlüsselunterlagen auch als Walze I identifiziert werden kann, für W_{1n} findet man:

W_I	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J

Mit den Schlüsselunterlagen vom Oktober kann auf gleiche Weise die korrekte Verdrahtungsvariante für die zweite Walze bestimmt werden, welche lautet:

W_{II}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E

Angenommen, in den Geheimunterlagen von September oder Oktober 1932 seien in einem der beiden Monate vier Tage mit Grundstellungen mit für die dritte Walze fortlaufenden Drehstellungen oder zumindest Drehstellungen mit gleichbleibenden Abständen enthalten gewesen. Man hätte demnach im September folgende Einstellungen vorgefunden:

Monat September: Walzenlage III-II-I und Ringstellung 01-01-01

Tag 1: Grundstellung 01-01-01
Steckerverbindungen (BE)(RS)(KD)(WM)(CX)(PQ)

Tag 2: Grundstellung 02-02-02
Steckerverbindungen (AB)(CD)(EF)(GH)(IJ)(KL)

Tag 3: Grundstellung 03-03-03
Steckerverbindungen (MN)(OP)(QR)(ST)(UV)(WX)

Tag 4: Grundstellung 04-04-04
Steckerverbindungen (CR)(DJ)(EK)(FZ)(GP)(HW)

Für diese Tage hätte man weiters folgende Stellentransformationen durch Erraten von Spruchschlüssel gefunden:

$Stelle_{1\_T1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T

$Stelle_{1\_T2}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	W	P	E	Z	C	M	T	V	O	L	S	J	F	Y	I	B	X	U	K	G	R	H	A	Q	N	D

$Stelle_{1\_T3}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	X	S	T	H	Q	N	W	D	K	O	I	Z	R	F	J	V	E	M	B	C	Y	P	G	A	U	L

$Stelle_{1\_T4}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	T	Y	F	N	I	C	Z	J	E	H	P	O	V	D	L	K	W	U	X	A	R	M	Q	S	B	G

Für diese vier Stellentransformationen gilt folgendes Gleichungssystem:

$$Stelle_{1\_T1} = S_1\ D\ W_I\ D^{-1}\ W_{II}\ W_{III}\ U\ W_{III}^{-1}\ W_{II}^{-1}\ D\ W_I^{-1}\ D^{-1}\ S_1^{-1}$$
$$Stelle_{1\_T2} = S_2\ D\ W_I\ D^{-1}\ W_{II}\ W_{III}\ U\ W_{III}^{-1}\ W_{II}^{-1}\ D\ W_I^{-1}\ D^{-1}\ S_2^{-1}$$
$$Stelle_{1\_T3} = S_3\ D\ W_I\ D^{-1}\ W_{II}\ W_{III}\ U\ W_{III}^{-1}\ W_{II}^{-1}\ D\ W_I^{-1}\ D^{-1}\ S_3^{-1}$$
$$Stelle_{1\_T4} = S_4\ D\ W_I\ D^{-1}\ W_{II}\ W_{III}\ U\ W_{III}^{-1}\ W_{II}^{-1}\ D\ W_I^{-1}\ D^{-1}\ S_4^{-1}$$

Im Allgemeinen gelten für Permutationen folgende Beziehungen:

$$(D\,W\,D^{-1})^{-1} = D\,W^{-1}\,D^{-1} \quad \text{bzw.} \quad (D^2\,W\,D^{-2})^{-1} = D^2\,W^{-1}\,D^{-2} \quad \text{usw.}$$

Da die einzelnen Grundstellungen zwar unterschiedlich, aber bekannt sind, können alle auf eine Grundstellung zurückgeführt werden. Im vorliegenden Beispiel sind die Grundstellungen für jede Walze um jeweils eine Position weitergedreht:

$$\text{Stelle}_{1\_T1} = S_1\,D\,W_I\,D^{-1}\,W_{II}\,W_{III}\,U\,W_{III}^{-1}\,W_{II}^{-1}\,D\,W_I^{-1}\,D^{-1}\,S_1^{-1}$$
$$\text{Stelle}_{1\_T2} = S_2\,D^2\,W_I\,D^{-2}\,D\,W_{II}\,D^{-1}\,D\,W_{III}\,D^{-1}\,U\,D\,W_{III}^{-1}\,D^{-1}\,D\,W_{II}^{-1}\,D^{-1}\,D^2\,W_I^{-1}\,D^{-2}\,S_2^{-1}$$
$$\text{Stelle}_{1\_T3} = S_3\,D^3\,W_I\,D^{-3}\,D^2\,W_{II}\,D^{-2}\,D^2\,W_{III}\,D^{-2}\,U\,D^2\,W_{III}^{-1}\,D^{-2}\,D^2\,W_{II}^{-1}\,D^{-2}\,D^3\,W_I^{-1}\,D^{-3}\,S_3^{-1}$$
$$\text{Stelle}_{1\_T4} = S_4\,D^4\,W_I\,D^{-4}\,D^3\,W_{II}\,D^{-3}\,D^3\,W_{III}\,D^{-3}\,U\,D^3\,W_{III}^{-1}\,D^{-3}\,D^3\,W_{II}^{-1}\,D^{-3}\,D^4\,W_I^{-1}\,D^{-4}\,S_4^{-1}$$

Nach Eliminierung der trivialen Permutationen erhält man:

$$\text{Stelle}_{1\_T1} = S_1\,D\,W_I\,D^{-1}\,W_{II}\,W_{III}\,U\,W_{III}^{-1}\,W_{II}^{-1}\,D\,W_I^{-1}\,D^{-1}\,S_1^{-1}$$
$$\text{Stelle}_{1\_T2} = S_2\,D^2\,W_I\,D^{-1}\,W_{II}\,W_{III}\,D^{-1}\,U\,D\,W_{III}^{-1}\,W_{II}^{-1}\,D\,W_I^{-1}\,D^{-2}\,S_2^{-1}$$
$$\text{Stelle}_{1\_T3} = S_3\,D^3\,W_I\,D^{-1}\,W_{II}\,W_{III}\,D^{-2}\,U\,D^2\,W_{III}^{-1}\,W_{II}^{-1}\,D\,W_I^{-1}\,D^{-3}\,S_3^{-1}$$
$$\text{Stelle}_{1\_T4} = S_4\,D^4\,W_I\,D^{-1}\,W_{II}\,W_{III}\,D^{-3}\,U\,D^3\,W_{III}^{-1}\,W_{II}^{-1}\,D\,W_I^{-1}\,D^{-4}\,S_4^{-1}$$

Nach Umformung der Ausdrücke und Abkürzung mit Z erhält man:

$$Z_1 = W_{III}\,U\,W_{III}^{-1} = W_{II}^{-1}\,D\,W_I^{-1}\,D^{-1}\,S_1^{-1}\;\text{Stelle}_{1\_T1}\,S_1\,D\,W_I\,D^{-1}\,W_{II}$$
$$Z_2 = W_{III}\,D^{-1}\,U\,D\,W_{III}^{-1} = W_{II}^{-1}\,D\,W_I^{-1}\,D^{-2}\,S_2^{-1}\;\text{Stelle}_{1\_T2}\,S_2\,D^2\,W_I\,D^{-1}\,W_{II}$$
$$Z_3 = W_{III}\,D^{-2}\,U\,D^2\,W_{III}^{-1} = W_{II}^{-1}\,D\,W_I^{-1}\,D^{-3}\,S_3^{-1}\;\text{Stelle}_{1\_T3}\,S_3\,D^3\,W_I\,D^{-1}\,W_{II}$$
$$Z_4 = W_{III}\,D^{-3}\,U\,D^3\,W_{III}^{-1} = W_{II}^{-1}\,D\,W_I^{-1}\,D^{-4}\,S_4^{-1}\;\text{Stelle}_{1\_T4}\,S_4\,D^4\,W_I\,D^{-1}\,W_{II}$$

Analog zu den normierten Transformationen T, die alle auf eine bestimmte Maschineneinstellung Bezug nehmen, sind auch die normierten Transformationen Z alle auf eine Stellung, hier etwa auf die Grundstellung 01-01-01, ausgerichtet.

Das Ziel in der weiteren Umformung ist es wiederum, die unbekannte, aber konstante Umkehrwalze U aus den Gleichungen zu eliminieren, um die Verdrahtung der noch fehlenden dritten Walze berechnen zu können. Dazu bildet man nacheinander Produkte der einzelnen Transformationen Z und fasst die Gleichungen zusammen:

$$Z_1\,Z_2 = W_{III}\,U\,W_{III}^{-1}\,W_{III}\,D^{-1}\,U\,D\,W_{III}^{-1} = W_{III}\,(U\,D^{-1}\,U\,D)\,W_{III}^{-1}$$
$$Z_2\,Z_3 = W_{III}\,D^{-1}\,U\,D\,W_{III}^{-1}\,W_{III}\,D^{-2}\,U\,D^2\,W_{III}^{-1} = W_{III}\,D^{-1}\,(U\,D^{-1}\,U\,D)\,D\,W_{III}^{-1}$$
$$Z_3\,Z_4 = W_{III}\,D^{-2}\,U\,D^2\,W_{III}^{-1}\,W_{III}\,D^{-3}\,U\,D^3\,W_{III}^{-1} = W_{III}\,D^{-2}\,(U\,D^{-1}\,U\,D)\,D^2\,W_{III}^{-1}$$

Dabei spielen die jeweiligen Grundstellungen der vier Tage für die erste und zweite Walze keine Rolle mehr. In den Gleichungen kann der Term mit der Umkehrwalze eliminiert werden:

$$Z_1 Z_2 = W_{III} (U D^{-1} U D) W_{III}^{-1} = W_{III} D W_{III}^{-1} Z_2 Z_3 W_{III} D^{-1} W_{III}^{-1}$$
$$Z_1 Z_2 = (W_{III} D W_{III}^{-1}) Z_2 Z_3 (W_{III} D W_{III}^{-1})^{-1}$$
$$Z_2 Z_3 = (W_{III} D W_{III}^{-1}) Z_3 Z_4 (W_{III} D W_{III}^{-1})^{-1}$$

Mit Hilfe der bereits berechneten Walzen W_I und W_{II} sowie den ebenso bekannten Stellentransformationen können die jeweiligen Z–Terme berechnet werden:

$$Z_1 = W_{III} U W_{III}^{-1} = W_{II}^{-1} D W_I^{-1} D^{-1} S_1^{-1} Stelle_{1\_T1} S_1 D W_I D^{-1} W_{II}$$

W_{II}^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	J	P	C	Z	W	R	L	F	B	D	K	O	T	Y	U	Q	G	E	N	H	X	M	I	V	S
D	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
W_I^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	U	W	Y	G	A	D	F	P	V	Z	B	E	C	K	M	T	H	X	S	L	R	I	N	Q	O	J
D^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
S_1^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
$Stelle_{1\_T1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T
S_1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	E	X	K	B	F	G	H	I	J	D	L	W	N	O	Q	P	S	R	T	U	V	M	C	Y	Z
D	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
W_I	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
D^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
W_{II}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
Z_1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	I	D	X	B	K	S	W	Q	A	M	E	R	J	U	T	Y	H	L	F	O	N	Z	G	C	P	V

Ebenso findet man für den zweiten Term:

$$Z_2 = W_{III}\, D^{-1}\, U\, D\, W_{III}^{-1} = W_{II}^{-1}\, D\, W_I^{-1}\, D^{-2}\, S_2^{-1}\, Stelle_{1\_T2}\, S_2\, D^2\, W_I\, D^{-1}\, W_{II}$$

W_{II}^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	J	P	C	Z	W	R	L	F	B	D	K	O	T	Y	U	Q	G	E	N	H	X	M	I	V	S
D	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
W_I^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	U	W	Y	G	A	D	F	P	V	Z	B	E	C	K	M	T	H	X	S	L	R	I	N	Q	O	J
D^{-2}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
S_2^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	A	D	C	F	E	H	G	J	I	L	K	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$Stelle_{1\_T2}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	W	P	E	Z	C	M	T	V	O	L	S	J	F	Y	I	B	X	U	K	G	R	H	A	Q	N	D
S_2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	A	D	C	F	E	H	G	J	I	L	K	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D^2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
W_I	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
D^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
W_{II}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
Z_2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	M	L	I	V	Y	Z	X	N	C	S	R	B	A	H	U	Q	P	K	J	W	O	D	T	G	E	F

Und für die restlichen beiden Terme ergibt sich analog:

$$Z_3 = W_{III}\, D^{-2}\, U\, D^2\, W_{III}^{-1} = W_{II}^{-1}\, D\, W_I^{-1}\, D^{-3}\, S_3^{-1}\, Stelle_{1\_T3}\, S_3\, D^3\, W_I\, D^{-1}\, W_{II}$$

$$Z_4 = W_{III}\, D^{-3}\, U\, D^3\, W_{III}^{-1} = W_{II}^{-1}\, D\, W_I^{-1}\, D^{-4}\, S_4^{-1}\, Stelle_{1\_T4}\, S_4\, D^4\, W_I\, D^{-1}\, W_{II}$$

Z_3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	L	J	E	W	C	M	T	V	U	B	O	A	F	Q	K	R	N	P	X	G	I	H	D	S	Z	Y

Z_4	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	A	K	J	Z	X	R	I	H	D	C	Q	O	Y	M	W	L	G	U	V	S	T	P	F	N	E

Die resultierenden Produkte lauten:

Z_1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	I	D	X	B	K	S	W	Q	A	M	E	R	J	U	T	Y	H	L	F	O	N	Z	G	C	P	V
Z_2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	M	L	I	V	Y	Z	X	N	C	S	R	B	A	H	U	Q	P	K	J	W	O	D	T	G	E	F
$Z_1 Z_2$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	C	V	G	L	R	J	T	P	M	A	Y	K	S	O	W	E	N	B	Z	U	H	F	X	I	Q	D

bzw.

$Z_2 Z_3$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	A	U	H	Z	Y	S	Q	E	X	P	J	L	V	I	N	R	O	B	D	K	W	G	T	C	M

$Z_3 Z_4$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Q	D	Z	P	K	O	V	T	S	A	M	B	X	L	C	G	Y	W	F	R	H	I	J	U	E	N

Die entsprechenden Zyklen der Produkte können einfach abgelesen werden:

$Z_1 Z_2$ = (ACGTUHPERBVFJ) (DLKYQNOWXIMSZ)
$Z_2 Z_3$ = (AFYCUKPNVWGSB) (DHQROIEZMLJXT)
$Z_3 Z_4$ = (AQYEKMXUHTRWJ) (BDPGVISFOCZNL)

Die Zyklen der Produkte haben alle die gleiche Struktur, sie bestehen alle aus je zwei Zyklen der Länge 13. Da die normierten Transformationen Z aber alle dem gleichen Verdrahtungszustand entstammen, müssen alle Buchstabentransformationen der Produkte identisch zueinander sein. Man versucht nun wieder durch geschicktes Untereinanderschreiben der Zyklen diese konsistent zueinander auszurichten:

$Z_1 Z_2$ = (Q N O W X I M S Z D L K Y) (R B V F J A C G T U H P E)
$Z_2 Z_3$ = (E Z M L J X T D H Q R O I) (K P N V W G S B A F Y C U)
$Z_3 Z_4$ = (U H T R W J A Q Y E K M X) (O C Z N L B D P G V I S F)

Mit der Beziehung

$$Z_1 Z_2 = W_{III} (U D^{-1} U D) W_{III}^{-1} = (W_{III} D W_{III}^{-1}) Z_2 Z_3 (W_{III} D W_{III}^{-1})^{-1}$$

folgt schließlich für den Term mit der dritten Walze:

$$(W_{III} D W_{III}^{-1}) = (QEUFVNZHYIXJWLRKOMTAGBPCSD)$$

Für die Lösung von W_{III} ergeben sich wieder 26 verschiedene mögliche Verdrahtungsmuster, deren jedes einer Weiterdrehung um eine Drehposition entspricht:

W_{IIIa}	Q	E	U	F	V	N	Z	H	Y	I	X	J	W	L	R	K	O	M	T	A	G	B	P	C	S	D
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

W_{IIIb}	Q	E	U	F	V	N	Z	H	Y	I	X	J	W	L	R	K	O	M	T	A	G	B	P	C	S	D
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Nach Ordnen der Buchstaben der ersten Zeile in alphabetischer Reihenfolge findet man folgende 26 möglichen Verdrahtungsmuster:

W_{III}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	T	V	X	Z	B	D	U	H	J	L	P	N	R	F	Q	W	A	O	Y	S	C	E	M	K	I	G
b	U	W	Y	A	C	E	V	I	K	M	Q	O	S	G	R	X	B	P	Z	T	D	F	N	L	J	H
c	V	X	Z	B	D	F	W	J	L	N	R	P	T	H	S	Y	C	Q	A	U	E	G	O	M	K	I
d	W	Y	A	C	E	G	X	K	M	O	S	Q	U	I	T	Z	D	R	B	V	F	H	P	N	L	J
e	X	Z	B	D	F	H	Y	L	N	P	T	R	V	J	U	A	E	S	C	W	G	I	Q	O	M	K
f	Y	A	C	E	G	I	Z	M	O	Q	U	S	W	K	V	B	F	T	D	X	H	J	R	P	N	L
g	Z	B	D	F	H	J	A	N	P	R	V	T	X	L	W	C	G	U	E	Y	I	K	S	Q	O	M
h	A	C	E	G	I	K	B	O	Q	S	W	U	Y	M	X	D	H	V	F	Z	J	L	T	R	P	N
i	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
j	C	E	G	I	K	M	D	Q	S	U	Y	W	A	O	Z	F	J	X	H	B	L	N	V	T	R	P
k	D	F	H	J	L	N	E	R	T	V	Z	X	B	P	A	G	K	Y	I	C	M	O	W	U	S	Q
l	E	G	I	K	M	O	F	S	U	W	A	Y	C	Q	B	H	L	Z	J	D	N	P	X	V	T	R
m	F	H	J	L	N	P	G	T	V	X	B	Z	D	R	C	I	M	A	K	E	O	Q	Y	W	U	S
n	G	I	K	M	O	Q	H	U	W	Y	C	A	E	S	D	J	N	B	L	F	P	R	Z	X	V	T
o	H	J	L	N	P	R	I	V	X	Z	D	B	F	T	E	K	O	C	M	G	Q	S	A	Y	W	U
p	I	K	M	O	Q	S	J	W	Y	A	E	C	G	U	F	L	P	D	N	H	R	T	B	Z	X	V
q	J	L	N	P	R	T	K	X	Z	B	F	D	H	V	G	M	Q	E	O	I	S	U	C	A	Y	W
r	K	M	O	Q	S	U	L	Y	A	C	G	E	I	W	H	N	R	F	P	J	T	V	D	B	Z	X
s	L	N	P	R	T	V	M	Z	B	D	H	F	J	X	I	O	S	G	Q	K	U	W	E	C	A	Y
t	M	O	Q	S	U	W	N	A	C	E	I	G	K	Y	J	P	T	H	R	L	V	X	F	D	B	Z
u	N	P	R	T	V	X	O	B	D	F	J	H	L	Z	K	Q	U	I	S	M	W	Y	G	E	C	A
v	O	Q	S	U	W	Y	P	C	E	G	K	I	M	A	L	R	V	J	T	N	X	Z	H	F	D	B
w	P	R	T	V	X	Z	Q	D	F	H	L	J	N	B	M	S	W	K	U	O	Y	A	I	G	E	C
x	Q	S	U	W	Y	A	R	E	G	I	M	K	O	C	N	T	X	L	V	P	Z	B	J	H	F	D
y	R	T	V	X	Z	B	S	F	H	J	N	L	P	D	O	U	Y	M	W	Q	A	C	K	I	G	E
z	S	U	W	Y	A	C	T	G	I	K	O	M	Q	E	P	V	Z	N	X	R	B	D	L	J	H	F

Nach der Berechnung des Verdrahtungsmusters der dritten Walze bleibt noch, die richtige Drehposition dieser Walze zu bestimmen. Dazu vergleicht man zwei Stellentransformationen von je einem Tag im September und Oktober miteinander, da diese unterschiedlichen Walzenlagen für die dritte Walze entspringen.

Beispielsweise findet man durch Erraten von Spruchschlüsseln im September die erste Stellentransformation, wobei die Schlüsseleinstellung Walzenlage III-II-I, Ringstellung 01-01-01, Steckerverbindungen (BE)(RS)(KD)(WM)(CX)(PQ) und Grundstellung 01-01-01 vorgegeben sind:

$Stelle_{1\_T1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T

Im Oktober wäre beispielsweise mit der Schlüsseleinstellung Walzenlage I-III-II, Ringstellung 01-01-01, Steckerverbindungen (AB)(CD)(EF)(GH)(IJ)(KL) und Grundstellung 01-01-06 folgende Stellentransformation gefunden:

$Stelle_{1\_T2}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	S	O	J	L	W	X	H	G	Q	C	U	D	V	P	B	N	I	Z	A	Y	K	M	E	F	T	R

Im September gilt:

$$U = W_{III}^{-1}\, W_{II}^{-1}\, D\, W_{I}^{-1}\, D^{-1}\, S_1^{-1}\, Stelle_{1\_T1}\, S_1\, D\, W_I\, D^{-1}\, W_{II}\, W_{III}$$

Im Oktober – die rechte Walze ist gemäß der Grundstellung um sechs Drehpositionen gegenüber jener vom September weitergedreht – gilt entsprechend:

$$U = W_{III}^{-1}\, W_{II}^{-1}\, D^{7}\, W_{I}^{-1}\, D^{-7}\, S_2^{-1}\, Stelle_{1\_T2}\, S_2\, D^{7}\, W_I\, D^{-7}\, W_{II}\, W_{III}$$

Beide Ausdrücke müssen aber dasselbe Ergebnis liefern, da jeweils die konstante Umkehrwalze auf der linken Seite der Gleichungen vorkommt, wenn man nacheinander alle 26 Möglichkeiten für die dritte Walze W_{III} für den Monat September einsetzt:

$$U_a = W_{IIIa}^{-1}\, W_{II}^{-1}\, D\, W_{I}^{-1}\, D^{-1}\, S_1^{-1}\, Stelle_{1\_T1}\, S_1\, D\, W_I\, D^{-1}\, W_{II}\, W_{IIIa}$$
$$U_b = W_{IIIb}^{-1}\, W_{II}^{-1}\, D\, W_{I}^{-1}\, D^{-1}\, S_1^{-1}\, Stelle_{1\_T1}\, S_1\, D\, W_I\, D^{-1}\, W_{II}\, W_{IIIb}$$

usw.

Und analog für den Monat Oktober erhält man:

$$U_a = W_{IIIa}^{-1}\, W_{II}^{-1}\, D^{7}\, W_{I}^{-1}\, D^{-7}\, S_2^{-1}\, Stelle_{1\_T2}\, S_2\, D^{7}\, W_I\, D^{-7}\, W_{II}\, W_{IIIa}$$
$$U_b = W_{IIIb}^{-1}\, W_{II}^{-1}\, D^{7}\, W_{I}^{-1}\, D^{-7}\, S_2^{-1}\, Stelle_{1\_T2}\, S_2\, D^{7}\, W_I\, D^{-7}\, W_{II}\, W_{IIIb}$$

usw.

Nach Berechnung aller Varianten findet man im September für die gesuchte Umkehrwalze U:

U	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	H	P	F	Y	G	C	E	A	W	T	X	R	U	O	N	B	S	L	Q	J	M	Z	I	K	D	V
b	W	I	Q	G	Z	H	D	F	B	X	U	Y	S	V	P	O	C	T	M	R	K	N	A	J	L	E
c	F	X	J	R	H	A	I	E	G	C	Y	V	Z	T	W	Q	P	D	U	N	S	L	O	B	K	M
d	N	G	Y	K	S	I	B	J	F	H	D	Z	W	A	U	X	R	Q	E	V	O	T	M	P	C	L
e	M	O	H	Z	L	T	J	C	K	G	I	E	A	X	B	V	Y	S	R	F	W	P	U	N	Q	D
f	E	N	P	I	A	M	U	K	D	L	H	J	F	B	Y	C	W	Z	T	S	G	X	Q	V	O	R
g	S	F	O	Q	J	B	N	V	L	E	M	I	K	G	C	Z	D	X	A	U	T	H	Y	R	W	P
h	Q	T	G	P	R	K	C	O	W	M	F	N	J	L	H	D	A	E	Y	B	V	U	I	Z	S	X
i	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T
j	U	Z	S	V	I	R	T	M	E	Q	Y	O	H	P	L	N	J	F	C	G	A	D	X	W	K	B
k	C	V	A	T	W	J	S	U	N	F	R	Z	P	I	Q	M	O	K	G	D	H	B	E	Y	X	L
l	M	D	W	B	U	X	K	T	V	O	G	S	A	Q	J	R	N	P	L	H	E	I	C	F	Z	Y
m	Z	N	E	X	C	V	Y	L	U	W	P	H	T	B	R	K	S	O	Q	M	I	F	J	D	G	A
n	B	A	O	F	Y	D	W	Z	M	V	X	Q	I	U	C	S	L	T	P	R	N	J	G	K	E	H
o	I	C	B	P	G	Z	E	X	A	N	W	Y	R	J	V	D	T	M	U	Q	S	O	K	H	L	F
p	G	J	D	C	Q	H	A	F	Y	B	O	X	Z	S	K	W	E	U	N	V	R	T	P	L	I	M
q	N	H	K	E	D	R	I	B	G	Z	C	P	Y	A	T	L	X	F	V	O	W	S	U	Q	M	J
r	K	O	I	L	F	E	S	J	C	H	A	D	Q	Z	B	U	M	Y	G	W	P	X	T	V	R	N
s	O	L	P	J	M	G	F	T	K	D	I	B	E	R	A	C	V	N	Z	H	X	Q	Y	U	W	S
t	T	P	M	Q	K	N	H	G	U	L	E	J	C	F	S	B	D	W	O	A	I	Y	R	Z	V	X
u	Y	U	Q	N	R	L	O	I	H	V	M	F	K	D	G	T	C	E	X	P	B	J	Z	S	A	W
v	X	Z	V	R	O	S	M	P	J	I	W	N	G	L	E	H	U	D	F	Y	Q	C	K	A	T	B
w	C	Y	A	W	S	P	T	N	Q	K	J	X	O	H	M	F	I	V	E	G	Z	R	D	L	B	U
x	V	D	Z	B	X	T	Q	U	O	R	L	K	Y	P	I	N	G	J	W	F	H	A	S	E	M	C
y	D	W	E	A	C	Y	U	R	V	P	S	M	L	Z	Q	J	O	H	K	X	G	I	B	T	F	N
z	O	E	X	F	B	D	Z	V	S	W	Q	T	N	M	A	R	K	P	I	L	Y	H	J	C	U	G

Für den Monat Oktober findet man analog:

U	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	L	R	Q	O	G	K	E	Y	N	S	F	A	P	I	D	M	C	B	J	W	V	U	T	Z	H	X
b	F	T	R	K	P	A	I	X	G	V	D	M	L	U	Y	E	W	C	Z	B	N	J	Q	H	O	S
c	K	D	J	B	Z	G	F	W	L	C	A	I	Q	P	R	N	M	O	T	S	X	Y	H	U	V	E
d	T	G	W	L	J	V	B	Z	M	E	N	D	I	K	P	O	R	Q	U	A	S	F	C	Y	X	H
e	W	F	V	R	K	B	Q	U	O	Y	E	Z	T	X	I	S	G	D	P	M	H	C	A	N	J	L
f	P	W	Q	V	H	O	N	E	Y	Z	M	R	K	G	F	A	C	L	X	U	T	D	B	S	I	J
g	I	H	G	T	N	M	C	B	A	V	X	W	F	E	S	U	Z	Y	O	D	P	J	L	K	R	Q
h	S	I	H	J	Z	L	Y	C	B	D	T	F	U	V	Q	W	O	X	A	K	M	N	P	R	G	E
i	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T
j	B	A	R	G	U	W	D	I	H	S	V	P	T	O	N	L	X	C	J	M	E	K	F	Q	Z	Y
k	G	X	J	Q	P	O	A	N	R	C	S	Y	Z	H	F	E	D	I	K	W	V	U	T	B	L	M
l	K	C	B	I	J	N	H	G	D	E	A	W	P	F	Y	M	V	U	Z	X	R	Q	L	T	O	S
m	F	Q	S	X	K	A	Y	W	M	R	E	T	I	P	U	N	B	J	C	L	O	Z	H	D	G	V
n	T	F	E	H	C	B	O	D	L	P	M	I	K	Z	G	J	U	V	W	A	Q	R	S	Y	X	N
o	E	G	Z	W	A	M	B	U	O	K	J	R	F	T	I	Y	X	L	V	N	H	S	D	Q	P	C
p	H	W	G	R	M	L	C	A	K	N	I	F	E	J	T	Z	Y	D	X	O	V	U	B	S	Q	P
q	N	M	Q	J	T	K	L	V	X	D	F	G	B	A	W	U	C	Y	Z	E	P	H	O	I	R	S
r	S	U	H	G	Q	R	D	C	T	V	O	M	L	P	K	N	E	F	A	I	B	J	Y	Z	W	X
s	T	O	L	Q	Z	G	F	Y	P	X	V	C	W	U	B	I	D	S	R	A	N	K	M	J	H	E
t	B	A	P	L	U	Y	J	X	O	G	N	D	Z	K	I	C	V	W	T	S	E	Q	R	H	F	M
u	J	W	Y	E	D	N	Q	L	R	A	S	H	T	F	P	O	G	I	K	M	X	Z	B	U	C	V
v	W	C	B	V	I	O	X	J	E	H	Q	T	P	Z	F	M	K	Y	U	L	S	D	A	G	R	N
w	F	K	H	U	X	A	O	C	Y	R	B	W	V	T	G	S	Z	J	P	N	D	M	L	E	I	Q
x	P	H	E	W	C	Z	Y	B	L	X	U	I	R	V	T	A	S	M	Q	O	K	N	D	J	G	F
y	I	G	F	H	U	C	B	D	A	K	J	N	S	L	W	V	Y	X	M	Z	E	P	O	R	Q	T
z	Z	I	U	R	M	P	T	V	B	L	S	J	E	O	N	F	X	D	K	G	C	H	Y	Q	W	A

Eine Übereinstimmung für die Umkehrwalze in den beiden Lösungssätzen für die Monate September und Oktober findet man in der Zeile i, die nicht nur für die Umkehrwalze, sondern auch gleich für die dritte Walze das richtige Verdrahtungsmuster liefert:

U_B	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T

W_{III}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O

Im hier gezeigten Beispiel findet man die Verdrahtung für die Umkehrwalze B. Bis November 1937 ist jedoch die Umkehrwalze A im Einsatz, die mit den Unterlagen von September und Oktober 1932 von Rejewski berechnet wird.

Aufgrund der Angaben in den Unterlagen von September und Oktober 1932 ist mit den Tageseinstellungen auch die jeweilige Ringstellung bekannt. Wenn die Berechnung der Walzen nicht bei der beispielhaften Ringstellung 01-01-01 durchgeführt wird, sondern beispielsweise bei einer Ringstellung 01-03-05, so findet man als richtige Verdrahtungsvariante für die erste Walze anstatt der Lösung n jene um vier Stellen verschobene für j, welche nun – mit der Ringstellung 05 der ersten Walze nachjustiert – wieder die richtige Lösung n ergibt.

Die Überträge der Walzen können nun relativ einfach durch Dechiffrierung einzelner Funksprüche zu den gegebenen Quartalen 1932 gewonnen werden. Solange kein Übertrag stattfindet, ergibt sich aus den Chiffren Klartext, die ab einer Stelle wo ein Übertrag vorkommt, in Chiffren übergehen. Erst nach Weiterrücken der zweiten bzw. der dritten Walze um eine Stelle entsteht wieder Klartext.

Die einzelnen Überträge für die Walzen können somit an folgenden Drehstellungen identifiziert werden:

Walze I:	Übertrag bei 17 auf 18
Walze II:	Übertrag bei 05 auf 06
Walze III:	Übertrag bei 22 auf 23

09
08
07
06
05
04
03
13365

Metoda rusztu – Rejewskis Rastermethode

Anfang 1933 hat Rejewski alle Teile der Enigma rekonstruiert und es kann ein Nachbau veranlasst werden. Damit hat man eine vollständige Maschine zur Verfügung, die für die Entschlüsselung der Tageseinstellungen benutzt werden kann.

In der mathematischen Beschreibung der Enigma für eine Stelle sind nun alle inneren Teile der Maschine bekannt, aber alle Größen der Tageseinstellung sind Unbekannte, nämlich die Walzenlage, die Ringstellung, die Steckerverbindungen und die Grundstellung:

$$\text{Stelle} = S\,(D^{x}\,W_1\,D^{-x})\,W_2\,W_3\,U\,W_3^{-1}\,W_2^{-1}\,(D^{x}\,W_1\,D^{-x})^{-1}\,S^{-1}$$

Dabei stellt nun D^{x} eine unbekannte Drehstellung der ersten Walze dar, also eine unbekannte Permutation des Alphabets. Da vorerst auch die Walzenlage nicht gegeben ist, kann jede der drei Walzen W_I, W_{II} und W_{III} in jeder Lage vorkommen.

Die Ringstellung erzeugt nur eine relative Verschiebung zur eingestellten Grundstellung des Tages, weshalb in obiger Beziehung die effektive Drehstellung der Walzen vorausgesetzt ist. Wird eine effektive Drehstellung berechnet, ergibt sich die eingestellte Grundstellung wiederum einfach aus der Verschiebung der effektiven Grundstellung um die jeweilige Ringstellung.

51 *Die Reihenfolge der Walzen schlägt sich in den Transformationen des Tages nieder.*

Berechnet man nun alle 26 Möglichkeiten des Ausdrucks ($D^{x} W_I D^{-x}$) für die Walze W_I erhält man folgende Tabelle:

$D^{x} W_I D^{-x}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	J	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T	R	O	Z	H	A	Q	B	I	D
2	K	D	J	E	B	O	T	X	L	R	M	U	W	F	V	S	Q	N	Y	G	Z	P	A	H	C	I
3	C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R	P	M	X	F	Y	O	Z	G	B	H	J
4	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q	O	L	W	E	X	N	Y	F	A	G	I	B
5	B	Y	L	Q	U	I	O	J	R	T	C	S	P	N	K	V	D	W	M	X	E	Z	F	H	A	G
6	X	K	P	T	H	N	I	Q	S	B	R	O	M	J	U	C	V	L	W	D	Y	E	G	Z	F	A
7	J	O	S	G	M	H	P	R	A	Q	N	L	I	T	B	U	K	V	C	X	D	F	Y	E	Z	W
8	N	R	F	L	G	O	Q	Z	P	M	K	H	S	A	T	J	U	B	W	C	E	X	D	Y	V	I
9	Q	E	K	F	N	P	Y	O	L	J	G	R	Z	S	I	T	A	V	B	D	W	C	X	U	H	M
10	D	J	E	M	O	X	N	K	I	F	Q	Y	R	H	S	Z	U	A	C	V	B	W	T	G	L	P
11	I	D	L	N	W	M	J	H	E	P	X	Q	G	R	Y	T	Z	B	U	A	V	S	F	K	O	C
12	C	K	M	V	L	I	G	D	O	W	P	F	Q	X	S	Y	A	T	Z	U	R	E	J	N	B	H
13	J	L	U	K	H	F	C	N	V	O	E	P	W	R	X	Z	S	Y	T	Q	D	I	M	A	G	B
14	K	T	J	G	E	B	M	U	N	D	O	V	Q	W	Y	R	X	S	P	C	H	L	Z	F	A	I
15	S	I	F	D	A	L	T	M	C	N	U	P	V	X	Q	W	R	O	B	G	K	Y	E	Z	H	J
16	H	E	C	Z	K	S	L	B	M	T	O	U	W	P	V	Q	N	A	F	J	X	D	Y	G	I	R
17	D	B	Y	J	R	K	A	L	S	N	T	V	O	U	P	M	Z	E	I	W	C	X	F	H	Q	G
18	A	X	I	Q	J	Z	K	R	M	S	U	N	T	O	L	Y	D	H	V	B	W	E	G	P	F	C
19	W	H	P	I	Y	J	Q	L	R	T	M	S	N	K	X	C	G	U	A	V	D	F	O	E	B	Z
20	G	O	H	X	I	P	K	Q	S	L	R	M	J	W	B	F	T	Z	U	C	E	N	D	A	Y	V
21	N	G	W	H	O	J	P	R	K	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z	X	U	F
22	F	V	G	N	I	O	Q	J	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y	W	T	E	M
23	U	F	M	H	N	P	I	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X	V	S	D	L	E
24	E	L	G	M	O	H	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W	U	R	C	K	D	T
25	K	F	L	N	G	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V	T	Q	B	J	C	S	D
26	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J

Für die Walze W_{II} ergibt sich eine analoge Tabelle:

$D^{x} W_{II} D^{-x}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	I	C	J	R	H	Q	T	W	A	K	G	V	S	L	B	P	F	Y	M	O	X	E	U	N	D	Z
2	B	I	Q	G	P	S	V	Z	J	F	U	R	K	A	O	E	X	L	N	W	D	T	M	C	Y	H
3	H	P	F	O	R	U	Y	I	E	T	Q	J	Z	N	D	W	K	M	V	C	S	L	B	X	G	A
4	O	E	N	Q	T	X	H	D	S	P	I	Y	M	C	V	J	L	U	B	R	K	A	W	F	Z	G
5	D	M	P	S	W	G	C	R	O	H	X	L	B	U	I	K	T	A	Q	J	Z	V	E	Y	F	N
6	L	O	R	V	F	B	Q	N	G	W	K	A	T	H	J	S	Z	P	I	Y	U	D	X	E	M	C
7	N	Q	U	E	A	P	M	F	V	J	Z	S	G	I	R	Y	O	H	X	T	C	W	D	L	B	K
8	P	T	D	Z	O	L	E	U	I	Y	R	F	H	Q	X	N	G	W	S	B	V	C	K	A	J	M
9	S	C	Y	N	K	D	T	H	X	Q	E	G	P	W	M	F	V	R	A	U	B	J	Z	I	L	O
10	B	X	M	J	C	S	G	W	P	D	F	O	V	L	E	U	Q	Z	T	A	I	Y	H	K	N	R
11	W	L	I	B	R	F	V	O	C	E	N	U	K	D	T	P	Y	S	Z	H	X	G	J	M	Q	A
12	K	H	A	Q	E	U	N	B	D	M	T	J	C	S	O	X	R	Y	G	W	F	I	L	P	Z	V
13	G	Z	P	D	T	M	A	C	L	S	I	B	R	N	W	Q	X	F	V	E	H	K	O	Y	U	J
14	Y	O	C	S	L	Z	B	K	R	H	A	Q	M	V	P	W	E	U	D	G	J	N	X	T	I	F
15	N	B	R	K	Y	A	J	Q	G	Z	P	L	U	O	V	D	T	C	F	I	M	W	S	H	E	X
16	A	Q	J	X	Z	I	P	F	Y	O	K	T	N	U	C	S	B	E	H	L	V	R	G	D	W	M
17	P	I	W	Y	H	O	E	X	N	J	S	M	T	B	R	A	D	G	K	U	Q	F	C	V	L	Z
18	H	V	X	G	N	D	W	M	I	R	L	S	A	Q	Z	C	F	J	T	P	E	B	U	K	Y	O
19	U	W	F	M	C	V	L	H	Q	K	R	Z	P	Y	B	E	I	S	O	D	A	T	J	X	N	G
20	V	E	L	B	U	K	G	P	J	Q	Y	O	X	A	D	H	R	N	C	Z	S	I	W	M	F	T
21	D	K	A	T	J	F	O	I	P	X	N	W	Z	C	G	Q	M	B	Y	R	H	V	L	E	S	U
22	J	Z	S	I	E	N	H	O	W	M	V	Y	B	F	P	L	A	X	Q	G	U	K	D	R	T	C
23	Y	R	H	D	M	G	N	V	L	U	X	A	E	O	K	Z	W	P	F	T	J	C	Q	S	B	I
24	Q	G	C	L	F	M	U	K	T	W	Z	D	N	J	Y	V	O	E	S	I	B	P	R	A	H	X
25	F	B	K	E	L	T	J	S	V	Y	C	M	I	X	U	N	D	R	H	A	O	Q	Z	G	W	P
26	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E

Und für die Walze W_{III} erhält man diese Tabelle:

$D^{x} W_{III} D^{-x}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	C	E	G	I	K	B	O	Q	S	W	U	Y	M	X	D	H	V	F	Z	J	L	T	R	P	N	A
2	D	F	H	J	A	N	P	R	V	T	X	L	W	C	G	U	E	Y	I	K	S	Q	O	M	Z	B
3	E	G	I	Z	M	O	Q	U	S	W	K	V	B	F	T	D	X	H	J	R	P	N	L	Y	A	C
4	F	H	Y	L	N	P	T	R	V	J	U	A	E	S	C	W	G	I	Q	O	M	K	X	Z	B	D
5	G	X	K	M	O	S	Q	U	I	T	Z	D	R	B	V	F	H	P	N	L	J	W	Y	A	C	E
6	W	J	L	N	R	P	T	H	S	Y	C	Q	A	U	E	G	O	M	K	I	V	X	Z	B	D	F
7	I	K	M	Q	O	S	G	R	X	B	P	Z	T	D	F	N	L	J	H	U	W	Y	A	C	E	V
8	J	L	P	N	R	F	Q	W	A	O	Y	S	C	E	M	K	I	G	T	V	X	Z	B	D	U	H
9	K	O	M	Q	E	P	V	Z	N	X	R	B	D	L	J	H	F	S	U	W	Y	A	C	T	G	I
10	N	L	P	D	O	U	Y	M	W	Q	A	C	K	I	G	E	R	T	V	X	Z	B	S	F	H	J
11	K	O	C	N	T	X	L	V	P	Z	B	J	H	F	D	Q	S	U	W	Y	A	R	E	G	I	M
12	N	B	M	S	W	K	U	O	Y	A	I	G	E	C	P	R	T	V	X	Z	Q	D	F	H	L	J
13	A	L	R	V	J	T	N	X	Z	H	F	D	B	O	Q	S	U	W	Y	P	C	E	G	K	I	M
14	K	Q	U	I	S	M	W	Y	G	E	C	A	N	P	R	T	V	X	O	B	D	F	J	H	L	Z
15	P	T	H	R	L	V	X	F	D	B	Z	M	O	Q	S	U	W	N	A	C	E	I	G	K	Y	J
16	S	G	Q	K	U	W	E	C	A	Y	L	N	P	R	T	V	M	Z	B	D	H	F	J	X	I	O
17	F	P	J	T	V	D	B	Z	X	K	M	O	Q	S	U	L	Y	A	C	G	E	I	W	H	N	R
18	O	I	S	U	C	A	Y	W	J	L	N	P	R	T	K	X	Z	B	F	D	H	V	G	M	Q	E
19	H	R	T	B	Z	X	V	I	K	M	O	Q	S	J	W	Y	A	E	C	G	U	F	L	P	D	N
20	Q	S	A	Y	W	U	H	J	L	N	P	R	I	V	X	Z	D	B	F	T	E	K	O	C	M	G
21	R	Z	X	V	T	G	I	K	M	O	Q	H	U	W	Y	C	A	E	S	D	J	N	B	L	F	P
22	Y	W	U	S	F	H	J	L	N	P	G	T	V	X	B	Z	D	R	C	I	M	A	K	E	O	Q
23	V	T	R	E	G	I	K	M	O	F	S	U	W	A	Y	C	Q	B	H	L	Z	J	D	N	P	X
24	S	Q	D	F	H	J	L	N	E	R	T	V	Z	X	B	P	A	G	K	Y	I	C	M	O	W	U
25	P	C	E	G	I	K	M	D	Q	S	U	Y	W	A	O	Z	F	J	X	H	B	L	N	V	T	R
26	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O

Gegeben seien folgende, aus erratenen Spruchschlüsseln hergeleitete Transformationen der sechs Stellen eines Tages:

$Stelle_1$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T

$Stelle_2$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	T	F	G	J	U	B	C	Q	P	D	W	O	N	M	L	I	H	S	R	A	E	Z	K	Y	X	V

$Stelle_3$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Z	T	U	Y	Q	S	W	M	J	I	R	N	H	L	P	O	E	K	F	B	C	X	G	V	D	A

$Stelle_4$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	W	K	I	F	G	D	E	Y	C	R	B	X	V	Q	Z	S	N	J	P	U	T	M	A	L	H	O

Stelle$_5$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	G	Q	J	H	N	W	A	D	R	C	X	T	Y	E	Z	V	B	I	U	L	S	P	F	K	M	O

Stelle$_6$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	I	K	T	W	M	U	X	S	A	L	B	J	E	Q	P	O	N	V	H	C	F	R	D	G	Z	Y

Werden bei der Gleichung für eine Stelle nun die Stecker und der Ausdruck für die erste Walze auf die linke Seite gebracht, ergibt sich:

$$(D^{x}\, W_1\, D^{-x})^{-1}\, S^{-1}\, \text{Stelle}\, S\, (D^{x}\, W_1\, D^{-x}) = W_2\, W_3\, U\, W_3^{-1}\, W_2^{-1} = U_C$$

Man setzt wieder voraus, dass sich die zweite und dritte Walze gerade nicht drehen, und daher die zweite und dritte Walze zusammen mit der Umkehrwalze zu einer konstanten fiktiven Umkehrwalze Uc zusammengefasst werden können. Dieser Ausdruck muss bei korrekter Drehstellung x für die jeweiligen Stellen 1 bis 6 (unter Berücksichtigung der Vorrückung von x) ein identisches Permutationsmuster ergeben. Da die sechs Steckerverbindungen aber noch unbekannt sind, werden diese bei Uc ignoriert, weshalb dies bei einem Vergleich nur zu teilweiser Übereinstimmung führen kann (entsprechend der 14 ungesteckten Buchstaben). Wie sich herausstellt, sind jedoch die fragmentarischen Teile für eine Identifizierung ausreichend.

Praktischerweise werden nun mit Hilfe der Tabellen für die einzelnen Walzen die Terme Uc mit den täglichen Transformationen für die Stellen berechnet und zwar so, dass mit einem Überhang von sechs Stellen die Ausdrücke der Tabellen (für jede der drei Walzen getrennt) aufgeschrieben werden. Diese Tabellen sind natürlich für jeden Tag dieselben. Auf einem Blatt Papier schreibt man nun untereinander die sechs Transformationen der Stellen eines Tages, und zwar so, dass zwischen ihnen jeweils ein Zeilenfenster ausgeschnitten bleibt. Dieses Rasterformular legt man zeilenweise nacheinander über die Tabellen der Walzen, bis gewisse Übereinstimmungen sichtbar werden. Diese Methode wird Rasterverfahren („*metoda rusztu*“) genannt.

Werden die täglichen Stellentransformationen über die ersten sechs Zeilen der Tabelle für die Walze W_I gelegt, ergibt sich folgendes Bild:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$D^{1}\, W_I\, D^{-1}$	J	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T	R	O	Z	H	A	Q	B	I	D
Stelle$_1$	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$D^{2}\, W_I\, D^{-2}$	K	D	J	E	B	O	T	X	L	R	M	U	W	F	V	S	Q	N	Y	G	Z	P	A	H	C	I
Stelle$_2$	T	F	G	J	U	B	C	Q	P	D	W	O	N	M	L	I	H	S	R	A	E	Z	K	Y	X	V

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$D^{3}\,W_I\,D^{-3}$	C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R	P	M	X	F	Y	O	Z	G	B	H	J
Stelle$_3$	Z	T	U	Y	Q	S	W	M	J	I	R	N	H	L	P	O	E	K	F	B	C	X	G	V	D	A

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$D^{4}\,W_I\,D^{-4}$	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q	O	L	W	E	X	N	Y	F	A	G	I	B
Stelle$_4$	W	K	I	F	G	D	E	Y	C	R	B	X	V	Q	Z	S	N	J	P	U	T	M	A	L	H	O

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$D^{5}\,W_I\,D^{-5}$	B	Y	L	Q	U	I	O	J	R	T	C	S	P	N	K	V	D	W	M	X	E	Z	F	H	A	G
Stelle$_5$	G	Q	J	H	N	W	A	D	R	C	X	T	Y	E	Z	V	B	I	U	L	S	P	F	K	M	O

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$D^{6}\,W_I\,D^{-6}$	X	K	P	T	H	N	I	Q	S	B	R	O	M	J	U	C	V	L	W	D	Y	E	G	Z	F	A
Stelle$_6$	I	K	T	W	M	U	X	S	A	L	B	J	E	Q	P	O	N	V	H	C	F	R	D	G	Z	Y

Damit lassen sich nun die Ausdrücke für die fiktive Umkehrwalze U_C sofort ablesen (man beginnt mit A in der zweiten Zeile findet B in der dritten Zeile und geht weiter über B der ersten Zeile zu L der zweiten Zeile, entsprechend dem Ausdruck). Für die sechs Ausdrücke von U_C ergibt sich somit (ohne Berücksichtigung der Stecker):

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U_{C1}	L	T	J	Z	R	V	S	W	P	C	X	A	O	Y	M	I	U	E	G	B	Q	F	H	K	N	D

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U_{C2}	M	Z	H	O	R	W	K	C	P	T	G	S	A	Y	D	I	X	E	L	J	V	U	F	Q	N	B

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U_{C3}	H	Z	J	O	K	S	W	A	Y	C	E	Q	N	M	D	R	L	P	F	X	V	U	G	T	I	B

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U_{C4}	H	O	U	G	S	T	D	A	P	R	Z	X	V	Y	B	I	W	J	E	F	C	M	Q	L	N	K

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U_{C5}	P	O	H	Y	M	I	K	C	F	Q	G	T	E	U	B	A	J	W	X	L	N	Z	R	S	D	V

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U_{C6}	F	O	U	P	L	A	T	M	Z	V	R	E	H	Y	B	D	W	K	X	G	C	J	Q	S	N	I

Man erkennt gewisse Ähnlichkeiten, die ein Indiz für die richtige Walze und ihre Drehstellung darstellen (hier Walze I bei Drehposition 1).

Nun untersucht man zuerst die gehäuft auftretenden Transformationen der einzelnen Stellen im Detail, wobei die Steckerverbindungen noch unbekannt sind:

$(D^{1} W_I D^{-1})^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	V	X	F	Z	C	E	O	U	Y	A	D	B	J	L	S	G	W	R	K	Q	H	M	P	N	I	T
S^{-1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Stelle$_1$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	V	R	N	M	A	Y	W	L	S	O	I	E	D	K	U	X	C	J	Z	P	B	H	Q	G	T
S	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$D^{1} W_I D^{-1}$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	J	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T	R	O	Z	H	A	Q	B	I	D
U_{C1}	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	L	T	J	Z	R	V	S	W	P	C	X	A	O	Y	M	I	U	E	G	B	Q	F	H	K	N	D

Untersucht man auch die Transformationen von Y bei den anderen Ausdrücken von U_C ergibt sich folgende Tabelle:

U_{C1}	Y	Walze	I	Stecker	I	Stelle	L	Stecker	L	Walze	N
U_{C2}	Y	Walze	S	Stecker	S	Stelle	R	Stecker	R	Walze	N
U_{C3}	Y	Walze	T	Stecker	T	Stelle	B	Stecker	B	Walze	I
U_{C4}	Y	Walze	U	Stecker	U	Stelle	T	Stecker	T	Walze	N
U_{C5}	Y	Walze	B	Stecker	B	Stelle	Q	Stecker	Q	Walze	D
U_{C6}	Y	Walze	U	Stecker	U	Stelle	F	Stecker	F	Walze	N

Für die Transformationen Y auf N ergeben sich folgende Schlussfolgerungen:

(IL) ist entweder ein Steckerpaar oder I und L sind ungesteckt.
(RS) ist entweder ein Steckerpaar oder R und S sind ungesteckt.
(TU) ist entweder ein Steckerpaar oder T und U sind ungesteckt.
(FU) ist entweder ein Steckerpaar oder F und U sind ungesteckt.

Da die letzten beiden Bedingungen für den Fall eines Steckerpaares aber einen Widerspruch erzeugen, ergibt sich die konsistente Bedingung:

F, T und U sind ungesteckt.

Wird dies im Ausdruck an der Stelle 3 berücksichtigt, erhält man ein erstes Steckerpaar, damit die Transformation Y auf N erfüllt wird:

U_{C3}	Y	Walze	T	Stecker	T	Stelle	B	Stecker	E	Walze	N

Stecker (BE)

Untersucht man beispielsweise die Transformation an der Stelle 2 für den Buchstaben B mit Einsetzen der bereits gefundenen Beziehungen, folgt, dass in U_C immer B auf O und umgekehrt transformieren muss:

U_{C2}	B	Walze	E	Stecker	B	Stelle	F	Stecker	F	Walze	O

Für die Stelle 3 ergibt sich damit ein weiteres Steckerpaar:

U_{C3}	B	Walze	X	Stecker	C	Stelle	U	Stecker	U	Walze	O

Stecker (CX)

Bei der Stelle 1 ergibt sich daraus ein drittes Steckerpaar:

U_{C1}	B	Walze	X	Stecker	C	Stelle	R	Stecker	S	Walze	O

Stecker (RS)

Auf analoge Weise können aus den restlichen Transformationen für den Buchstaben B nun weitere Bedingungen abgeleitet werden:

U_{C4}	B	Walze	Z	Stecker	Z	Stelle	O	Stecker	O	Walze	O
U_{C5}	B	Walze	A	Stecker	A	Stelle	G	Stecker	G	Walze	O
U_{C6}	B	Walze	J	Stecker	J	Stelle	L	Stecker	L	Walze	O

(OZ) ist entweder ein Steckerpaar oder O und Z sind ungesteckt.
(AG) ist entweder ein Steckerpaar oder A und G sind ungesteckt.
(JL) ist entweder ein Steckerpaar oder J und L sind ungesteckt.

Mit obigen gefundenen Bedingungen folgt daher:

I, J und L sind ungesteckt.

Untersucht man beispielsweise die Transformationen für D an der Stelle 2, findet man eine neue gültige Transformation für U_C, nämlich D auf Z und umgekehrt:

U_{C2}	D	Walze	B	Stecker	E	Stelle	U	Stecker	U	Walze	Z

Für die Stelle 3 ergibt sich daher:

U_{C3}	D	Walze	C	Stecker	X	Stelle	V	Stecker	V	Walze	Z

V ist ungesteckt.

Um die restlichen Stellen von U_C konsistent zu machen, muss gelten:

U_{C1}	D	Walze	Z	Stecker	Z	Stelle	T	Stecker	T	Walze	Z
U_{C4}	D	Walze	L	Stecker	L	Stelle	X	Stecker	C	Walze	Z
U_{C5}	D	Walze	Q	Stecker	P	Stelle	V	Stecker	V	Walze	Z
U_{C6}	D	Walze	T	Stecker	T	Stelle	C	Stecker	X	Walze	Z

Stecker (PQ)

Und mit der Bedingung von früher folgt weiters:

Z und O sind ungesteckt.

Untersucht man die Transformationen für den Buchstaben A, ergibt sich für die Stelle 1, dass in U_C die Transformation A auf F gelten muss:

U_{C1}	A	Walze	V	Stecker	V	Stelle	B	Stecker	E	Walze	F

Dies impliziert für die Stelle 6 folgende Beziehung:

U_{C6}	A	Walze	Z	Stecker	Z	Stelle	Y	Stecker	Y	Walze	F

Y ist ungesteckt.

Die Ausdrücke für die Stellen 3 und 4 führen schließlich zu den Steckerpaaren:

U_{C3}	A	Walze	D	Stecker	K	Stelle	R	Stecker	S	Walze	F
U_{C4}	A	Walze	W	Stecker	M	Stelle	V	Stecker	V	Walze	F

Stecker (DK) und Stecker (MW)

Zur Überprüfung werden alle gewonnen Steckerbeziehungen in die jeweiligen Ausdrücke für U_C eingesetzt. Bei richtiger Identifizierung der Stecker muss dies zu ein und demselben Ausdruck für alle U_C führen, nämlich:

U_C	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	F	O	J	Z	W	A	K	T	P	C	G	Q	R	Y	B	I	L	M	X	H	V	U	E	S	N	D

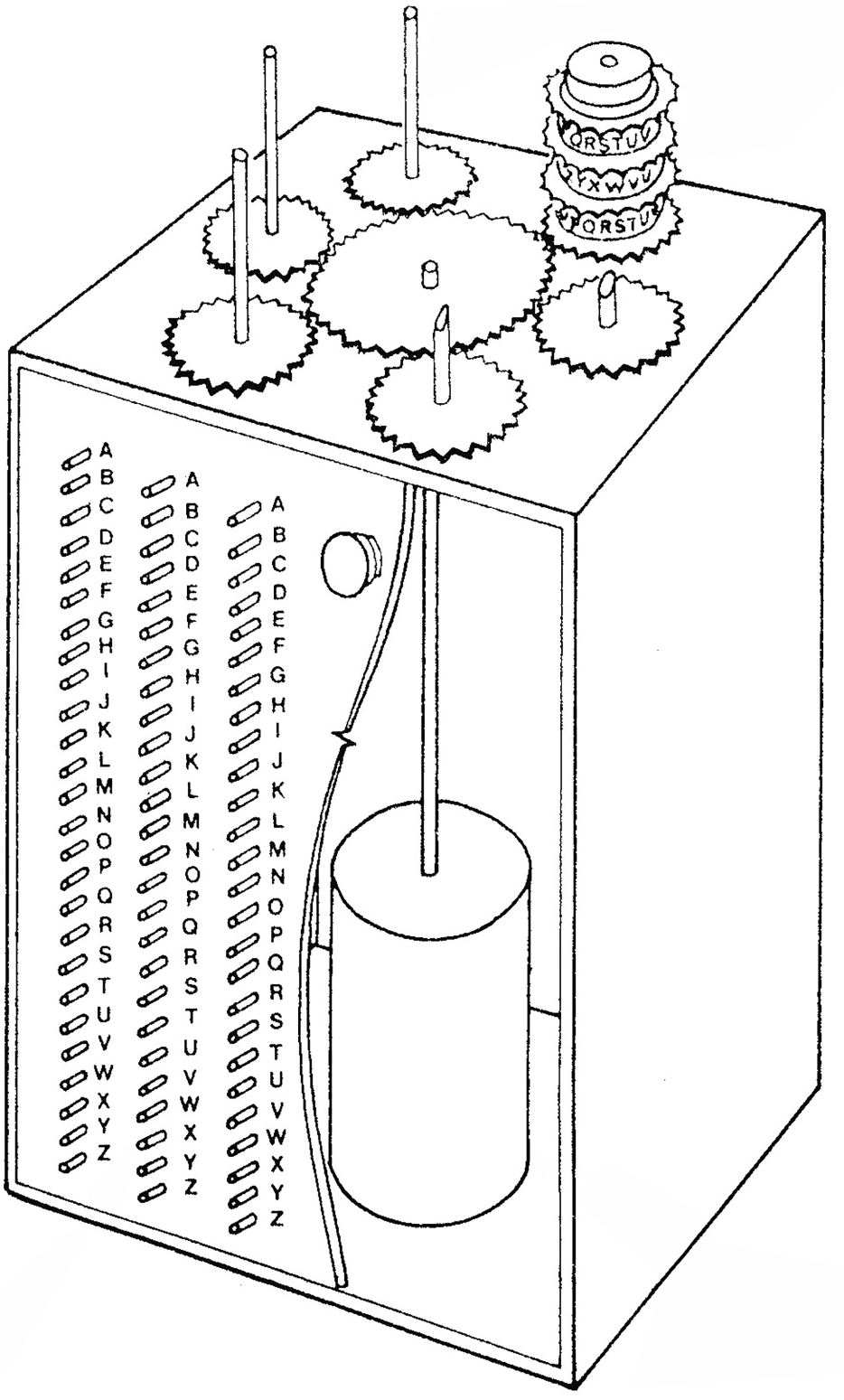
Damit sind die rechte Walze (hier beispielsweise die Walze W_I im laufenden Quartal), die effektive Anfangsstellung der rechten Walze (hier beispielsweise die Drehstellung 01 des betreffenden Tages) und alle Steckerverbindungen (hier beispielsweise die Steckerverbindungen (BE)(CX)(DK)(MW)(PQ)(RS) im laufenden Monat) bekannt. Diese Methode zum Auffinden der Stecker muss von Rejewski einmal pro Monat durchgeführt werden, da sich die Steckerbelegung nur monatlich ändert.

Nach Bestimmung der rechten Walze mit der Rastermethode und danach der Steckerverbindungen erhält Rejewski die Buchstabentransformationen für die konstant gesetzte Umkehrwalze U_C des Tages. Um die mittlere und die linke Walze samt ihrer Drehstellungen zu identifizieren, legt er den Q-Katalog an, benannt nach der fiktiven Umkehrwalze U_C, die er als Q bezeichnet. Darin sind alle Variationen für U_C verzeichnet und können sofort nachgeschlagen werden. Damit sind die gesuchten Walzen und ihre Drehstellungen ablesbar.

Für den im obigen, mit der Rastermethode untersuchten Fall sehen die Einträge im betreffenden Abschnitt des Katalogs wie folgt aus (in der ersten Spalte ist die linke Walze und in der zweiten Spalte die mittlere Walze mit all ihren Drehstellungen aufgelistet, geordnet nach den Buchstabentransformationen der konstant gesetzten Umkehrwalze U_C):

W_{III}	W_{II}	Q = U_C																									
07	10	F	M	H	E	D	A	P	C	K	R	I	N	B	L	V	G	U	J	T	S	Q	O	X	W	Z	Y
18	16	F	O	H	L	G	A	E	C	J	I	Q	D	U	W	B	X	K	T	Z	R	M	Y	N	P	V	S
01	01	F	O	J	Z	W	A	K	T	P	C	G	Q	R	Y	B	I	L	M	X	H	V	U	E	S	N	D
03	26	F	O	Q	R	U	A	J	X	V	G	T	M	L	Y	B	Z	C	D	W	K	E	I	S	H	N	P
02	18	F	O	V	G	N	A	D	Q	M	U	X	R	I	E	B	S	H	L	P	W	J	C	T	K	Z	Y
10	20	F	R	L	M	O	A	J	X	K	G	I	C	D	Y	E	T	U	B	W	P	Q	Z	S	H	N	V

Der Q-Katalog enthält insgesamt 4.096 Einträge, die sich aus den Kombinationsmöglichkeiten zweier Walzen mit je 26 Drehstellungen bei insgesamt 6 möglichen Walzenlagen ergeben.


ORSTUV
YXWVU
ORSTUV
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Maschinenpower: Bomba

Folgende doppelte Spruchschlüssel – alle mit einem Einserzyklus etwa H – mit den frei gewählten und unchiffrierten Grundstellungen seien bei einer unbekannten Tageseinstellung mit der Walzenlage III-II-I, der Ringstellung 03-03-03 und den Steckerverbindungen (BE)(RS)(KD)(WM)(CX)(PQ) gegeben:

Grundstellung	DNW	Spruchschlüssel	HYE HOQ
	EOK		EHB XHZ
	NVA		TEH VMH

Diese Spruchschlüsselkombinationen werden auf der Bomba so eingestellt, dass die jeweiligen Einserzyklen die Startpositionen bilden: Die ersten beiden Walzensätze werden daher jeweils um drei Stellen verschoben auf die Grundstellung DNW und DNZ gedreht, die nächsten beiden auf EOL und EOO und schließlich die letzten beiden Walzensätze auf NVC und NVF justiert. Den Umstand nutzend, dass die beiden Chiffren H in den Spruchschlüsselchiffren gleichen, wenngleich unbekannten Klarbuchstaben entsprechen müssen, wird nun in Umkehrung ein H in die drei Walzensätze eingespeist. Die Bomba startet, alle Walzensätze beginnen sich synchron Schritt für Schritt zu drehen. Sie hält erst an, wenn auf jedem der drei Walzensatzpaare zwei gleiche Buchstaben auftauchen.

Beispielsweise erfolgt ein Treffer bei folgenden Konstellationen: Die Walzenlage der Walzensätze sei III-II-I und der erste Walzensatz steht auf BLU und verwandelt das eingehende H in ein B; analog dazu der um drei Stellen vorgerückte Walzensatz BLX. Der zweite Walzensatz steht auf CMJ und verwandelt das H in ein Q; analog an der Stelle CMM. Der dritte Walzensatz schließlich verwandelt an LTA das H ebenfalls in ein Q; analog an der Stelle LTD.

Eine mögliche Ringstellung ist nun ablesbar, als Differenz der aufgefangenen Spruchschlüssel zu den gefundenen Stellungen der Bomba, welche hier mit 03-03-03 identifiziert werden kann, gemäß der Differenz der Grundstellungen zu den aufgefundenen Drehstellungen: DNW-BLU, EOL-CMJ und NVC-LTA.

Wenn ein solcher Treffer auf der Bomba gefunden wird, stellt man auf der nachgebauten Enigma die entsprechende Walzenlage, die mögliche Ringstellung und die unverschlüsselte Grundstellung ein, wobei das Steckerfeld ungesteckt bleibt, also beispielsweise Walzenlage III-II-I, Ringstellung 03-03-03 und Grundstellung DNW.

Mit dieser Einstellung liefert die Enigma für die aufgefangenen chiffrierten doppelten Spruchschlüssel folgende Klartextmuster, die durch mehreres Auftreten gleicher Buchstaben vielversprechend erscheinen:

Grundstellung	DNW	Spruchschlüssel	HYE HOQ	dechiffriert	BSA BSI
	EOK		EHB XHZ		NQQ OQY
	NVA		TEH VMH		MMQ MHQ

Hierbei stören jedoch nach wie vor die unbekannten Steckerverbindungen. Fünf bis acht täglich einzustellende Steckerverbindungen ergeben eine durchschnittliche Wahrscheinlichkeit von rund 50 % für einen gesteckten oder ungesteckten Buchstaben. Aber mit den gefundenen Einstellungen können weitere doppelte Spruchschlüssel des Tages untersucht werden, auch jene ohne die besonderen Einserzyklen:

Grundstellung	VBU	Spruchschlüssel	UGD JBO	dechiffriert	NWE NLL
	AFI		PXS YMN		IUD AUK
	WVT		CVF KMN		FAY JEY
	OSR		TEI OAX		ELU EHQ
	NWB		TMS JHA		RDY RKF
	RXK		OJZ GNI		TZU TZU
	WGH		CDD WJO		LIS DFX
	ZFD		NZU BLK		MBS TBU
	EBD		CTS ZAM		TEA HER
	JGS		RUH QCL		WNB GEB
	JUM		OOL WIF		WAC MAC
	PEW		UWV VEA		STT SGT
	SCP		WPP LZF		VTN RAW
	HEM		GBA PVC		ZVG VUL
	BVE		DBU GLN		JZD SID
	WGK		PXR IWT		ARZ KCF
	SOL		JXN YYA		HWT HUT
	VOR		AXG XUP		YSM KLE

Beispielsweise sei bei dem gefundenen dechiffrierten Spruchschlüssel TZU TZU folgende chiffrierte Nachricht angehängt:

GGDXM PLDOV OLKJZ MJLYK TQWBC HUCPL JVBWI KJXPI DUWWJ YEPEW
MQSHA OJVQV XRGMP MCOAS OBIAQ JWJIZ NCFLZ UHAXA SAPOE FVBKL
BMIAV IEXYC ZNKKJ JMCBH NWPLJ XRZHE VBQPE AMEGA NUIHZ TOJIW LHYZB
HZTUD VRRTC OPBIN WGLPR MDYLM QUVTX MVVTU BBONM ZOOQJ KN

Ohne Steckerverbindungen erhält man nach der Dechiffrierung mit der gefundenen Tageseinstellung folgende Textfragmente:

KIQOX FQTBN KBQSO KBNAL WIXDH EBWJI BREBB HTVFH VHZSS BUCJV HPMIN BINVW YWRHI BJINC BCNGA ROHLO RGBNA LLBLO VNKNX BNHRF NFTTU NKZHM BSPGU QZWLK UDFHB JCBOY FEVMS VTTBR KBUTR XHBNL BBSBX VOWRE BXCNR NGLUB LMBFH OAHBR IAEBY QIXHN JTHTF SFUUL ST

Mit Hilfe der Sprachstatistik der deutschen Sprache lässt sich hier bei gehäuften Vorkommen einzelner Buchstaben auf Steckerverbindungen schließen. Der Buchstabe B kommt beispielsweise überproportional oft vor, nämlich 28 Mal. Daher wird dieser Buchstabe mit dem am häufigsten auftretenden Buchstaben der deutschen Sprache E angenommen, also eine Steckerverbindung (BE) versucht und der verschlüsselte Text auf der Enigma mit diesem Stecker nochmals überprüft:

KIQOX FQTEN KEQSO KENAL WIXHH BEWJI EREEE HTVFH VHZSS ERCSV HPMIN EINVW YWRHI EJINC EINGA ROHLO RGENA LLELO VNKNG ENARF SFTTU NGZHM ESPGU QZWNK UDFHE JCEOF FEVMI VTKER KEUTR XHENL EESER VOWRB EXCNR NGRUE LMEFH OAHER IABEY QIXHN IXHTF SFUUL ST

Dabei erscheint im Textfragment bereits 30 Mal der Buchstabe E, was ein gutes Indiz für eine richtige Steckerwahl darstellt. Nun erkennt man beispielsweise ein Textfragment SFTTUNG, welches mit einer weiteren Steckerannahme (RS) etwa das Wort RETTUNG bilden könnte. Nach neuerlicher Überprüfung der chiffrierten Nachricht mit den beiden Steckerverbindungen (BE)(RS) ergibt sich:

KIQOX FQTEN KEQRO KENAL WIXHH BEWJI ESEEE HTVFH VHZRR ESCRV HPEIN EINVW YESHI EJING EINGA SOHLO SGENA LLELO FNKNG ENASF RFTTU NGZHM ERPGU QZWNK UDFHE JNEOF FEVMI VTKES KEUTS XHENL EERES VOWSB EKENS NGSUE LMEFT OAHES IABEY QIXHN IXHTF RFUUL RT

Hinter dem Textfragment KEUTSXH könnte im Klartext DEUTSCH stecken, also werden die zwei weiteren Stecker (DK)(CX) ausprobiert:

DIETC FQQEN DERRO DENAR WICHA BENJI ESEEE UTSFH EHZRR ESXRV HPEIN EINVW FESHI ERING EINGA SOHLO SSENA LLEHO FNDNG ENAUF RFTTU NGIHR ERTRU QZEND UKFHE INEOF FEVMI VTDES DEUTS CHENL EERES VOWSU EDENU NGSUE LMEFT ONHES IABEN QICHN ICHTF RFUUL LT

Ein Stecker (PQ) könnte die Worte TRUPPEN ergeben, eine Überprüfung ergibt (man erkennt nun bereits größere lesbare Textfragmente):

DIETC UPPEN DERRO DENAR WECHA BENDI ESEEE UTSCH EHZRR ESGRV HPEIN EINEW FESHE ERING EINGE SOHLO SSENA LLEHO FNUNG ENAUF RFTTU NGIHR ERTRU PZEND UKCHE INEOF FENSI VTDES DEUTS CHENL EERES VOWSU EDENU NDSUE LMEST ONHES HABEN PICHN ICHTF RFUEL LT

Um aus dem Textfragment ARWEC offensichtlich das Wort ARMEE zu bilden, wird schließlich die sechste Steckerverbindung (MW) versucht:

DIETR UPPEN DERRO TENAR MEEHA BENDI ESEDE UTSCH EHEER ESGRU PPEIN EINEM FESTE NRING EINGE SCHLO SSENA LLEHO FNUNG ENAUF RETTU NGIHR ERTRU PPEND URCHE INEOF FENSI VEDES DEUTS CHENH EERES VOMSU EDENU NDSUE DWEST ENHER HABEN SICHN ICHTE RFUEL LT

Somit sind alle sechs Steckerverbindungen (BE)(RS)(KD)(WM)(CX)(PQ) identifiziert und die Tageseinstellung komplett entschlüsselt. Mit dieser Methode können natürlich auch andere Nachrichten von anderen Schlüsseln ausprobiert werden, wenn keine sinnvollen Textfragmente bei der Analyse eines Funkspruchs zu erkennen sind.

HW 25/3

CCR 1
102(1)

TOP SECRET
ULTRA

65/4/7A

I. A description of the mach ine.

We begin by describing the 'unsteckered enigma'. The machine consists of a box with 26 keys labelled with the letters of the alphabet and 26 bulbs which shine through stencils on which letters are marked. It also contains wheels whose function will be described later on. When a key is depressed the wheels are made to move in a certain way and a current flows through the wheels to one of the bulbs. The letter which appears over the bulb is the result of enciphering the letter on the depressed key with the wheels in the position they have when the bulb lights.

To understand the working of the machine it is best to separate in our minds

The electric circuit of the machine without the wheels.

The circuit through the wheels.

The mechanism for turning the wheels and for describing the positions of the wheels.

The circuit of the machine without the wheels.

Fig 1

Eintrittswalz

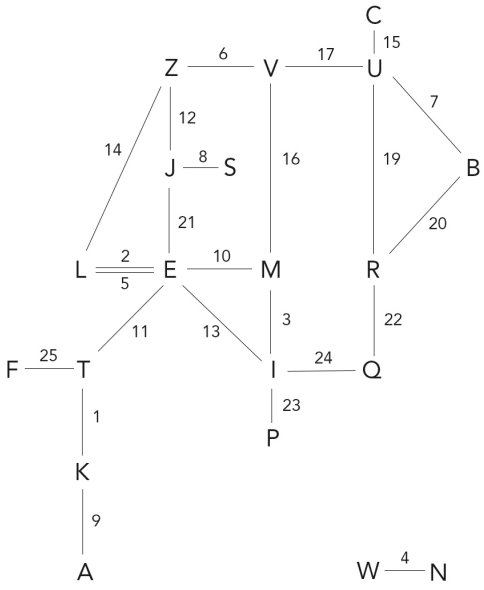
The machine contains a cylinder called the Eintrittswalz (E.W) on which are 26 contacts $C_1, \ldots, C_{26}$. The effect of the wheels is to connect these contacts up in pairs, the actual pairings of course depending on the positions of the wheels.

Turings
Cribs und Closures

Turing verändert die Dechiffrierstrategie dahingehend, dass er mithilfe von Cribs unmittelbar in die Chiffren eines Funkspruchs einzubrechen versucht, wie dies im nachstehenden Beispiel geschieht. Als Crib für den Suchlauf auf der Bombe benutzt er die Phrase „*Keine Zusätze zum Vorbericht*", die er in einem aufgefangenen Funkspruch vermutet:

Stelle	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Chiffren	T	L	M	W	L	V	B	J	K	M	E	J	I	L	C	V	U	E	U	R	J	Q	P	J	F
Klartext	K	E	I	N	E	Z	U	S	A	E	T	Z	E	Z	U	M	V	O	R	B	E	R	I	Q	T

Untersucht man die Transformationen von Klarbuchstaben und Chiffren, findet man mitunter Schleifen, „Closures", die er zunächst in einem „Diagram" abbildet:



Im Diagramm werden einzelne „Central Letters" erkennbar, die Ausgangspunkt mehrerer Schleifen sind. So muss etwa das E an der zehnten Stelle des Cribs in ein M übergehen, M an der dritten Stelle in ein I und das I schließt an der dreizehnten Stelle

53 *The Prof's book: Abhandlung von Alan Turing über die Enigma*

die Schleife. Da die Enigma invers funktioniert, gilt die Schleife auch in die Gegenrichtung, also I in M, M in E und E in I. In einer weiteren Schleife geht das E an der zweiten Stelle in ein L über und L an der fünften wieder in ein E.

Der untersuchte Crib weist also zwischen der zweiten und der dreizehnten Stelle diese beiden Schleifen, die als „Menu" für den Suchlauf in der Bombe dienen. Dass die Schleifen innerhalb von nur elf Stellen liegen, erhöht die Chance, dass kein Übertrag vorliegt, wodurch erst die Bombe ein korrektes Ergebnis liefern kann.

Daraus ergibt sich folgendes Menu, das auf fünf hintereinandergeschalteten Enigma-Walzensätzen in der Bombe durchgespielt wird: E – L – E – M – I – E. Die Bombe hält an, wenn Eingangs- und Ausgangsbuchstabe identisch sind, im vorliegenden Beispiel bei F. An dieser Stelle können die Walzenlage und die Schlüsselstellung der Walzen abgelesen werden, in diesem Fall: Walzenlage III-II-I, Schlüsselstellung 22-21-21.

E	2	L	5	E	10	M	3	I	13	E
A	2	C	5	Z	10	J	3	L	13	K
K	2	F	5	K	10	W	3	D	13	W
W	2	V	5	E	10	G	3	A	13	E
E	2	H	5	N	10	H	3	T	13	J
J	2	Z	5	C	10	X	3	C	13	Z
Z	2	J	5	A	10	V	3	Z	13	C
C	2	A	5	J	10	Z	3	V	13	I
I	2	Y	5	L	10	B	3	E	13	A
B	2	R	5	B	10	L	3	J	13	T
T	2	S	5	W	10	K	3	P	13	X
X	2	D	5	P	10	D	3	W	13	D
D	2	X	5	U	10	O	3	F	13	S
S	2	T	5	G	10	E	3	B	13	O
O	2	P	5	D	10	P	3	K	13	L
L	2	M	5	Q	10	T	3	H	13	Y
Y	2	I	5	O	10	U	3	N	13	R
R	2	B	5	R	10	Y	3	Q	13	G
G	2	N	5	H	10	N	3	U	13	M
M	2	L	5	Y	10	R	3	I	13	V
V	2	W	5	S	10	I	3	R	13	N
N	2	G	5	T	10	Q	3	Y	13	H
H	2	E	5	V	10	A	3	G	13	Q
Q	2	U	5	X	10	C	3	X	13	P
P	2	O	5	I	10	S	3	M	13	U
U	2	Q	5	M	10	F	3	O	13	B
F	2	K	5	F	10	M	3	S	13	F

Nachdem der Ausgangsbuchstabe im Menu E war und im Ergebnis ein F steht, muss E mit F gesteckt sein. Darüber hinaus findet man hier mit (KL) und (SI) zwei weitere Stecker. M muss demnach ungesteckt sein.

Nun wird eine andere Schleife, ausgehend vom Buchstaben U, untersucht:

U	7	B	20	R	19	U
A	7	S	20	Y	19	H
H	7	D	20	C	19	P
P	7	Q	20	K	19	Q
Q	7	P	20	G	19	R
R	7	B	20	A	19	S
S	7	A	20	B	19	T
T	7	U	20	Z	19	N
N	7	K	20	Q	19	K
K	7	N	20	J	19	X
X	7	M	20	H	19	Y
Y	7	J	20	N	19	Z
Z	7	E	20	O	19	V
V	7	I	20	V	19	O
O	7	C	20	D	19	F
F	7	L	20	X	19	J
J	7	Y	20	S	19	A
B	7	R	20	W	19	E
E	7	Z	20	U	19	I
I	7	V	20	I	19	U
U	7	T	20	F	19	D
D	7	H	20	M	19	L
L	7	F	20	T	19	B
C	7	O	20	E	19	W
W	7	G	20	P	19	C
G	7	W	20	R	19	G
M	7	X	20	L	19	M

Da M ungesteckt sein muss, ist U mit G gesteckt. Des Weiteren muss B mit W gesteckt sein und R ungesteckt.

Gibt es keine Schleifen mehr zum Untersuchen, können zum Steckersuchen auch vorkommende Ketten wie E – T – K – A herangezogen werden:

E	11	T	1	K	9	A
F	11	Y	1	L	9	A

Wendet man den bereits bekannten Stecker (EF) bei dieser Kette an, so zeigt sich der letzte fehlende Stecker (TY).

Bis auf die Ringeinstellungen sind damit alle Einstellungen des Tagesschlüssels bekannt.

Abbildungen

Abb. 10
Marian Rejewski, um 1932, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:MR_1932_small.jpg, abgerufen am 22. November 2017)

Abb. 11
Schlüsselwalze der Enigma, Inv.Nr. 33304,
Technisches Museum Wien

Abb. 12
Gebrauchsanleitung für die Chiffriermaschine Enigma, 1937,
Technisches Museum Wien

Abb. 13
Synchronisierte Funksprüche der Uhrenmethode,
Technisches Museum Wien

Abb. 14
Umkehrwalze der Enigma, Inv.Nr. 33304,
Technisches Museum Wien

Abb. 15
Die polnische Bomba, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Bomba_full.jpg, abgerufen am 22. November 2017)

Abb. 16
Steckerfeld der Enigma, Inv.Nr. 33304,
Technisches Museum Wien

Abb. 17
Luftangriff auf Polen mit „Stukas", 1939, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Bundesarchiv_Bild_183-1987-1210-502,_Polen,_Stukas.jpg, abgerufen am 22. November 2017)

Abb. 18
Überfall auf Polen, 1939, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Bundesarchiv_Bild_146-1976-071-36,_Polen,_an_der_Brahe,_deutsche_Panzer.jpg, abgerufen am 22. November 2017)

Abb. 19
Hut 6 in Bletchley Park, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Hut6.jpg, abgerufen am 22. November 2017)

Abb. 20
Funkhorchstation der Royal Air Force, 1939–1945, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Royal_Air_Force_Radio-countermeasures,_1939-1945_CH16682.jpg, abgerufen am 22. November 2017)

Abb. 21
Der Schlüssel M – Verfahren M Allgemein, 1940, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Schl%C3%BCssel_M.jpg, abgerufen am 22. November 2017)

Abb. 22
Zahlenreihentafel zum R. H. V. Allgemein, 1942, Dirk Rijmenants

Abb. 23
Enigma-Verschlüsselung, General Guderian in Frankreich 1940, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Bundesarchiv_Bild_101I-769-0229-11A,_Frankreich,_Guderian,_%22Enigma%22.jpg, abgerufen am 22. November 2017)

Abb. 24
Aufgefangener Funkspruch in Bletchley Park, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Typical_Bletchley_intercept_sheet.jpg, abgerufen am 22. November 2017)

Abb. 25
Royal Air Force Fighter Command, 1939–1945, Imperial War Museum, CH 11887

Abb. 26
Luftschlacht um England, 1940, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Spitfires_camera_gun_film_shows_tracer_ammunition.jpg, abgerufen am 22. November 2017)

Abb. 27
Alan Turing, ca. 1930–1935, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Alan_Turing_az_1930-as_%C3%A9vekben.jpg, abgerufen am 22. November 2017)

Abb. 28
Enigma-Verschlüsselung im Unterseeboot U-124, 1941, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Bundesarchiv_Bild_101II-MW-4222-02A,_%22Enigma%22_auf_U-Boot_U-124.jpg, abgerufen am 22. November 2017)

Abb. 29
Closure zur Programmierung auf einer Bombe, Technisches Museum Wien

Abb. 30
Bombes in Bletchley Park Crown. Reproduced by kind permission, Director GCHQ

Abb. 31
Banbury Sheet, gefunden in Bletchley Park 2014, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Part_of_a_Banbury_Sheet_as_used_in_Banburismus.jpg, abgerufen am 22. November 2017)

Abb. 32
Amerikanischer Schiffskonvoi, 1941, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Convoy_WS-12_en_route_to_Cape_Town,_1941.jpg, abgerufen am 22. November 2017)

Abb. 33
Sinkender alliierter Tanker nach U-Boot-Angriff, 1942, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Allied_tanker_torpedoed.jpg, abgerufen am 22. November 2017)

Abb. 34
Ausschnitt aus: The Prof's Book: Turing's Treatise on the Enigma, 1940, Internet Archive (https://archive.org/details/hw-25-3, abgerufen am 22. November 2017)

Abb. 35
Marine-Enigma M4, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Bletchley_Park_Naval_Enigma_IMG_3604.JPG, abgerufen am 22. November 2017)

Abb. 36
Chiffrierwalzen der M4, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Enigma_rotors_and_spindle_showing_contacts_rachet_and_notch.jpg, abgerufen am 22. November 2017)

Abb. 37
Zuteilungsliste für Kenngruppen zum K. Buch, Wikimedia Commons, (https://upload.wikimedia.org/wikipedia/commons/4/48/Zuteilungsliste_From_Kenngruppen.jpg, abgerufen am 2. April 2018)

Abb. 38
Amerikanische Highspeed-Bombe, ca. 1943, National Security Agency

Abb. 39
Deutsches Kriegsschiff Tirpitz, ca. 1943–1944, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Tirpitz_altafjord.jpg, abgerufen am 22. November 2017)

Abb. 40
Offiziere auf einem Zerstörer, 1941, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Officers_on_the_bridge.jpg, abgerufen am 22. November 2017)

Abb. 41
Aufstellung deutscher U-Boote im Atlantik, 1941, Jürgen Rohwer

Abb. 42
Angriff auf die deutschen U-Boote U-66 und U-117, 1944
Wikimedia Commons (https://commons.wikimedia.org/wiki/File:U-66_U-117_Luftangriff.jpg, abgerufen am 22. November 2017)

Abb. 43
Enemy Submarine Tracking Section, Joint Operations Control Room in New York, Captain Jerry Mason, http://uboatarchive.net

Abb. 44
Landung der Alliierten in der Normandie, 1944, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:NormandySupply_edit.jpg, abgerufen am 22. November 2017)

Abb. 45
Zerstörte Enigma, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Enigma_machine.jpg, abgerufen am 22. November 2017)

Abb. 46
Enigma-Uhr, Wikimedia Commons (https://de.wikipedia.org/wiki/Enigma-Uhr#/media/File:ENIGMA_Uhr_(%27clock%27)_-_National_Cryptologic_Museum_-_DSC07787.JPG, abgerufen am 2. April 2018)

Abb. 47
Lückenfüllerwalze, Crypto Museum, Duivendrecht (NL)
(http://www.cryptomuseum.com/crypto/enigma/img/300698/009/full.jpg, abgerufen am 2. April 2018)

Abb. 48
Anzeige der Enigma, Inv.Nr. 33304, Technisches Museum Wien

Abb. 49
Tastenfeld der Enigma, Inv.Nr. 33304, Technisches Museum Wien

Abb. 50
Schaltbild der Enigma, Schlüsselanleitung zur Chiffriermaschine Enigma, 1937, Technisches Museum Wien

Abb. 51
Chiffrierwalzen der Enigma, Inv.Nr. 33304, Technisches Museum Wien

Abb. 52
Die polnische Bomba, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Bomba_full.jpg, abgerufen am 22. November 2017)

Abb. 53
The Prof's Book: Turing's Treatise on the Enigma, 1940, Internet Archive (https://archive.org/details/hw-25-3, abgerufen am 22. November 2017))

Ausgewählte Literatur

C. H. O. D. Alexander: Cryptographic History Of Work On The German Naval Enigma, The National Archives. London 1945.

Allgemeine Schlüsselregeln für die Wehrmacht vom 1. 4. 1944, H. Dv. g. 7, M. Dv. Nr. 534, L. Dv. g. 7. Berlin 1944.

Andrew J. Avery: All the King´s Men. British Codebreaking Operations: 1938–43, Masterarbeit. Johnson City 2015.

Friedrich L. Bauer: Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie. Berlin, Heidelberg, New York 2000.

Friedrich L. Bauer: Historische Notizen zur Informatik. Berlin, Heidelberg 2009.

Patrick Beesly: Geheimdienstkrieg der britischen Admiralität 1939–1945. Frankfurt am Main, Berlin 1978.

Hans-Otto Behrendt: Rommels Kenntnis vom Feind im Afrikafeldzug. Freiburg im Breisgau 1980.

Gustave Bertrand: Enigma ou la plus grande énigme de la guerre 1939–1945. Paris 1973.

Gilbert Bloch, Ralph Erskine: Enigma. The Dropping of the Double Encipherment, in: Cryptologia, Volume X, Number 3, July 1986.

Gilbert Bloch: Enigma Before Ultra. Polish Work and the French Contribution, in: Cryptologia, Volume XI, Number 3, July 1987.

Gilbert Bloch: Enigma Before Ultra. The Polish Success and Check (1933–1939), in: Cryptologia, Volume XI, Number 4, October 1987.

Gilbert Bloch: Enigma Avant Ultra. Enigma Before Ultra, in: Cryptologia, Volume XII, Number 3, July 1988.

Gilbert Bloch: The French Contribution To The Breaking of „Enigma", in: The Enigma Bulletin, Number 1, December 1990.

Hellmut Blume (Hg.): Die Führungstruppe der Wehrmacht. Die Nachrichtentruppen in Krieg und Frieden. Stuttgart, Berlin, Leipzig 1934.

Heinz Bonatz: Die deutsche Marine-Funkaufklärung 1914–1945. Darmstadt 1970.

Heinz Bonatz: Seekrieg im Äther. Die Leistungen der Marine-Funkaufklärung 1939–1945. Herford 1981.

Anthony Cave Brown: Die unsichtbare Front. Entschieden Geheimdienste den 2. Weltkrieg? München 1976.

Stephen Budiansky: Battle of Wits. The Complete Story of Codebreaking in World War II. New York 2002.

Georg Bychelberg: Kamerad Funker. Geschichte und Einsatz des Nachrichtenwesens. Berlin 1940.

John Cairncross: The Enigma Spy. The Story of the Man who changed the Course of World War Two. London 1997.

Peter Calvocoressi: Top Secret Ultra. New York 1980.

B. Jack Copeland: The Essential Turing. The ideas that gave birth to the computer age. Oxford 2013.

John Costello, Terry Hughes: Atlantikschlacht. Der Krieg zur See 1939–1945. Bindlach 1989.

C. A. Deavours, James Reeds: The Enigma. Historical Perspectives, Part I, in: Cryptologia, October 1977.

Andreas Figl: Systeme des Chiffrierens. Graz 1926.

Final Report written by Wachmeister Otto Buggisch of OKH/Chi and OKW/Chi, TICOM 8. October 1945.

W. J. R. Gardner: Decoding History. The Battle of the Atlantic and Ultra. London 1999.

Józef Garliński: The Enigma War. The Inside Story of the German Enigma Codes and How the Allies Broke Them. New York 1980.

Gebrauchsanleitung für die Chiffriermaschine Enigma vom 12. 1. 1937, H. Dv. g. 13, L. Dv. g. 13. Berlin 1937.

Georg Glünder: Als Funker und „Geheimschreiber" im Krieg, 1941–1945, in: The Enigma Bulletin, Number 1, December 1990.

Linda Y. Gouazé: Needles and Haystacks. The Search for Ultra in the 1930´s (An Excerpt), in: Cryptologia, Volume XI, Number 2, April 1987.

Stephen Harper: Kampf um Enigma. Die Jagd auf U-559. Hamburg 2004.

Harry Hinsley, Alan Stripp: Codebreakers. The inside story of Bletchley Park. Oxford 2001.

Karl Otto Hoffmann: Die Geschichte der Luftnachrichtentruppe, Band I: Die Anfänge – von 1935–1939. Neckargemünd 1965.

Karl Otto Hoffmann: Die Geschichte der Luftnachrichtentruppe, Band II – Der Weltkrieg, Teil 1: Der Flugmelde- und Jägerleitdienst 1939–1945. Neckargemünd 1968.

Otto J. Horak: Andreas Figl. Altmeister der österreichischen Enträtselungskunst und kryptographischen Wissenschaft, Leben und Werk 1873–1967. Wien 2005.

Otto J. Horak: Was übrig blieb. Kommentare und Dokumente zu Andreas Figl, Leben und Werk 1873–1967. Wien 2005.

David Kahn: The Codebreakers. The Comprehensive History of Secret Communication from Ancient Times to the Internet. New York 1996.

Hans Georg Kampe: Nachrichtentruppe des Heeres und der Reichspost. Militärisches und staatliches Nachrichtenwesen in Deutschland 1830 bis 1945. Waldesruh bei Berlin 1999.

Zdzisław J. Kapera: Bericht des Obstlt. i. G. K. G. Langer: Funkaufklärung der Alliierten im Frankreichfeldzug 1940, in: The Enigma Bulletin, Number 1, December 1990.

Rudolf Kippenhahn: Verschlüsselte Botschaften. Geheimschrift, Enigma und Chipkarte. Reinbek bei Hamburg 2003.

Wladyslaw Kozaczuk: Geheimoperation Wicher. Polnische Mathematiker knacken den deutschen Funkschlüssel „Enigma“. Erlangen 1999.

Wladyslaw Kozaczuk: Enigma Solved, in: Cryptologia, Volume VI, Number 1, January 1982.

Kurzsignalheft 1944, M. Dv. Nr. 96. Berlin 1944.

Ronald Lewin: Entschied Ultra den Krieg? Alliierte Funkaufklärung im 2. Weltkrieg. Koblenz, Bonn 1981.

Kenneth Macksey: Without Enigma. The Ultra and Fellgiebel Riddles. Shepperton 2000.

A. P. Mahon: The History Of Hut Eight 1939–1945, The National Archives. London 1945.

Sinclair McKay: The Secret Life of Bletchley Park. The WWII Codebreaking Centre and the Men and Women Who Worked There. London 2010.

Fritz Niederlein: „mb1 kampfbereit". Kampferlebnisse von Nachrichtensoldaten. Aus eigenen Kriegserlebnissen und Erlebnisschilderungen der Truppe. Berlin 1941.

Albert Praun: Soldat in der Telegraphen- und Nachrichtentruppe. Würzburg 1965.

Albert Praun, Kunibert Randewig: Eine Untersuchung über den Funkdienst des russischen, britischen und amerikanischen Heeres im Zweiten Weltkrieg vom deutschen Standpunkt aus, unter besonderer Berücksichtigung ihrer Sicherheit. Bonn 1999.

Michael Pröse: Chiffriermaschinen und Entzifferungsgeräte im Zweiten Weltkrieg. Technikgeschichte und informatikhistorische Aspekte, Dissertation. Leipzig 2004.

Elisabeth Rakus-Andersson: The Brains behind the Enigma Code Breaking before the Second World War, in: Bernhelm Booß-Bavnbek, Jens Høyrup (Hg.): Mathematics and War. Basel, Boston, Berlin 2003.

Marian Rejewski: How Polish Mathematicians Deciphered The Enigma, in: Annals of the History of Computing, Volume III, Number 3, July 1981.

Reservehandverfahren Allgemein R. H. V. Allg., M. Dv. Nr. 929/1. Berlin 1940.

Jürgen Rohwer: Der Einfluss der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges, in: Vierteljahresschrift für Zeitgeschichte, Heft 8/1979.

Jürgen Rohwer, Eberhard Jäckel (Hg.): Funkaufklärung und ihre Rolle im 2. Weltkrieg. Stuttgart 1979.

Tony Sale (Hg.): The US 6812th Division Report On The British Bombe, 1944. Bletchley Park Museum 2002.

Schlüsselanleitung zur Chiffriermaschine Enigma vom 8. Juni 1937, H. Dv. G. 14, M. Dv. Nr. 168, L. Dv. G. 14. Berlin 1937.

Schlüsselanleitung zur Schlüsselmaschine Enigma vom 13. 1. 1940, H. Dv. g. 14, M. Dv. Nr. 168, L. Dv. g. 14. Berlin 1940.

Der Schlüssel M. Verfahren M Allgemein, M. Dv. Nr. 32/1. Berlin 1940.

Klaus Schmeh: Die Welt der geheimen Zeichen. Die faszinierende Geschichte der Verschlüsselung. Dortmund 2004.

Klaus Schmeh: Enigma-Zeitzeugen berichten, Teil 1. Eine Ansammlung von spinnerten oder genialen Individuen, in: http://www.heise.de/tp/r4/artikel/20/20605/1.html

Alfons Schulz: Drei Jahre in der Nachrichtenzentrale des Führerhauptquartiers. Stein am Rhein 1996.

Hugh Sebag-Montefiore: Enigma. The Battle for the Code. London 2002.

Signalschlüssel für den Funksignaldienst. Berlin 1939.

Simon Singh: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. München 2004.

Michael Smith: Enigma entschlüsselt. Die „Codebreakers" von Bletchley Park. München 2000.

Alan M. Turing, The Prof's Book (Turing's Treatise On The Enigma), The National Archives. London 1940.

Siegfried Türkel: Chiffrieren mit Geräten und Maschinen. Eine Einführung in die Kryptographie. Graz 1927.

Heinz Ulbricht: Die Chiffriermaschine Enigma. Trügerische Sicherheit. Ein Beitrag zur Geschichte der Nachrichtendienste, Dissertation. Braunschweig 2005.

Die Wehrmachtschlüssel vom 13. 1. 1940, H. Dv. g. H., M. Dv. Nr. 390, L. Dv. g. H. Berlin 1940.

Gordon Welchman: The Hut Six Story. Breaking the Enigma Codes. London 1982.

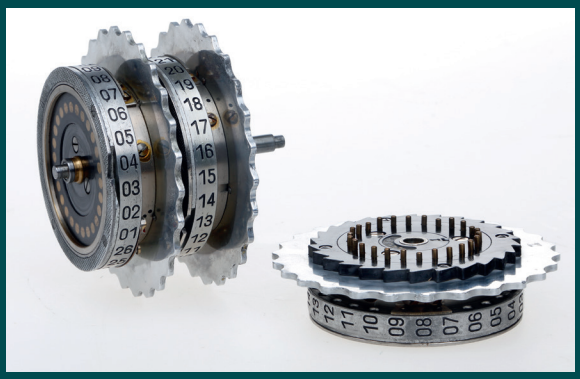
Karl Heinz Wildhagen: Erich Fellgiebel. Meister operativer Nachrichtenverbindungen. Ein Beitrag zur Geschichte der Nachrichtentruppe. Hannover 1970.

Brian J. Winkel, Cipher A. Deavours, David Kahn, Louis Kruh (Hg.): The German Enigma Cipher Machine. Beginnings, Success, and Ultimate Failure. London 2005.

Frederick Winterbotham: Aktion Ultra. Frankfurt am Main, Berlin 1976.

Richard Woytak: Polish Military Intelligence and Enigma, in: East European Quarterly, XXV, Number 1, March 1991.

Richard Woytak: On the Border of War and Peace. Polish Intelligence and Diplomacy in 1937–1939 and the Origins of the Ultra Secret. New York 1979.



„Top Secret Ultra“ war die Geheimhaltungsstufe, die im britischen Bletchley Park galt, wo Mathematiker und Ingenieure fieberhaft daran arbeiteten, die Codes der deutschen Chiffriermaschine Enigma zu knacken, um den militärischen Funkverkehr von Hitlers Wehrmacht mitlesen zu können. Gleichzeitig fühlte man sich auf deutscher Seite mit der Wundermaschine, die eine astronomisch hohe Zahl an Verschlüsselungsmöglichkeiten erzeugte, lange Zeit vor ungebetenen Lauschern sicher. Zu Unrecht, wie sich Jahrzehnte nach dem Krieg herausstellte.

Der vorliegende Band rekapituliert die spannende Geschichte der mittlerweile berühmt gewordenen Enigma, beschreibt, wie sie funktionierte, wie sie eingesetzt und letztlich auch geknackt wurde.

9 783903 242012