“The secret weapon that won the war” – Inwiefern war die Entschlüsselung der Enigma Maschine tatsächlich so ausschlagegebend für den Sieg der Alliierten im Zweiten Weltkrieg?

Inhalt

Einleitung

Anfänge der Enigma Maschine

Die Funktionsweise der Maschine (Informatik)

Die Nutzung der Enigma im Krieg

Die Entschlüsselung der Maschine

Die Auswirkungen der Entschlüsselung der Enigma auf den Verlauf des Krieges

Andere Wendepunkte des Krieges (Stalingrad, D-Day, Midway)

Fazit

**Einleitung**

8. März 2022. Der *Guardian* bekommt ein aufgezeichnetes Telefonat[[1]](#footnote-1) zwischen zwei russischen FSB-Offizieren durch das ukrainische Verteidigungsministerium zugespielt. In diesem Mitschnitt sprechen die Offiziere nicht nur über den angeblichen Tod des russischen Generals Vitaly Gerasimov, sondern beschweren sich auch über den akuten Ausfall des 2021 durch das russische Verteidigungsministerium vorgestellte abhörsichere Telekommunikationssystem *Era.* Andere Quellen [[2]](#footnote-2) berichten, dass das russische Militär aus diesem Grund auf reguläre, SIM-Karten basierte Mobiltelefone sowie VHF bzw. unverschlüsselte, hochfrequente Radiokommunikation zurückgreift. Laut den Aussagen zweier Offizieller des US-Militärs gegenüber der NYT [[3]](#footnote-3), wurde mindestens ein russischer General aufgrund eines abgefangen, unverschlüsselten Telefonats, welches seine Position verriet, durch Ukrainische Truppen getötet. Zwei Tage nach dem verheerenden Einschlag der amerikanischen HIMAR-Raketen in Donetsk[[4]](#footnote-4) am Neujahrstag diesen Jahres, welche den Tod von mehreren Dutzend russischen Soldaten zur Folge hatte, äußert sich das russische Verteidigungsministerium[[5]](#footnote-5) und nennt als Hauptgrund für diesen, aus russischer Sicht katastrophalen Schlag, die Benutzung von unverschlüsselten Mobiltelefonen seitens der russischen Soldaten.

Wieder einmal zeigt sich, wie verheerend der Verlust von militärstrategisch relevanten Informationen in einem Krieg sein kann und wie dieser Verlust auch oft mit dem Verlust von Menschenleben korreliert. Die russische Armee ist momentan als ein perfektes Negativbeispiel bezüglich der innermilitärischen Kommunikation zu verstehen und legt dar, wie wichtig sichere, verschlüsselte Kommunikationsmittel in einem militärischen Konflikt sind.

Diese Erkenntnis ist jedoch nicht neu, sondern war bereits den Beteiligten des ersten Weltkriegs bewusst. Nachdem Ende des 19. Jahrhunderts das Prinzip der Telegrafie im öffentlichen Bereich aber auch in militärischer Hinsicht großen Anklang fand[[6]](#footnote-6), stellte sich unweigerlich die Frage nach einer möglichst effizienten und sichere Verschlüsselungsmethode, die auf die Telegraphie angewandt werden konnte. Der Erste Weltkrieg gilt deshalb als einer der ersten großen militärischen Konflikte, in welchem die Möglichkeiten der Kryptoanalyse also die Entschlüsselung von chiffrierten Nachrichten erprobt und weiterentwickelt wurde. Eine damals gängige Verschlüsselungsmethode, welche auch durch das deutsche Heer im ersten Weltkrieg angewandt wurde, war das Verwenden sogenannter Codebücher. Vereinfacht gesagt waren dies Verzeichnisse die den meisten gängigen Wörtern sowie Zahlen bestimmte Zeichenkombinationen also Codes zuordneten. Das enorme Risiko einer Dechiffrierung der durch dieses kryptographische Verfahren verschlüsselten Nachrichten liegt wohl auf der Hand: Geraten diese Codebücher auch nur in Teilen an den Feind können die Botschaften unter vergleichsweise geringem Aufwand zuverlässig entschlüsselt werden. Genau dieser Fall ist bei einem 1917 durch den deutschen Außenminister Arthur Zimmermann versandten Telegramm (Zimmermann-Depesche) an die deutsche Botschaft in Mexico eingetreten, nachdem drei deutsche Codebücher bereits 1914, im Zuge der russischen Bergung der SMS-Magdeburg, in feindliche Hände gefallen waren[[7]](#footnote-7). Die Dechiffrierung der Brieten dieses Telegramms wahr aus deutscher Sicht verehrend für den weiteren Verlauf des Krieges. Es versprach der Mexikanischen Regierung territoriale Gewinne Innerhalb der Vereinigten Staaten von Amerika, sollten sie sich auf deutsche Seite schlagen. Das Bekanntwerden dieser brisanten Informationen sorgte letztendlich für den Kriegseintritt der Vereinigten Staaten [[8]](#footnote-8)in den Ersten Weltkrieg und besiegelte damit die Niederlage der Mittelmächte. Da die deutschen Militärs einer Wiederholung dieses kryptographischen Desasters unbedingt entgegenwirken wollten[[9]](#footnote-9), sahen sie sich gezwungen auf neue Möglichkeiten der Verschlüsselung zurückzugreifen und entschieden sich schließlich für die Rotor-Chiffriermaschine Enigma welche heute besonders durch den Roman „Enigma“ von Robert Harris sowie den 2015 erschienen Film „The Imitation Game“ mediale Aufmerksamkeit erlangte. Im Verlauf des Zweiten Weltkrieges wurde jedoch auch dieses kryptographische Verschlüsselungsverfahren der deutschen durch die Alliierten dechiffriert, mit dem Unterschied, dass die Achsenmächte diesmal über diesen Sachbestand im Dunkeln gelassen wurden und die Entschlüsselung der Maschine erst im Jahre 1974 durch die Veröffentlichung des Buches „The Ultra Secret“ von F. W. Winterbotham bekannt wurde.

Im der Folgenden Arbeit werde ich mich mit genau dieser Maschine sowohl in geschichtlicher, als auch informationstechnischer (informatischer) Sicht bezogen auf die Problemfrage (“The secret weapon that won the war” – Inwiefern war die Entschlüsselung der Enigma Maschine tatsächlich so ausschlagegebend für den Sieg der Alliierten im Zweiten Weltkrieg?) auseinandersetzen, um am Ende ein abschließendes Urteil über die militärstrategische Relevanz der, durch die Entschlüsselung der Enigma Maschine, erlangten Informationen, für die Alliierten, fällen zu können.

**Anfänge**

Entgegen mancher Annahmen, ist die Enigma Maschine keineswegs eine Erfindung die speziell für den militärisch-strategischen Gebrauch im Zweiten Weltkrieg konzipiert wurde, sondern hat ihre Anfänge bereits wesentlich früher zu Zeiten des Ersten Weltkriegs. Tatsächlich beschreibt der Name „Enigma Maschine“ eine ganze Serie von Geräten was konträr zur häufig benutzten Phrase „*Die* Enigma Maschine“ steht. Als Erfinder dieser Maschinen gilt der deutsche Ingenieur und Elektrotechniker Arthur Scherbius, welcher gegen Ende des ersten Weltkriegs an eine Chiffrier- und Dechiffriermaschine arbeitete, bevor er am 23 Februar 1918 sein erstes Patent für selbige Einreichte[[10]](#footnote-10). Noch im gleichen Jahr stellt Scherbius seine Erfindung der Reichs-Marine Führung vor, welche schon damals eine „gute Schlüsselsicherheit“ selbst bei einer Kompromittierung der Maschine anerkennt[[11]](#footnote-11). Trotzdem sieht das Reichs Marineamt von einer weitgehenden Anschaffung jener Maschine ab und begründet diese Entscheidung damit, dass sich die Anwendungen von Enigmen für die Art des „Marine-Schlüsselverkehrs“ nicht als lohnenswert erweisen würde[[12]](#footnote-12). Nach dieser Absage durch das Militär, versucht Scherbius seine Erfindung für den wirtschaftlich-kommerziellen Bereich attraktiv zu machen. Zu diesem Zweck wurde im Jahre 1923 die Chiffriermaschinen Aktiengesellschaft gegründet, welche die Geräte auf dem zivilen Markt bewerben und vertreiben sollte. Auf dem 1924 stattfindenden Weltkongress der internationalen Postunion in Bern hatte Scherbius mit seiner anfangs noch klobigen, Typ A Enigma Maschine nur begrenzten Erfolg, sodass kurz darauf die Enigma B (1923) und wenig später die Enigma C (1926) folgte, welche von Aufbau und Funktion bereits stark an diejenigen Enigma Maschinen erinnert, welche im Zweiten Weltkrieg durch Nazi-Deutschland verwendet wurden. Wie bereits erwähnt handelt es sich hierbei um eine Rotor-chiffrier- und dechiffrier-Maschine, welche drei sogenannte Rotoren (später Walzen) besitz, die die Aufgabe haben, den eingegebene Buchstaben mittels ihrer unterschiedlichen Verdrahtungen zu einem anderen Buchstaben zu verschlüsseln. Die Enigma Typ C enthält als eine Neuerung[[13]](#footnote-13) bereits die, von einem Mitarbeiter Scherbius, Willi Korn[[14]](#footnote-14) erfundene, sogenannte Umkehrwalze, die ursprünglich zur Erhöhung der Kryptographischen Sicherheit eingebaut wurde. Diese Umkehrwalze sorgt dafür, dass der Strom die drei Rotoren nicht nur einmal sondern jeweils zweimal (also in Umgekehrter Reihenfolge) durchlief. Korn schreibt in seinem Patent[[15]](#footnote-15) was 1928 ausgestellt wurde, dass durch den Einbau dieser Walze eine zusätzliche „Verwürfelung“ stattfindet, was die kryptographische Sicherheit zusätzlich erhöhen würde. Diese Annahme soll sich jedoch später als katastrophale Fehleinschätzung durch Korn herausstellen, da besagte Umkehrwalze heute als kryptographische Hauptschwäche der Maschine angesehen wird.

Tatsächlich weckte die Enigma Typ C Jahre 1926 also acht Jahre später erneut das Interesse der Marine[[16]](#footnote-16). Diesmal wurden die Geräte, unter minimalen Veränderungen durch die Militärs, auch großflächig unter dem Namen „Funkschlüssel C“ eingeführt. Zwei Jahre später adaptierte auch das Reichsheer die Maschine, welche wiederum leicht verändert wurde und als „Enigma-G“ bekannt wurde.[[17]](#footnote-17) Die wichtigste Neuerung dieses Geräts markiert das hinzugefügte Steckerbrett, welches das Individuelle vertauschen von Buchstaben, zusätzlich zu den Rotoren erlaubte.[[18]](#footnote-18)

Kurz darauf verschwanden die Enigma Modelle der Chiffriermaschinen Aktiengesellschaft vom zivilen Markt [[19]](#footnote-19)und die Enigmen wurden nun in großen Mengen gefertigt und an das Militär vertrieben, welche die Maschinen sogleich in Betrieb nahm. Die britischen Kryptoanalytiker, welche auch noch lange nach dem Ende des ersten Weltkriegs den Funk der der deutschen abhörten und entschlüsselten, wurden ab 1926 plötzlich mit Funksprüchen konfrontiert, die mit keiner ihnen, bis dahin bekannten, Verschlüsselung chiffriert waren. Nach gescheiterten Versuchen diese Enigma Verschlüsselung zu brechen gaben es die Briten zunächst auf, den deutschen Funk mitzuhören[[20]](#footnote-20). Auch die französischen und amerikanischen Kryptologen wurden durch den Einsatz der Enigma vor ein scheinbar unlösbares Rätsel gestellt, was die Funksprüche der deutschen Betraf.

Immer mehr Enigmen kamen jetzt zum Einsatz und wurden auch in anderen Anwendungsbereichen eingesetzt, so etwa in der deutschen Verwaltungsstruktur und auch der Reichsbahn[[21]](#footnote-21). Schätzungen zu Folge hat allein das Militär bis Kriegsende über 30.000 Maschinen erworben[[22]](#footnote-22). Im Jahre 1934 führte das Heer die nochmals verbesserte Enigma 1 ein, welche dann später auch bei der 1935 gegründeten Luftwaffe zum Einsatz kam. Die Kriegsmarine zog noch im selben Jahr mit der „Enigma 1“ ähnlichen Maschine „Funkschlüssel M“ bzw. „Enigma M1“ nach.[[23]](#footnote-23) Der wichtigste Unterschied zwischen den beiden Maschinen lag in der Anzahl und Verwendung der Walzen (Rotoren). Während die Enigma 1 des Heeres fünf Walzen besaß, von welchen bis 1938 nur die ersten drei benutz werden durften, hatte die Enigma M1 der Marine von Anfang an sechs Walzen, von denen keine gesperrt war. Der Hintergedanke des Generalstabes bei der vorläufigen Sperrung von Walzen lag darin, sie bei einer Mobilmachung unverzüglich einzusetzen, um gegebenenfalls erzielte Erfolge der generischen Kryptologen mit einem Schlag zunichtezumachen.[[24]](#footnote-24) Im Laufe der Jahre gab es noch viele weitere Enigmen Model, deren Untersuchung an dieser Stelle jedoch den Rahmen sprengen würde.

**Funktionsweise**

Heutzutage sind Einbruchssichere Verschlüsselungen nicht mehr wegzudenken. Das Anwendungsfeld reicht von recht einfachen Verschlüsselungen, zum Beispiel in Mails, über nahezu unknackbare Verschlüsselungsmethoden, beispielsweise beim Versenden einer Whatsapp oder beim Aufrufen einer https-Website. Tatsächlich ist das Konzept der Verschlüsselung, etwa zum Geheimhalten einer wichtigen Nachricht in Kriegszeiten sehr alt und geht bis in die Antike zurück.

Ein besonders bekanntes Beispiel für den Einsatz einer frühen Verschlüsselungsmethode ist die sogenannte Caesar Verschlüsselung. Caesar soll damals diese Methode verwendet haben, um seine Truppen zu koordinieren, ohne Gefahr zu laufen seine Strategie an den Feind preiszugeben. Hierbei werden vereinfacht gesagt zwei Alphabete übereinandergeschrieben, wobei das untere der Beiden um drei Buchstaben nach links verschoben wird, sodass unter dem A nun kein A, sondern ein D steht usw. Damit wurde also einem Klartext Buchstabe immer ein anderer Buchstabe des Alphabets zugewiesen, um die Verschlüsselung der Nachricht zu gewährleisten. Eine solche Art der Verschlüsslung bezeichnet man als Monoalphabetische Substitution (Ersetzung) von Buchstaben. Ein Ausgangsalphabet wird dementsprechend mit genau einem anderen Alphabet, einer sogenannten Permutation des Ausgangsalphabets verschlüsselt. Für jeden Buchstaben wird genau ein anderer Buchstabe verwendet. Das bedeutet, dass das K immer mit dem gleichen Buchstaben verschlüsselt wird, zum Beispiel dem C.

Das Kerckhoffsche Prinzip ist ein wichtiger Grundsatz der Kryptographie und besagt „Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.“ Im Falle der Caesar Verschlüsselung würde dieser Satz jedoch nur bedingt bzw. gar nicht zutreffen, da der Schlüssel durch die Verschlüsselung mit einer Verschiebung des Alphabets um drei Stellen bereits bekannt ist. Doch auch eine andere, wahllos gewählte Monoalphabetische Verschlüsselung ist etwa durch Häufigkeitsanalysen leicht zu brechen. Hierbei werden vor allem Linguistische Anomalien im Verschlüsselten Text betrachtet. Kommt zum Beispiel ein Buchstabe sehr häufig vor dann ist bei einem ausreichend langen Text davon auszugehen, dass es sich hierbei um ein E handeln muss, welches in der deutschen Sprache den häufigsten Buchstaben markiert. Die Nazis mussten sich also eine etwas raffiniertere Methode einfallen lassen, um ihre Nachrichten zu chiffrieren.

Um zu verstehen, wie es letztendlich gelungen ist, den Enigma Code im Vergleich zu händischen Verschlüsselungsmethoden so sicher zu gestalten und wie dieser dennoch geknackt wurde, gilt es zunächst sich mit dem Grundsätzlichen Aufbau und der Funktionsweise einer solchen Enigma Maschine zu befassen. Wie bereits im Obigen angerissen handelt es sich bei Scherbius Erfindung um eine sogenannte Rotor Chiffrier- und Dechiffrier-Maschine. Wie der Name schon vermuten lässt, findet die hauptsächliche Verschlüsselungsarbeit in den sogenannten Rotoren (Walzen) statt. Jede Walze hat auf der Außenseite die 26 Buchstaben des Alphabets eingraviert und besitzt auf beiden jeweils Seiten ebenso viele Schleifkontakte, die bei richtiger Ausrichtung in Relation zur darauffolgenden Walze den Stromkreis zu dieser Walze schließen. Tatsächlich funktionierte die Enigma Maschine nämlich im Grundprinzip wie ein Stromkreis, der am Ende mit einer Lampe verbunden wurde. Innerhalb jeder Walze fand die Verdrahtung der Schleifkontakte auf den gegenüberliegenden Seiten statt, wobei jeder Kontakt auf der einen Seite willkürlich mit genau einem Kontakt auf der anderen Seite verbunden wurde. Jede Walze hatte ihre individuelle Verdrahtung. Bei der Enigma 1 auf welche ich mich in der folgenden Erklärung beschränken werde, gab es fünf unterschiedlich verdrahtete Walzen, von denen der Chiffreur nach Belieben drei auswählen und in die dafür vorgesehene Einlassung im hinteren Teil der Maschine einsetzen kann. Dabei lassen sich die Walzen beliebig in eine von 26 Positionen drehen. Das kleine Sichtfenster, welches bei geschlossener Abdeckung direkt über den drei Rotoren liegt, gibt den Blick auf den Obersten Buchstaben eines jeden Rotors frei. Außerdem gab es eine sogenannte Umkehrwalze, welche ebenfalls eine zufällige innere Verdrahtung besaß. Drückte man eine Taste dann wurde der Stromkreis zur Batterie der Maschine geschlossen. Angenommen es wurde zum Beispiel die Taste H gedrückt dann lief der Strom zunächst durch das H-Kabel in die Eingangswalze mit dem Schleifkontakt H. Der gegenüberliegen Schleifkontakt gehört zum ersten Rotor (Walze) und ist je nach Position des Rotors ein anderer. So kommt es, dass der Strom in den ersten Rotor schon nicht mehr als H sondern als ein S eintritt. Durch die Innere Verdrahtung des Rotors wird dafür gesorgt, dass der Strom (in der Regel) nicht am gegenüberliegen Kontakt, sondern einen willkürlichen Kontakt auf der anderen Seite austritt. Von dort aus findet eben beschriebenes zwei weitere Male statt: der Strom tritt wieder in den gegenüberliegenden Schleifkontakt der nächsten Walze ein, etwa dem F Kontakt und verlässt sie durch einen anderen Schleifkontakt auf der gegenüberliegenden Seite. Schließlich ist der Strom durch die Letze Walze hindurch, wurde über den K Draht aufgenommen und tritt nun in Umkehrwalze als ein A ein. Diese Walze unterscheidet sich insofern von den anderen, als dass sie nur auf einer Seite Schleifkontakte hat und die einzelnen Buchstaben paarweise verbunden sind, das heißt, dass die Umkehrwalze beispielweise ein A immer mit einem X ersetzt und umgekehrt ein X immer als ein A verschlüsselt wird.[[25]](#footnote-25) Von hier aus durchläuft der Strom alle Walzen noch einmal Rückwärts, bis zur Eingangswalze. In unserem Beispiel nehmen wir an der Buchstabe X in der Umkehrwalze wurde zunächst als ein T, dann ein I und Z verschlüsselt und tritt wieder in die Eintrittswalze als ein U ein. Von hier aus läuft der Strom über das U Kabel über die Entsprechende Lampe und in die Batterie zurück, sodass der Stromkreis geschlossen ist und die U Lampe leuchtet. Die Enigma Maschine hat also erfolgreich ein H in ein U chiffriert. Dieser Aufbau alleine würde jedoch nur einen verschwindend geringen Verschlüsselungsgrad bieten und man könnte die chiffrierte Nachricht innerhalb weniger Minuten entziffern. Dies liegt daran, dass im eben beschrieben Aufbau eine Monoalphabetische Verschlüsselung (siehe Oben) stattfindet. Das heißt dass Ein H immer mit einem U chiffriert werden würde, was es dem Feinddenkbar einfach machen würde die Nachricht zu entziffern. Wie der Name „Rotor“ jedoch schon vermuten lässt, handelt es sich hierbei um ein bewegliches, drehbares Teil. Bei jedem Tastendruck dreht sich zunächst der Rotor ganz rechts um eine Position weiter. Das bedeutet, wenn man nun noch einmal die H-Taste drückt, dann wird H diesmal mit einem anderen Buchstaben verschlüsselt werden. Jeder Rotor hat nun an einer Bestimmten Stelle eine Einkerbung, die sogenannte Übertragungskerbe. Jedes Mal, wenn sich der erste Rotor bis zu übertragungskerbe gedreht hat und daraufhin eine weitere Taste gedrückt wird, dann dreht sich der Rotor links daneben einmalig um eine Position weiter. Das bedeutet, das bei drei Rotoren der Rechte sich bei jedem Tastendruck, der mittlere bei jedem 26 Tastendruck und der linke sich bei nur jedem 676 Tastendruck um eine Position weiterdreht.

Damit handelt es sich um eine Polyalphabetische Verschlüsselung da ein Buchstabe nicht mit einem sondern mit vielen verschiedenen Alphabeten verschlüsselt wird. Der Schlüssel für eine Polyalphabetische Verschlüsselung bzw. Substitution ergibt sich also aus einer Anzahl A der verschiedenen Permutationen des Ausgangsalphabets. Je mehr Permutationen verwendet werden, desto sicherer wird eine Polyalphabetische Verschlüsselung.[[26]](#footnote-26) Die hängt vor allem damit zusammen, dass es bei einer größeren Anzahl an Permutationen länger dauert bis sich das Verschlüsselungsmuster wiederholt, die sogenannte Periodenlänge ist also länger. Bei drei fest verbauten Rotoren wären dies 263 also 17 576 verschiedene Permutationen des Ausgangsalphabets. Die Periodenlänge beträgt also eben diese 17 676 Permutationen. Wie bereits erwähnt erhielten die Chiffreure nicht nur drei, sondern gleich fünf Walzen, die noch dazu auch noch unterschiedlich angeordnet werden, konnte. So wurden also zunächst drei Walzen ausgewählt, die dann in einer beliebigen Reihenfolge in die Enigma Maschine eingesetzt werden konnten. Damit ergaben sich Insgesamt 5! / 2! also 60 unterschiedliche Walzenlagen, was die Zahl der möglichen Schlüssel bzw. Alphabete auf 17 576 \* 6 also ganze 105 456 erhöhte. Dennoch war dieser Schlüsselraum immer noch im Bereich des menschlich Möglichen und konnte mit genügend Zeit und Personal geknackt werden. Deshalb entschieden sich die Deutschen für die Einführung einer weiteren Kryptographischen Hürde. An der Gerätefront wurde ein Steckerbrett installiert, welches dazu genutzt wurde mit den beiliegenden Steckerverbindungen beliebige zwei Buchstaben miteinander zu Vertauschen. Das heißt wenn etwa eine Steckverbindung vom F zum O gezogen wurde, dann waren diese Buchstaben in Beide Richtungen vertauscht. Dem Chiffreur wurde damit freigestellt bis zu 10 Steckverbindungen zu installieren, um also insgesamt maximal 20 Buchstaben zu vertauschen. Damit erweiterte sich auch der Stromkreis. Nach einem Tastendruck wurde der Strom nun erst durch das Steckerbrett, dann die Rotoren, die Umkehrwalze und die Rotoren in umgekehrter Reihenfolge und schließlich noch einmal durch das Steckerbrett geleitet, um schließlich die Entsprechende Lampe zum Leuchten zu bringen. Die „ungesteckerten“ Buchstaben blieben daher unverändert und der Strom wurde auf direktem Weg an die Rotoren bzw. die Lampe weitergeleitet. Das Steckerbrett erweiterte den Schlüsselraum um ein Vielfaches. Seit 1939 war es vorgeschrieben genau 10 Steckerverbindungen zu stecken. Unter dieser Annahme lässt sich nun die Anzahl der Möglichen Steckerverbindungen vergleichsweise einfach berechnen. Mit zehn Steckerverbindungen lassen sich also 10 Paare an Buchstaben verbinden. Für den ersten Stecker gibt es 26 Möglichkeiten, für den zweiten 25 usw. Dieser Sachverhalt lässt sich also mit 26! / 6! Beschreiben. Nun ist es aber so, dass es keine Rolle spielt ob zuerst A mit Y gesteckert wird und dann B mit Z oder umgekehrt. Die Reihenfolge, in der die Steckerpaare verbunden werden, spielt also keine Rolle. Für 10 Verbindungen gibt es also 10! Fakultät Anordnungen, die Entfallen, daher teilen wir zusätzlich durch 10! (26! / (6! \* 10!)). Zusätzlich gilt zu beachten, dass die Reihenfolge der Stecker in einem Steckerpaar ebenfalls belanglos ist. Es ist unerheblich, ob ein Steckerkabel zuerst in A und dann in Y gesteckt wird oder umgekehrt. Daher entfallen für jedes Steckerpaar noch einmal die Hälfte aller Kombinationen, dementsprechend muss durch 210 geteilt werden. Die vollständige Rechnung, um die Anzahl der möglichen Steckerverbindungen auf dem Steckerbrett mit genau zehn Steckerkabeln zu ermitteln lautet also 26! / (6! \* 10! \* 210) und ergibt 150 738 274 937 250 Möglichkeiten. Um den Schlüsselraum der Enigma zusätzlich zu erweitern war es möglich den Verdrahtungsring zu drehen und somit die innere Verdrahtung der Walzen zu verschieben. Dieses Verändern der Ringstellung sorgte dafür, dass die Übertragungskerbe der Walze relativ zur Verdrahtung verändert wurde. Damit ist die Ringstellung ebenfalls Teil des Schlüssels. Hierbei sei jedoch angemerkt, dass die ganz linke Walze die letzte ist, deren Übertragungskerbe daher kein Fortschreiten einer weiteren Walze bewirkt, weshalb nur die Ringstellungen der ersten und zweiten Walze eine Rolle für den Schlüssel spielen, sodass sich die Anzahl der Stellungen auf 676 (262) beschränkt.[[27]](#footnote-27)

Der Gesamte Schlüsselraum der Enigma 1 ergibt sich aus der Anzahl der Walzenlagen, der Ringstellung, der Walzenstellung, welche den Buchstaben im kleinen Sichtfenster der Enigma entspricht sowie natürlich der verbundenen Steckerverbindungen auf dem Steckerbrett. Damit ergibt sich ein theoretischer Schlüsselraum von 107 458 687 327 250 619 360 000 möglichen Schlüsseln. In der Realität war der Schlüsselraum etwas kleiner, da die Maschine beim Fortschalten der Rotoren eine Anomalie, den sogenannten Doppelschritt aufwies, welcher zur Folge hatte, dass die mittlere Walze zweimal hintereinandergeschaltet wurde und somit 262 bzw. 676 Möglichkeiten der Walzenstellung ausgelassen wurden.[[28]](#footnote-28) Der Tatsächliche Schlüsselraum liegt also bei 103 325 660 891 587 134 000 000 möglichen Schlüsseln (60 \* 676 16 900 \* 150 738 274 937 250). Dies entspricht einer Schlüssellänge von etwa 76 Bit und ist daher selbst mit modernen Mitteln kaum vollständig zu durchsuchen, wenn man sich auf ein einfaches Brute-Force Verfahren, daher das Ausprobieren eines jeden Schlüssels beschränkt.

Die Nazis versprachen sich von einer solchen Verschlüsselungsmaschine eine bisher nie dagewesene Sicherheit beim Versenden einer Nachricht. Scherbius Enigma besaß für ihre Zeit nicht nur einen unvorstellbar großen Schlüsselraum, sie hatte auch den enormen Vorteil, dass man nur eine Maschine sowohl zum ver- als entschlüsseln verwenden musste. Dies ist dem Einbau der Umkehrwalze durch Willi Korn zu verdanken, welche zur Folge hatte, dass in gleicher Walzenstellung Buchstaben immer paarweise verschlüsselt wurden. Das bedeutet, wenn ein A beispielsweise mit einem K verschlüsselt wurde, wurde das K in der gleichen Walzenstellung auch als ein A verschlüsselt. Die Enigma Verschlüsselung ist also involutorisch bzw. selbstinvers.[[29]](#footnote-29) Das hatte für die deutschen Chiffreure den Vorteil, dass sie aufgefangen Nachrichten sofort dechiffrieren konnten, vorausgesetzt sie kannten die Einstellung der Enigma. Diese Einstellungen waren in den Schlüsselbüchern vermerkt, welche die Tagesschlüssel für einen ganzen Monat enthielten und an jeden Chiffreur ausgeteilt wurden. [[30]](#footnote-30) Sie gehörten zu den geheimsten Dokumenten des Kriegs und wurden zu diesem Zwecke auf leicht wasserlöslichem Papier gedruckt, um eine Bergung durch den Feind aus gesunkenen Schiffen erfolglos zu machen.[[31]](#footnote-31)

Wie bereits oben erläutert besteht der Enigma Schlüssel aus vier Elementen, die sich in den Bauteilen der Enigma widerspiegeln. Die Codebücher enthielten bis zum 15 September 1938 für jeden Tag die Walzenlage, die Ringstellung sowie die Steckerverbindungen und natürlich die Walzenstellung selbst. Danach änderte sich die Vorschrift und der Tagessschlüssel bestand von nun an nur noch aus den drei Komponenten, die Walzenstellung entfiel, dafür sollten sich die Enigma Operatoren für jeden Spruch eine eigene Walzenstellung überlegen. Diese wurde zunächst im Klartext an den Empfänger versendet, bevor der eigentliche Spruchschlüssel gewählt und auf Basis dieser Grundstellung verschlüsselt und verschickt wurde. Mit diesem Spruchschlüssel wurde dann schließlich die einzelne Nachricht verschlüsselt.

**Die Entschlüsselung**

Wie bereits im vorangegangenen Abschnitt festgestellt werden konnte, ist die Maschine in ihrer Funktionsweise sehr komplex und bietet aufgrund ihres modularen Aufbaus eine Unmenge an möglichen Tagesschlüsseln. Nicht nur die verwendeten Walzen an sich, sondern auch deren Anordnung und Startposition kann verändert werden. Hinzu kommt die hohe Anzahl an möglichen Steckerverbindungen, die für zusätzliche Variation bei der Auswahl der Tagesschlüssel sorgen.

So ist es nicht verwunderlich, dass die Dechiffrierdienste der Alliierten ab 1926 mit dem erstmaligen Einsatz der Enigma beschließen, dass die Entschlüsselung dieser Maschine ein unmögliches Problem sei und kurz darauf ihre Arbeit an der Enigma Verschlüsselung einstellen. Zudem glaubte Sie, den deutschen im Ersten Weltkrieg einen so vernichtenden Schlag versetz zu haben, dass sie zu gelähmt waren, um einen erneuten Krieg zu wagen. Sie fühlten sich sicher in ihrer Stellung und sahen keinen Sinn dahinter mehr Geld, Ressourcen und Energie in die Entschlüsselung des deutschen Funkverkehrs zu stecken.[[32]](#footnote-32) Polen jedoch, den Schrecken des ersten Weltkriegs noch mehr als Präsent, sah sich zwischen den Fronten. Im Osten die kommunistisch geprägte Sowjetunion, im Westen Deutschland, gierig darauf die abgetretenen Gebiete zurückzugewinnen. In dieser Lage konnte jede Information von unschätzbarem Wert sein, sodass die Polen, nachdem sie 1928 erstmalig mit Enigma-verschlüsselten Funksprüchen in Kontakt kamen, alles daran setzten diese zu entschlüsseln[[33]](#footnote-33). Schnell erkannte man, dass es sich um ein neuartiges Maschinenschlüsselverfahren handelte, das vermutlich auf der kommerziellen Enigma, die bis 1926 auf dem zivilen Markt verkauft wurde, aufbaute[[34]](#footnote-34). Doch auch das damals erstandene Exemplar der zivilen Enigma konnte den Polen nicht weiterhelfen, da die innere Verdrahtung der Walzen sich gänzlich von der militärischen Version der Maschine unterschied[[35]](#footnote-35). Hier half den Polen das militärisches Kooperationsabkommen, welches sie 1921 mit Frankreich geschlossen hatten.[[36]](#footnote-36) Der französische Geheimdienst hatte im November 1931 zwei Geheimdokumente zur Gebrauchsweise, Funktion und Verschlüsselung der Enigma Maschine durch den deutschen Spion Hans-Thilo Schmidt zugespielt bekommen[[37]](#footnote-37). Da die Franzosen auch nach genauerer Untersuchung der Dokumente die Entschlüsselung der deutschen Enigma als ein Mammut-Problem einordneten, übergaben sie die Geheimdokumente an den polnischen Dechiffrierdienst, das Biuro Szyfröw[[38]](#footnote-38). Bis 1939 sollte es noch etwa 20 weitere Treffen zwischen Schmidt und dem Kontaktmann im französischen Geheimdienst Gustave Bertrand geben, bei welchen die Schlüsselbücher für jeweils ganze Monate übergeben wurden, bevor sie dann auf direktem Weg nach Polen überstellt wurden.[[39]](#footnote-39) Eine weitere Hilfe erhielten die Polen durch einen Glücklichen Zufall zwei Jahre zuvor. Im Januar 1929 ging ein rätselhaftes Paket beim Warschauer Zollbüro ein. Ein deutscher Botschaftsangehöriger erregte den Verdacht des polnischen Geheimdienstes, da er eine umgehende Rückgabe des Paketes forderte. Kurzerhand öffneten die Polen die Kiste und sahen sich einer deutschen Enigma gegenüber. Innerhalb von zwei Tagen wird die Maschine ausführlich analysiert und auseinandergenommen, bevor sie wieder sorgfältig eingepackt und den deutschen Diplomaten „ungeöffnet“ übergeben wird.[[40]](#footnote-40) Damit waren die Polen der Lösung des Enigma Problems schon ein ganzes Stück nähergekommen. Der damalige Hauptmann des Biuro Szyfröw Maksymilian Ciezki[[41]](#footnote-41) stellte im Jahre 1932 drei junge, deutschsprechende Mathematiker ein, um sich der Dechiffrierung der Enigma Maschine anzunehmen[[42]](#footnote-42). Der talentierteste war wohl Marian Rejewski [[43]](#footnote-43) der schon nach nur zehn Wochen eine Gleichung aufstelle, um die innere Verdrahtung der Walzen rekonstruieren zu können. Dieses Gleichungsketten enthielten jedoch noch zu viele Unbekannte, um sie in vollständig lösen zu können, weshalb er sich Ende 1932 an Ciezki wandte, der ihn, mit denen durch Schmidt erhaltenen Geheimdokumente zur Enigma, versorgte. Die darin enthaltene Gebrauchsanweisung half Rejewski einige der Unbekannten zu eliminieren und so die innere Walzenverdrahtung herauszufinden.[[44]](#footnote-44) Außerdem gelang es ihm die Verschaltung des Eingangsstators mit der Tastatur zu „erraten“, sodass die Warschauer Firma AVA mit dem Bau der ersten Enigma Nachbauten beginnen konnte.[[45]](#footnote-45) Doch ohne die verwendeten Tagesschlüssel war der Nachbau effektiv nutzlos. Die Deutschen hatten diesen Fall vorhergesehen und damit gerechnet das den gegnerischen Kryptologen früher oder später ein Exemplar der Enigma in die Hände fallen würde. Dennoch schaffte Rejewski Ende 1932/Anfang 1933 den Enigma Code des von der Marine benutzten „Funkschlüssel C“s zu knacken. [[46]](#footnote-46) Eine Möglichkeit eine Polyalphabetische Verschlüsselung zu brechen ist, wie auch bei einer Monoalphabetischen Verschlüsselung die Häufigkeitsanalyse. Der Unterschied besteht lediglich darin, dass nicht alle, sondern nur diejenigen Buchstaben, die mit derselben Permutation des Ausgangsalphabets verschlüsselt wurden sind zur Analyse betrachtet werden dürfen. Damit ist diese Methode der Entzifferung für die Enigma hinfällig, da, wie bereits oben erwähnt eine Periodenläge von 17 576 Permutationen vorliegt, sodass nur jeder 17 576 Buchstabe betrachtet werden kann und die Nachrichten nur maximal 180 [[47]](#footnote-47) und später dann 250 Zeichen [[48]](#footnote-48) betragen durften.

Die Entschlüsselung gelang ihm jedoch trotzdem auf anderem Wege, vor allem durch einen schwerwiegenden Verfahrensfehler der Deutschen: die Spruchschlüsselverdopplung. Zur damaligen Zeit setzten die deutschen Militärs bereits auf Spruchschlüssel, also eine eigene Verschlüsselung jeder Nachricht anstelle des allgemein gültigen Tagesschlüssels. Dieser wurde nun nur noch zur Entschlüsselung des, sich am Anfang jeder Nachricht befindlichen 3-stelligen Spruchschlüssels verwendet. Den von H. T. Schmidt verschafften Dokumenten war jedoch zu entnehmen, dass die Deutschen aus Gewohnheit den Spruchschlüssel immer zweimal hintereinander eingaben.[[49]](#footnote-49) Rejewski nutze diese Information und erkannte das sich immer hinter dem ersten und vierten, zweiten und fünften und dritten und sechsten Buchstaben einer jeden verschlüsselten Nachricht derselbe Klartextbuchstabe verbarg[[50]](#footnote-50). Aufgrund der Funktionsweise der Maschine erkannte er, dass sich in 21 von 26 Fällen nur die Erste der drei Walzen bewegt haben musste, da es, wie bereits erwähnt, nur 6 Buchstaben zu verschlüsseln galt.[[51]](#footnote-51)

An dieser Stelle bietet es sich an einmal auf die Relevanz der Ringstellung einzugehen. Wie im Obigen bereits beschrieben, trug die Ringstellung, zumindest in der Theorie, zu einer Vergrößerung des Enigma-Schlüsselraums um den Faktor 676 (262) bei. In der Praxis lässt sich dieser Faktor um ein Vielfaches reduzieren, wenn nicht sogar gänzlich wegstreichen. Der linke Rotor dreht, wie bereits erwähnt nur bei jedem 676 Tastendruck, es kann also angenommen werden, dass er sich im Laufe einer Nachricht von maximal 250 Buchstaben in den meisten Fällen überhaupt nicht dreht. Da die Ringstellung, stark heruntergebrochen, nur die Position der Übertragungskerbe beeinflusst, spielt sie zumindest beim mittleren Rotor keine wirkliche Rolle, da dessen Übertragungskerbe nur alle 676 Tastendrücke die linke Walze dreht. Somit muss in der Regel nur die Ringstellung der rechten Walze betrachtet werden, da sich die mittlere Walze bei jedem 26 Tastendruck, und damit innerhalb einer Nachricht mehrere Male dreht. Somit kann man die Ringstellung auf die genannten 26 Fälle herunterbrechen.[[52]](#footnote-52) Für Rejewski war sie sogar gänzlich irrelevant, da er, mit einer hinreichenden Wahrscheinlichkeit davon ausgehen konnte, dass sich bei sechs Buchstaben ohnehin nur die Rechte Walze gedreht haben musste.

Mit diesem Wissen konnte er Buchstabenketten, sogenannte Zyklen bilden[[53]](#footnote-53), die auf den Tagesschlüssel schließen ließen. Rejewski erkannte, dass die Zyklenlängen gänzlich unabhängig von den Verkabelungen am Steckerbrett waren.[[54]](#footnote-54) Damit konnte er den zu durchsuchenden Schlüsselraum auf ein vielfaches Verkleinern. Insgesamt ergaben sich den Tagesschlüssel 105 456 mögliche Einstellungen. Dies lässt sich damit begründen, dass die Enigmen, die es damals zu analysieren galt, drei Walzen (Rotoren) beherbergten, die daher in sechs verschiedenen Walzenlagen angeordnet werden konnten (3! = 3\*2\*1 = 6). Für die Schlüssel gab es pro Walzenlage 263, also 17 576 Möglichkeiten. Multipliziert mit sechs ergeben sich damit genau die, schon damals von Rejewski ermittelten 105 456 Möglichkeiten. Diese Zahl war natürlich immer noch ungemein groß, jedoch wurde die Entzifferung durch die Arbeit Rejewskis in den Bereich des menschlich möglichen gerückt. Er hatte es geschafft die Aufgabe, die die Franzosen und Engländer für ein Jahrhundertproblem halten in weniger als einem Jahr so weit zu vereinfachen, dass sie durch eine kleine Gruppe von Mathematikern gelöst werden konnte. Innerhalb eines Jahres erstelle Rejewskis Team einen Katalog an Tagesschlüsseln und die Dechiffrierung konnte beginnen.[[55]](#footnote-55) So kam es, dass das Biuro Szyfröw im Laufe des Jahres 1943 einen Großteil des deutschen Funkverkehrs mithören konnte. Ein erstes maschinelles Hilfsmittel, welches den polnischen Kryptologen zu diesem Zweck zur Verfügung stand, war das Zyklometer welches 1937 in Betrieb genommen wurde.

Knapp ein Jahr vor Kriegsbeginn am 15 September 1938 trat eine neue Betriebsvorschrift der Wehrmacht für die Enigma in Kraft. Das Prinzip der Grundstellung im Tageschlüssels entfiel, stattdessen vereinbarte der Chiffren Operator eine Grundeinstellung im Klartext und verschlüsselte mit dieser den jeweiligen Spruchschlüssel, mit welchem dann wiederum die Nachricht verschlüsselt wurde.[[56]](#footnote-56) Somit bestand der Tagesschlüssel ab diesem Zeitpunkt nur noch aus drei Komponenten. Damit wurden die mühsam von Rejewski erstellten Kataloge an Spruchschlüsseln nutzlos.[[57]](#footnote-57) Da die Spruchschlüsselverdopplung jedoch beibehalten wurde gelang es ihm einen Algorithmus zur Dechiffrierung zu entwickeln. Rejewski gab den Bau von sechs sogenannten „Bombas“ (Bomben) bei den Warschauer AVA-Werken in Auftrag, da es, wie bereits im Vorangegangen beschrieben sechs Walzenlagen gab. Diese Maschinen liefen parallel und arbeiteten die 105 456 möglichen Kombinationen innerhalb von zwei Stunden ab, sodass der deutsche Funkverkehr nun wieder abgehört werden konnte.[[58]](#footnote-58) Die polnischen Kryptologen ahnten all die Zeit nicht, dass der Oberleutnant Karol Gwido Langer des Biuro Szyfröw[[59]](#footnote-59) seit Einstellung der drei Mathematiker alles besessen hatte, um den deutschen Funk zu dechiffrieren. Wie Bereits im Vorangegangen erwähnt, übergab der Verräter Hans Thilo Schmidt bei seinen Treffen, nicht nur die Gebrauchsanweisung und die technischen Baupläne der Enigma an den französischen Geheimdienst sondern auch die Schlüsselbücher für ganze Monate. Langer hätte all die Jahre die Schlüssel problemlos benutzen können, um den gesamten deutschen Funkverkehr mitzulesen. Gewieft wie er war, wusste er jedoch, dass Schmidt eines Tages, spätestens mit dem Beginn des Krieges, keine Schlüsselbücher mehr liefern werden konnte, weshalb er Rejewski und sein Team für den Ernstfall üben ließ.[[60]](#footnote-60)

Als am 15 Dezember selben Jahres eine weitere Betriebsvorschrift zur Benutzung der Enigma durch den Wehrmacht Oberbefehl veranlasst wurde[[61]](#footnote-61) war die Kapazität des Biuro Szyfröw am Ende.[[62]](#footnote-62) Alle Chiffreure wurden zwei weitere Walzen ausgegeben. Somit gab es nun für jeden Schlüssel die Möglichkeit aus fünf zur Verfügung stehenden Walzen drei auszuwählen, womit sich die Anzahl der möglichen Schlüssel verzehnfachte (6! / 2! = 60 = 6 \* 10). Das hieß für das Biuro, dass auch 54 weitere Bombas gebaut werden mussten, um den Enigma Code in der gleichen Zeit zu knacken. Als die Verschlüsselung am 1 Januar 1939 durch die Einführung von vier weiteren Steckerverbindungen (10 statt ursprünglich 6) noch einmal verschärft wurde[[63]](#footnote-63) und kurz darauf der Nichtangriffspakt mit Polen im April selben Jahres durch die Nazis gekündigt wurde[[64]](#footnote-64), sah der Chef des Biuro Szyfröw Langer, sich und sein Land immer weiter in Bedrängnis geraten. Er sah sich dazu Berufen alles Wissen, was die Rejewski und sein Team in all den Jahren über die Enigma und ihre Entschlüsselung erarbeitet hatten an die Alliierten weiterzugeben, weshalb er am 24 Juli 1939, genau Vierzig Tage vor Kriegsbeginn Alliierte Kryptoanalytiker in das Hauptquartier des Biuro in Pyry nahe Warschau einlud.[[65]](#footnote-65) Dort übergab er den überraschten Alliierten nicht nur zwei Nachbauten der Enigma sondern auch die Baupläne für die Bomba, welche einige Wochen später unter höchster Geheimhaltungsstufe auf dem Seeweg nach London im Gepäck eines französischen Schauspielerpärchens geschmuggelt wurden.[[66]](#footnote-66)

Ab hier beginnt die Geschichte wie sie wohl heute in vielen Populärwissenschaftlichen Quellen häufig nacherzählt wird. Der unscheinbare Landsitz Bletchley Park (BP), etwa 70 Kilometer Nordwestlich von London, welcher sich heutzutage vor allem durch die Zahlreichen Romane und Filme wie beispielsweise „The Imitation Game“ (2014) großer Bekanntheit erfreut, beherbergte in der Zeit des Zweiten Weltkrieges die „Government Code and Cypher School“ um sich dem Enigma Problem anzunehmen. Nachdem der Enigma Code durch die Polen überraschend geknackt worden war, schöpften die Britischen Kryptoanalytiker neue Hoffnung. Schon nach kurzer Zeit gelang es Ihnen die polnischen Techniken zu adaptieren und ihren zehnjährigen Rückstand, bezüglich der Enigma Entschlüsselung, rasch aufzuarbeiten.[[67]](#footnote-67) Heutzutage ist die Entschlüsselung der Enigma Maschine vor allem unter dem Decknamen „Ultra“ bekannt. [[68]](#footnote-68)

Während das Gelände um Bletchley Park zu Kriegsbeginn noch etwa 200 Kryptologen beherbergte, stieg der Zahl der Beschäftigten innerhalb von 5 Jahren auf ganze 7 000 Mitarbeiter.[[69]](#footnote-69) Damit verfügte BP über weitaus mehr Mittel, sowohl was Personal, aber auch die Finanzierung von Geräten und kryptographischen Hilfsmitteln betraf. Nach nur kurzer Zeit gelang es den Kryptoanalytikern den deutschen Funkverkehr mitzulesen und die Arbeit des Biuro Szyfröw fortzusetzen. Zudem fanden Sie einige Abkürzungen, um den Entschlüsselungsprozess zu vereinfachen. So fanden sie beispielsweise bei der Analyse der gewählten Spruchschlüssel Auffälligkeiten, die auf menschliche Fehler bei der Bedienung der Maschine hindeuteten. Einige der Schlüssel entpuppten sich etwa als drei nebeneinanderliegende Buchstaben auf der Tastatur, oder wiederholten sich gar. Diese simplen Spruchschlüssel waren die Folge mangelnder Kreativität und Torheit seitens der deutschen Enigma Operatoren und erwies sich als ein perfektes Einfallstor für BP, weshalb die Kryptologen sie „cillies“ tauften, wahrscheinlich abgleitet vom englischen Wort silly (dumm/närrisch). Schnell fand man weitere solcher, durch menschliche Dummheit geschaffene, Schwachpunkte der Enigma. So war es beispielsweise vorgeschrieben, dass sich die Walzenlage jeden Tag so ändern musste, das sichergestellt war, dass keine der Walzen die gleiche Position hatte wie am Folgetag. Damit halbierte sich die die möglich Walzenkombinationen für den darauffolgende Tag und damit auch der Arbeitsaufwand der Kräfte in BP. Zudem gab es die Vorschrift, dass auf dem Steckerbrett alle Kable so gesteckt sind, dass kein Buchstabe mit seinem Vorgänger oder Nachfolger verbunden war. Die deutschen Versprachen sich dadurch eine mögliche Vertauschung beim einsetzten der Steckerkabel durch den Enigma Chiffreur zu vermeiden und senkten letztendlich die potenzielle Sicherheit der Maschine.[[70]](#footnote-70)

Auch wenn es durch diese Fehler einfacher geworden war den Tageschlüssel zu finden, basierte die Grundsätzliche Methode hinter dem Angriff immer noch auf Rejweskis Arbeit, welche sich einzig und allein auf die Spruchschlüsselverdopplung stützte. Sollten die deutschen diesen Fehler eines Tages bemerken und die Spruchschlüssel nur noch einmalig versenden dann wäre man in BP genauso Blind wie man es vor der Zusammenkunft in Pyry gewesen war.

Doch ein Mann sollte alles verändern und die Sorgen der britischen Kryptoanalytiker nehmen. Anfang September 1939 betrat Alan Turing erstmals das Gelände von Bletchley Park.[[71]](#footnote-71) Turing wurde vor allem aufgrund seines logischen Verstands und seinen mathematisch-algorithmischen Fähigkeiten rekrutiert[[72]](#footnote-72), kurz nachdem er 1936 mit seinen Überlegungen zur Turing-Maschine die damalige Mathematik revolutionierte und zu einem wichtiger Gründervater der heutigen Informatik wurde. Diese Fähigkeiten sollte er in der Abteilung des Linguisten Knox[[73]](#footnote-73) unter Beweis stellen, wo er damit betraut wurde alternative Methoden der Entschlüsselung zu finden, um die Schwäche des polnischen Verfahrens zu vermeiden.[[74]](#footnote-74) Zu diesem Zwecke sah sich Turing die bereits Entschlüsselten Funksprüche noch einmal genauer an und erkannte, dass viele der Meldungen sich sprachlich stark ähnelten. Durch die strengen militärischen Vorschriften war es möglich, bestimmte Wörter oder gar Wortgruppen innerhalb eines Geheimtextes vorherzusagen. So wurde etwa jeden Tag um kurz nach sechs ein verschlüsselter Wetterbericht versendet, der das Wort „wetter“ enthalten musste, welches immer an der gleichen Position im Text zu verorten war. Damit konnten also sechs verschlüsselten Buchstaben in einem Funkspruch, der kurz nach sechs abgefangen worden war, fast sicher das Klartextwort „wetter“ zugeordnet werden. Diese Anhaltpunkte wurden von den britischen Kryptoanalytikern „Cribs“ getauft und ersetzten in gewisser Weise die Schwachstelle der Spruchschlüsselverdopplung. Aufgrund der Involutorik der Enigma Maschine galt es nun herauszufinden, bei welcher Einstellung der Enigma Maschine, „wetter“ in die sechs bekannten verschlüsselten Buchstaben umgewandelt wurde. Wie auch schon Rejewski versuchte auch Turing den Schlüsselraum zu verkleinern, indem er die Verschlüsselung durch die Rotoren von der durch das Steckerbrett durchgeführten Verschlüsselung zu trennen versuchte. Dabei orientierte sich Turing auch an dem Prinzip der Polen, welche Buchstaben zu Zyklen verbanden. Er erkannte, dass sich die Wirkung der Steckerbretter aufhob, wenn man mehrere Maschinen miteinander verknüpft. Dies ist ebenfalls auf die Involutorik, bzw. die Umkehrwalze zurückzuführen, welche dafür sorgt, dass der Strom das Steckerbrett zweimal durchläuft (einmal beim Eintritt in die Maschine und einmal bei Austritt vor der Glühlampe).

Um dies zu verstehen, bedarf es eines Beispiels. Angenommen man verschalte zwei Enigma Maschinen so miteinander, dass immer die gleichen Eingänge miteinander verbunden waren, das heißt also auf der einen Maschine wurde der A Ausgang mit dem A Eingang der Zweiten Maschine verschalten und der A Ausgang dieser Maschine wieder mit dem A Eingang der Ersten. Dies wurde für alle Ein- und Ausgänge gemacht und ermöglichte den Beweis für die Aufhebung des Wirkens des Steckerbretts. Zwischen einen Ausgang der zweiten Maschine und den entsprechenden Eingang der ersten Maschine wurde nun eine Stromzufuhr und eine Lampe geschalten, sodass sich ein Stromkreis schloss, wenn alle Rotoren in der richtigen Position waren.

Damit dieses Konzept funktionierte, bedarf es einer Crib die eine innere Schleife enthielt, dass bedeutet, dass man, wenn das, wenn man Klartextwort und den zugehörigen Geheimtext Buchstabe für Buchstabe übereinanderschrieb eine gedachte Schleife ziehen konnte, die immer den verschlüsselten Buchstaben mit einem Klartextwort verband. Wenn etwa das Wort „wetter“ zu „tjwqho“ verschlüsselt wurde, dann ist es möglich eine Schleife zwischen Klartext und Verschlüsseltem Text zu bilden. Hierfür verbindet man das verschlüsselte t, was ursprünglich mal vom w des Klartextwortes stammte mit dem ersten t des Klartextwortes und verbindet anschließend das verschlüsselte w, in welches dieses t umgewandelt wird mit dem Klartext w und erhält eine Schleife. Dieses Gedankenexperiment mag zunächst unerheblich und abwegig wirken doch ist es nötig, um das Wirken des Steckerbretts zu eliminieren. Ausgehend von unserem Beispiel weiß man nun, dass eine Enigma Maschine in einer zufälligen Walzengrundstellung G ein w in ein t und zwei Walzendrehungen weiter, also in einer Stellung G+2, ein t in ein w verschlüsselt. Demzufolge stellen wir unsere erste Maschine also auf eine beliebige Grundstellung zum Beispiel AAA ein und unsere zweite Maschine auf diese Grundstellung zwei Umdrehungen weiter also AAC

Führen wir das Gedankenexperiment nun mit gedachten Steckerbrettern zwischen den Maschinen weiter. Dies bedeutet, dass das w in den ersten Rotor der ersten Maschine nicht mehr als w sondern als ein anderer, unbekannter Buchstabe B1 eintritt. Der Buchstabe durchläuft die Rotoren und kommt als B2 wieder heraus, bevor er erneut in das Steckerbrett eintritt und als t die erste Maschine verlässt. Dadurch, dass Buchstaben auf dem Steckerbrett immer paarweise vertauscht werden, ist es unumgänglich, dass das t in die zweite Maschine eintritt und hinter dem Steckerbrett als B2 wieder in die Rotoren eintritt. Es ist bekannt, dass aus der zweiten Maschine wieder ein w austreten soll, weshalb ebenfalls bekannt ist, dass die Rotoren den Buchstaben B2 zwangsläufig in den Buchstaben B1 Verschlüsseln müssen, da dieser über das Steckerbrett mit w verbunden ist, sodass am Ende wieder ein w aus der zweiten Maschine herauskommt.

Somit heben sich also die Steckerbetter der Maschinen gegenseitig auf und können gänzlich aus dem Aufbau entfernt werden. Damit wird der Schlüsselraum der Enigma um den Faktor 150 738 274 937 250 kleiner und beschränkt sich nun auf eine Kombination aus 17 576 Walzengrundstellungen, 60 Walzenlagen und theoretische 676 Walzenlagen wobei man diese theoretisch ebenfalls streichen könnte, da auch mit falscher Walzenlage bereits einige Textfragmente Lesbar sein sollten, wie oben bereits beschrieben. Somit lässt sich der Schlüsselraum der Enigma auf knapp eine Millionen (1 054 560) Schlüssel reduzieren. Wenn man nun also 60 Gruppen aus jeweils 2 Enigmen parallel laufen lässt, dann lässt sich der Schlüssel in angemessener Zeit herausfinden. [[75]](#footnote-75)

Doch auch mit dem Schlüssel galt es noch zwei Probleme zu lösen, die aber vergleichsweise so gut wie keiner Anstrengung bedurften. Zunächst galt es noch die Richtige Ringstellung zu finden, welche in über 50 Prozent der Fälle eine aus 26 möglicher Stellungen war, sodass der Zeitaufwand sich in Grenzen hielt. Noch einfacher war es die Verbindungen auf dem Steckerbrett zu finden, da es sich hierbei nur um eine einfache monoalphabetische Substitution handelt, welche zudem auch noch paarweise erfolgte. Bekam man als Klartext also „wteetr“ heraus dann lag es auf der Hand das die Buchstaben t und e auf dem Steckerbrett miteinander verbunden waren. Kombinierte man Turings geniale Überlegungen mit dem Wissen über die kryptographisch gesehen fatalen Vorschriften der Nazis dann lies sich die Zeit, die es brauchte, den Enigma Schlüssel zu finden noch einmal auf die Hälfte reduzieren, da wie erwähnt zum Beispiel keine Walze zweimal hintereinander an derselben Position verschaltet werden durfte.

Wie auch schon Rejewski erkannte Turing, dass man ein Maschinenschlüsselverfahren am besten mit Hilfe einer Maschine entschlüsseln konnte. Um sein Konzept zu verwirklichen, erhielt BP 100 000 Pfund[[76]](#footnote-76) und konnte so Anfang 1940 Turings Konzept einer automatischen Entschlüsselungsmaschine bei der Firma Britich Tabulating Machinery in Lechtford in Auftrag geben.[[77]](#footnote-77) Turing hatte also in nur ein paar Monaten eine Möglichkeit gefunden die Enigma Verschlüsselung zu brechen, und zwar auch dann noch, wenn die Deutschen den schwerwiegenden Verfahrensfehler der Spruchschlüsselverdopplung behoben hatten. Hierbei sei jedoch die Vorarbeit Rejewskis nicht zu vernachlässigen. Ohne das Treffen in Pyry und die daraus gewonnen Erkenntnisse hätte Turing laut Schätzungen etwa 7 Monate länger für den Entwurf seiner Entschlüsselungsmaschine gebraucht.[[78]](#footnote-78) Aufgrund der Mechanischen Ähnlichkeiten zwischen den bomby der Polen und Turings Maschine entschied man sich dieses Gerät ebenfalls Bombe (aus dem französischen) zu taufen, hierbei sei jedoch klarzustellen, dass die beiden Geräte sich von der Funktionsweise gänzlich unterschieden. Im Gegensatz zur Bomba, deren Erfolg davon abhängig war, dass möglichst wenige Buchstaben im Steckerbrett verbunden waren, konnte die Bombe auch mit beliebig vielen Steckerverbindungen operieren.

Tatsächlich hatten die Kryptoanalytiker von BP die richtigen Schlüsse gezogen und erkannt das die deutschen die Spruchschlüsselverdopplung bald einstellen würden. Dies passierte Anfang Mai vor dem Beginn des Westfeldzugs und BP sah sich erstmalig eines kompletten Blackouts gegenüber was die Funksprüche der Deutschen betraf. [[79]](#footnote-79) Dies änderte sich auch mit der Lieferung des ersten Prototyps von Turings Bombe am 14. Mai nicht, da diese viel zu langsam war, um Information von militärstrategischem Wert zu enthüllen. Erst am 8. August, als die zweite Version der Bombe geliefert wurde konnten die Briten wieder den deutschen Funkverkehr mitlesen.

Die Entschlüsselung der Enigma Maschine in Bletchley Park war keineswegs kosteneffizient, sowohl was die vielen Mitarbeiter als auch die nötigen Gelder etwa zum Bau der Bomben betraf. Um diese Ressourcen zu gewährleisten waren mächtige politische Verbündete notwendig die die Relevanz von „Ultra“ erkannten und bereit waren die erforderlichen Mittel bereitzustellen. Der wohl wichtigste Partner von BP war wohl Winston Churchill, welcher schon früh Interesse an der Entschlüsselung der Maschine zeigte. [[80]](#footnote-80) Er soll die Kryptoanalytiker mit den Worten „die Gänse, die goldene Eier legten und nie schnattern“ beschrieben haben und soll ihnen, als sie ihn auf den akuten Personalmangel im Oktober 1941 hingewiesen haben, jegliche Ressourcen, die benötigt wurden zur Verfügung gestellt haben. [[81]](#footnote-81)

Auch nachdem der Krieg gewonnen war, behielt Churchill seine Überzeugung für die Arbeit in BP und rund um Ultra bei. Dem Buch (Enigma ou la plus grande énigme de la guerre 1939–1945) des Französischen Geheimdienstmitarbeiters Gustave Bertrand, welcher, wie bereits erwähnt der Kontaktmann des deutschen Spions H.T. Schmidts war, ist zu entnehmen, dass Churchill in einem Gespräch mit König George dem VI (dem damals amtierenden König von Großbritannien) [Ultra] als „the secret weapon that won the war“ bezeichnet haben soll.[[82]](#footnote-82)

**Die Auswirkung der Entschlüsselung auf den Krieg**

Auf eben dieses Zitat bezieht sich meine Problemfrage: “The secret weapon that won the war” – Inwiefern war die Entschlüsselung der Enigma Maschine tatsächlich so ausschlagegebend für den Sieg der Alliierten im Zweiten Weltkrieg?

Nachdem nun also die Enigma Maschine und ihre Entschlüsselung ausführlich untersucht wurde, stellt sich nun unweigerlich die Frage, welche Auswirkung die Dechiffrierung auf den Zweiten Weltkrieg hatte. Zunächst lohnt es sich dabei einen Blick auf den Einsatz der Maschine zu werfen. Die Enigma in ihren unterschiedlichen Ausführungen wurde bei der Koordination im Heer, der Luftwaffe, der Kriegsmarine aber auch für die Verwaltung von offiziellen Behörden sowie der Reichsbahn genutzt.[[83]](#footnote-83)

Wie bereits in der Eileitung erwähnt, kann der Verlust von militärstrategischen Informationen in einem Krieg enorme Auswirkungen auf dessen Verlauf haben, ganz besonders dann, wenn der Feind eine Kompromittierung dieser Informationen für unmöglich hielt.[[84]](#footnote-84) So ist es nicht verwunderlich, dass viele Zeitgenossen und Historiker die Dechiffrierung der Enigma Maschine durch „Ultra“ als entscheidenden Faktor, wenn nicht sogar als den wichtigsten Umstand für den Sieg der Alliierten sehen.

So ist etwa der britische Zeitzeuge und Historiker Harry Hinseley der Meinung das die Funkaufklärung rund um Ultra den Krieg um mindestens zwei, wenn nicht sogar vier Jahre verkürzt hat[[85]](#footnote-85). Der amerikanische Historiker Harold Deutsch geht sogar noch weiter und stellt in Frage, ob die Alliierten den Krieg überhaupt ohne die nachrichtendienstlichen Erkenntnisse gewonnen hätten (“I feel that intelligence was a vital factor in the Allied victory – I think that without it we might not have won, after all.”)[[86]](#footnote-86).

Auf der anderen Seite stehen Historiker wie David Kahn, welche der Funkaufklärung ihren Beitrag zum Sieg der Alliierten fast in Gänze absprechen („I believe that even if we had had the worst intelligence and the Germans the best, we would still have defeated them.“).[[87]](#footnote-87)

Die Aussagen bezüglich der eigentlichen Auswirkungen der Entschlüsselung der Enigma Maschine reichen also vom einen bis zum anderen Extrem. Zieht man in Betracht, dass viele der bekanntesten Aussagen zu diesem Thema, welche für einen große Auswirkung der Arbeit von Ultra sprechen, von Zeitzeugen und ehemaligen Codebrechern in BP stammen, stellt sich für mich die Frage, inwieweit man sich auf diese verlassen kann. Neigen diese Zeitzeugen vielleicht dazu ihre eigene Arbeit zu beschönigen und die Auswirkungen von Ultra zu glorifizieren?[[88]](#footnote-88) Oder sorgte die schlagartige Aufdeckung der fast 30 Jahre alten Ultra-Akten 1974 für eine maßlose Überschätzung der Auswirkung dieser Institution? Der britische Historiker Noble Frankland vertritt die Meinung, dass die Bedeutung von Ultra übertrieben wurde („ULTRA, in my humble opinion, has been exaggerated in importance.“).[[89]](#footnote-89) Ebendieser Annahme möchte ich im Folgenden einmal näher Untersuchen. Dabei lohnt es sich zunächst einen Blick auf die Nordatlantikschlacht zu werfen.

Während man sich in BP bisweilen hauptsächlich auf die Funksprüche der deutschen Luftwaffe konzentrierte, blieb die Entschlüsselung der Marine Enigma zunächst aus. Dies lag vor allem an der Zahl der verfügbaren Walzen, welche schon im Juli 1939 auf ganze acht Stück erhöht wurde und eine Entschlüsselung damit enorm Zeitaufwändig machte, ganz abgesehen davon, dass die Verdrahtung der drei neuen Walzen unbekannt war.[[90]](#footnote-90)

Wie auch schon im ersten Weltkrieg beriefen sich die Engländer zu Kriegsbeginn auf eine Versorgung auf dem Seeweg durch Militär Konvois aus den USA. [[91]](#footnote-91) Die deutschen erkannten dies als Schwachstelle und versuchten von Beginn an die britischen Versorgungswege gezielt anzugreifen und Großbritannien somit massiv zu Schwächen. Diesen Seekrieg, welcher Hauptsächlich zwischen den Kräften der Royal Navy und denen der Kriegsmarine stattfand, bezeichnet man aufgrund seiner geographischen Verortung als (Nord-)Atlantikschlacht.

Als Karl Dönitz, Großadmiral und Oberbefehlshaber der Kriegsmarine eine neue Strategie zur Koordination und Angriffstaktik der deutschen U-Boote (Rudeltaktik) entwickelte, um die britischen Geleitzüge anzugreifen, geriet Großbritannien zunehmend in Bedrängnis. [[92]](#footnote-92) Zwischen Juni 1940 und Juni 1941 wurde monatlich etwa 50 Schiffe durch die deutsche Kriegsmarine versenkt, die meisten im Zuge des deutschen U-Boot-Kriegs. [[93]](#footnote-93) Die Briten erkannten, dass ein solcher Krieg ein hohes Maß an innermilitärischer Kommunikation erforderte und die deutschen diese Kommunikation nur über dem Funkweg abwickeln konnten.[[94]](#footnote-94)

Da eine ausführliche Analyse der Marine Enigma zu zeitaufwändig war,[[95]](#footnote-95) besann man sich auf die Lehren, die man aus dem Fall Hans Thilo Schmidt gezogen hatte. War ein Problem nicht durch geistige Anstrengung zu lösen dann musste man sich die fehlenden Informationen auf anderem Wege beschaffen. Im Zuge dessen wurden von Anfang 1940 bis 1941 gezielte Überfälle und Kaperungen von feindlichen Schiffen durchgeführt in der Hoffnung entscheidende Schlüsselunterlagen zu erbeuten. (evtl. weiter ausführen?)[[96]](#footnote-96) Dies gelang und man konnte die verbleibenden drei Walzen in ihrer Verdrahtung rekonstruieren, sodass man Mitte 1940 bereits erste Funksprüche mitlesen konnte. [[97]](#footnote-97) Im Laufe einiger Monate wurden die Kryptoanalytiker in BP aufgrund weiterer erfolgreicher Kaperungen und technischen Fortschritten immer schneller darin die Funksprüche der U-Boote mitzulesen.[[98]](#footnote-98) Dadurch war es möglich die Positionen der deutschen U-Boote herauszufinden und den britischen Geleitzügen sichere Alternativ-Routen anzubieten, um den U-Booten weitestgehend zu entgehen.[[99]](#footnote-99)

Diese Umleitung der Konvois[[100]](#footnote-100) durch die aus Ultra gewonnen Informationen in der Nordatlantikschlacht wird von einigen Historikern und Zeitzeugen als Paradebeispiel für den Erfolg von Ultra genutzt[[101]](#footnote-101), doch Konkrete Zahlen, die die Wirksamkeit der Funkaufklärung belegen, werden nur selten genannt. Jürgen Rohwer, Militärhistoriker und ehemalige Professor an der Universität Stuttgart, ist einer der wenigen, der versucht seine Aussagen über den Relevanz Ultras in der Atlantikschlacht mit Zahlen zu belegen.

Als Beispiel hierfür nutz er die Einführung der Marine Enigma M4 Anfang Februars 1942 unter dem Decknamen Triton, welche für ein Blackout in BP sorgte. [[102]](#footnote-102) Während im Jahre 1941 im Zeitraum Juni bis Dezember zwischen vier und 18 Prozent der britischen Konvois durch deutsche U-Boote abgefangen werden konnten, erhöhte sich die Zahl der Abgefangenen Geleitzüge in der zweiten Hälfte von 1942 also nach der Einführung des Funknetzes Triton auf 34 Prozent.[[103]](#footnote-103)

Als im Dezember 1942 aufgrund einiger grober Fehler bei der Bedienung der M4 deren Entschlüsselung in BP erstmalig gelang,[[104]](#footnote-104) soll sich die Sichtung von Konvois im Januar 1943 auf etwa 20 Prozent reduziert haben, so Rohwer[[105]](#footnote-105)

In sich scheinen diese Zahlen Schlüssig zu sein und den Erfolg der Konvoi-Umleitungen durch die aus den deutschen Funksprüchen gewonnenen Informationen zu beweisen.

Wirft jedoch einen Blick auf andere Quellen dann scheinen selbst diese durch Zahlen belegte Sachverhalte zweifelhaft. Eine aktuelle Ausarbeitung von Adam, Paul J.,[[106]](#footnote-106) welche 2017 veröffentlicht wurde und sich explizit mit denen bis dahin angenommenen Fakten bezüglich der militärischen Relevanz der Ultra Aufklärung beschäftigt, widerspricht Rohwer in seiner Begründung für die erhöhte Sichtungsrate britischer Konvois im Jahre 1942. Diese hinge nicht unbedingt mit dem Blackout von BP zusammen, sondern würde sich auf viele Faktoren Gründen wie etwa die erhöhte Anzahl an deutschen U-Booten, die ab Mitte 1942 zur Verfügung standen. Dies wird anhand von zwei Grafiken belegt welche sowohl die Versenkungsrate britischer Konvois durch deutsche U-Boote als auch die Anzahl an verfügbaren deutschen U-Booten aufzeigen. Legt man die beiden Kurven übereinander dann ist tatsächlich eine Korrelation dieser zu verzeichnen. Der Anstieg der Versenkungen in der Zweiten Hälfte des Jahres 1942 ist fast identisch mit dem Anstieg der Anzahl der U-Boote. Als weitere Gründe werden längere Patrouillenzeiten der deutschen U-Boote sowie die Lösung einiger schwerwiegenden Probleme mit den Torpedosystemen der Boote genannt.

Doch selbst wenn Rohwer mit seiner Begründung recht behält, und die Sichtungsrate der Konvois tatsächlich zu gewissem Teil von der Enigma Entschlüsselung abhängig war, ist es wichtig darauf hinzuweisen, dass in einigen Fällen der Arbeit in BP aufgrund von semantischen Missverständnissen eine zu hohe Gewichtung zugesprochen wird. Dafür bedarf es zunächst einer kurzen Begriffsklärung. Der britische Geheimdienst zog seine Informationen keineswegs nur aus der Funkaufklärung.[[107]](#footnote-107) Viele Informationen gelangen auch über Luftaufklärung, Spione, Diebstahl und gezielte Unterwanderung des Feindes zur britischen Itelligence[[108]](#footnote-108). Dies war unbedingt nötig, denn die Funkaufklärung hatte nur auf einen Bruchteil der im Krieg versendeten Nachrichten überhaupt Zugriff, da man sich der Gefahren durch Spionage bekannt war, sodass ein wesentlicher Teil der Nachrichtenübermittlung nur über Drahtverbindungen abgewickelt wurde.[[109]](#footnote-109)

Zusätzlich ist es essenziell zu erwähnen, dass selbst Ultra nur einen Teil der Funkaufklärung darstellte. Jürgen Rohwer beschreibt diesen Sachverhalt am besten, indem er die Funkaufklärung in drei Bereiche unterteilt. Zunächst einmal gab es die sogenannte Peilauswertung, welche sich ausschließlich auf die Lokalisation der Position der Sendestelle beschränkte und daraus ihre Erkenntnisse über die Standorte von Einheiten und Maschinerie gewann. Als zweiten Zweig der Funkaufklärung nennt Rohwer die Verkehrsauswertung, welche ebenfalls ohne Kenntnis des Inhalts des Funkspruchs, anhand von äußeren Merkmalen der Nachricht sowie Sendezeit und Menge an Sendungen Informationen sammelte. Das gezielte Abfangen, Entschlüsseln und Übersetzten und damit die Aufgaben von BP stellt die letzte Komponente der Funkaufklärung dar. [[110]](#footnote-110) Alle Informationen die die Itelligence auf diesem Weg zugespielt bekam erhielten die Tarnbezeichnung Ultra. Hierbei ist es jedoch wichtig zu verstehen, dass die deutsche Wehrmacht zum Zwecke der Geheimhaltung ihres Funkverkehrs nicht nur die Enigma Maschine, sondern auch noch andere Chiffriermaschinen sowie verschiedene Handschlüsselverfahren benutzte. Besonders für den Funkverkehr an der Front konnten oft keine Schlüsselmaschinen genutzt werden, da diese Maschinen schlicht und einfach zu sperrig waren um sie zu transportieren, sodass auf besagte Handverfahren zurückgegriffen wurde.[[111]](#footnote-111) Die Dechiffrierung dieser Techniken viel ebenfalls in den Aufgabenbereich der britischen Kryptoanalytiker, sodass der Begriff Ultra, entgegen weit verbreiteten Annahmen, nicht nur die über Enigmen verschlüsselten Funksprüche, sondern auch die Brechung anderer Chiffrierverfahren umfasst. [[112]](#footnote-112)

Im Vergleich zu allen anderen Methoden der Informationenbeschaffung durch die britische Itelligence hat die Arbeit in BP den Vorteil, dass die Informationen in der Regel wesentlich zuverlässiger waren als aus anderen Quellen.[[113]](#footnote-113) Diese Authentizität zu gewährleisten war jedoch immer mit viel Arbeit verbunden. Die Stationen der britischen Funkhorcher fingen täglich tausende deutsche Funksprüche ab.[[114]](#footnote-114) Die Aufgabe in BP war es also nicht nur diese unzähligen Meldungen zu entschlüsseln und zu übersetzten, sondern auch die vielen unwichtig erscheinenden Bruchstücke aus Tagesmeldungen, organisatorischer Nachrichten, Wettermeldungen und Administrativer Befehle zu sortieren, strukturieren und am Ende wie eine Art Puzzle zu einem größeren Bild zusammenzusetzten. [[115]](#footnote-115) Als wäre dies nicht schon genug versuchte man auf deutscher Seite den Gegner entweder durch gezielte Funkstille oder sogar Funktäuschung beziehungsweise unnötig viele Meldungen in die Irre zu führen.[[116]](#footnote-116) Zudem war es in einigen Bereichen der Wehrmacht, so etwa der Kriegsmarine üblich, bestimmte sensible Informationen, wie etwa Koordinaten und Ortsangaben noch einmal mit anderen Verfahren zu überschlüsseln[[117]](#footnote-117) oder die Meldungen abzukürzen indem man nur noch gewisse Buchstabenkombinationen sandte, welche dann für eine häufig gebrauchte Phrase oder Anweisung standen.[[118]](#footnote-118)

Aufgrund all dieser Komplikationen kam es nicht selten vor, dass die Nachrichten erst mit einigen Tagen Verzögerung an der Front ankamen und den dortigen Befehlshabern nur noch historischen Wert boten. Rohwer nennt als ein Beispiel für diesen Sachverhalt die Operation „Dynamo“ also die Evakuierung von Dunkirk im Jahre 1940, welche zwar über eine Direkte Nachrichtenverbindung zu BP verfügte, diese Informationen jedoch aufgrund der Verzögerung von einigen Tagen keinen militärstrategischen Wert mehr boten, sodass der Erfolg der Operation letztlich in keinster Weise von den Ultra Informationen abhing. [[119]](#footnote-119)

Einige der von den deutschen abgesetzten Funksprüche konnten auch nie entschlüsselt werden, da die deutschen Vorschriften es vorsahen bestimmten militärischen Abteilungen in verschiedene Schlüsselnetzte mit unterschiedlichen Verschlüsselungsgraden zu unterteilen, sodass je nach Empfänger der Nachricht eine andere Chiffre bzw. andere Enigma Einstellung verwendet wurde.[[120]](#footnote-120) In einigen dieser Schlüsselbereiche wurde der Schlüssel im Laufe des Krieges bis zu Drei Mal Täglich geändert[[121]](#footnote-121) oder es fiel gar so wenig Funkverkehr an, dass man es bis zum Ende des Krieges nicht schaffte einen Einbruch in diese Schlüsselnetzte zu erzielen.[[122]](#footnote-122)

Zusammenfassend ist zu sagen, dass die Entschlüsselung der Enigma Maschine mit wesentlich mehr Komplikationen einherging als in vielen Populärwissenschaftlichen Quellen dargestellt wird. Dazu soll angemerkt sein, dass es oft einfach erscheint, die Begriffe Itelligence, Ultra und Funkaufklärung mit der Entschlüsselung der Enigma Maschine gleichzusetzten, hier jedoch wesentlich Unterschiede vorliegen oder zumindest Abgrenzungen vorgenommen werden müssen. Dies wird besonders relevant, wenn Zitate von Historikern betrachtet werden, welche ohne dieses Wissen über die Trennung dieser Begrifflichkeiten zu Missverständnissen über die Tatsächliche Relevanz der Enigma Entschlüsselung führen können.

Doch selbst wenn die Dechiffrierung von Enigma Funksprüchen Präzise Informationen erbrachte, konnte man diese nicht immer voll ausschöpfen, da den Alliierten natürlich daran gelegen war die Quelle dieser Informationen um jeden Preis vor den Deutschen Geheimzuhalten. Das Geheimnis von BP kannten nur wenige außenstehende Militärs, die die Informationen unter höchstem Geheimhaltungsgrad erhielten und angewiesen waren die Quelle mit einer glaubwürdigen „cover story“ zu versehen, sodass nicht einmal die eigenen Soldaten über die Erfolge der Funkaufklärung Bescheid wussten.[[123]](#footnote-123) Das dies zu Problemen führen kann zeigt eine Geschichte, die sich im Seekrieg abspielte. Eine Enigma Meldung enthüllte die genaue Position von neun deutschen Tank- und Versorgungsschiffen, wobei jedoch nur sieben dieser Positionen an die eigenen Zerstörer weitergegeben wurden, um kein Mistrauen in der deutschen Admiralität zu erregen. Ganz der Erwartung nach wurden alle sieben Schiffe versenkt, doch zusätzlich gelang es den unwissenden Offizieren auf den britischen Zerstörern, welche einfach ihrer Pflicht nachgingen, die restlichen zwei Schiffe ebenfalls zu lokalisieren und zu versenken.

Tatsächlich erregte dieser Vorfall Verdacht in der Kriegsmarine und es kam zu einer Untersuchung bezüglich der Schlüsselsicherheit der Enigma, die jedoch, zum Glück der Briten, im Sande verlief.[[124]](#footnote-124)

Die Arbeit in BP erlaubte es der Royal Navy auch die Position von vielen deutschen U-Booten auszumachen doch wäre es leichtsinnig gewesen diese direkt anzugreifen. Stattdessen entschied man sich dazu einige U-Boote entkommen zu lassen und die Restlichen erst anzugreifen, nachdem man eine scheinbare Erklärung für die plötzliche U-Boot Sichtung fälschte. So wurden etwa Spähflugzeuge ausgesandt, um „zufällig“ auf deutsche U-Boote zu treffen oder Meldungen über U-Boot Sichtungen fabriziert, die so gesendete wurden, dass die Deutschen sie abfangen mussten, um die Offiziere im Glauben zu lassen das der plötzliche Erfolg der Royal Navy mit rechten Dingen zuging.[[125]](#footnote-125) (ggf. noch Coventry als Beispiel für eine Missinterpretation von BP-Informationen)

Als Fazit sei also zu vermerken, dass selbst wenn die Entschlüsselungsarbeit in BP verwertbare, präzise Informationen lieferte, diese in vielen Fällen nicht vollständig oder nur unter viel Vertuschungsarbeit ausgeschöpft werden konnten.

Doch bei all dieser Kritik an den Aussagen bezüglich einer extremen Relevanz der Entschlüsselungsarbeit in BP ist das wohl wichtigste Argument noch gar nicht zur Sprache gekommen.

Es ist eine bedeutende Frage, ob die Sowjetunion von den britischen Erfolgen bezüglich der Entschlüsselung des deutschen Funkverkehrs unterrichtet wurde. Die Antwort darauf ist so einfach wie verblüffend. Während des gesamten Krieges und auch bis weit in die Nachkriegszeit blieb die Arbeit in BP vor der Sowjetunion geheim. Zwar hatte man in Moskau einen Ultra-Experten stationiert, doch dieser lieferte seine Informationen, wenn überhaupt, nachdem die Quelle mit einer „cover story“ verschleiert worden war.[[126]](#footnote-126) Diese Verschleierung vor dem Bündnispartner ging so weit, dass die Sowjets in der Nachkriegszeit Exemplare der Enigma Maschine erwarben, ohne zu wissen das sie dem britischen Geheimdienst seine Spionageaufgabe im Kalten Krieg damit deutlich leichter gemacht hatten. [[127]](#footnote-127)

Trotz der dünnen Quellenlage auf diesem Gebiet ist also davon auszugehen, dass der Sowjetische Geheimdienst bis zum Ende des Krieges nicht in der Lage war, die Enigma-Chiffre zu brechen.[[128]](#footnote-128) Daraus folgt, dass der gesamte Krieg an der Ostfront auch ohne die Informationen aus den durch die Enigma verschlüsselten Nachrichten, gewonnen werden konnte.

Am 23. August 1942 um 16:18 Uhr wurde eine der brutalsten und grausamsten Schlachten des Zweiten Weltkriegs durch das Kreischen von unzähligen fallenden Bomben eigeleitet, welche den Industriestandort Stalingrad wie ein Teppich überzogen und nichts als Ruinen, Feuer und Leichen zurückließen.[[129]](#footnote-129) Die ist der Beginn der Schlacht um Stalingrad, welche einen entscheidenden Psychologischen Wendepunkt für den gesamten Deutsch-Sowjetischen Krieg markiert. Am 19. November 1942 startete die Rote Armee Operation „Uranus“, welche dafür sorgte, dass sich die 6. Armee[[130]](#footnote-130) unter der Leitung von General Paulus[[131]](#footnote-131) fünf Tage später im „Kessel von Stalingrad“ wiederfand, was den Anfang vom Ende der gesamten Schlacht einläutete.[[132]](#footnote-132) Die sowjetische Großoffensive Operation „Ring“ am 10. Januar 1943 besiegelte dann endgültig das Schicksal der 6. Armee als es gelang die deutschen Divisionen in zwei separate Kessel aufzuspalten. General Paulus kapitulierte am 31. Januar 1943, entgegen Hitlers Befehl bis zum Tod zu kämpfen, woraufhin die Truppen im Nordkessel zwei Tage später ebenfalls kapitulierten. [[133]](#footnote-133)

Diese Schlacht zeigt, dass es auch ohne Zugriff auf die feindlichen Kommunikationsmittel möglich ist den Gegner durch schiere taktische sowie personelle Überlegenheit zu besiegen, wobei natürlich anzumerken ist, dass die deutschen Truppen durch die Kälte und Hungersnot ohnehin geschwächt waren.

Dennoch ist es Grundsätzlich nicht von der Hand zu weisen, dass die Arbeit in BP zumindest in einigen Bereichen Einfluss auf die taktischen Entscheidungen der wohlgemerkt Westalliierten hatte. Wie Bereits erwähnt stellt die Nordatlantikschlacht eines der bekanntesten Beispiele für die Wirkung der Alliierten Funkaufklärung dar, wobei hier angemerkt sei, dass einige der Quellen kontrovers diskutiert werden können und die Gründe für einige zu beobachtenden Phänomene, wie etwa die erhöhte Versenkungsrate Alliierter Konvois im Jahre 1942, weit Vielschichtiger sein könnten als zunächst angenommen. Rohwer verweist darauf, dass ohne BP deutlich mehr Alliierte Ressourcen im Nordatlantik nötig gewesen wären, um eine Wende herbeizuführen. Ressourcen, die zur damaligen Zeit sehr knapp waren, sodass Kräften von anderen Gebieten abgezogen werden müssten.[[134]](#footnote-134) Laut Schätzungen von Historikern hieße dies, dass das die einige alliierte Unternehmungen sich in diesem Fall verzögert, hätten, sodass der Krieg in die Länge gezogen worden wäre. Als Beispiel hierfür wird die Landung in der Normandie angeführt, welche mindestens um ein halbes Jahr verschoben worden werde.[[135]](#footnote-135)

Tatsächlich ist die Gesamte Planung Rund um D-Day und Operation Overlord ebenfalls ein Beispiel für den Nutzen der Ultra Informationen. Für die Landung in der Normandie war es entscheidend den genauen Zielort dieser amphibischen Invasion um jeden Preis Geheimzuhalten.[[136]](#footnote-136) Zu diesem Zweck wurde eine die wohl bedeutendste und Größte Täuschungsoperation in der Geschichte des Zweiten Weltkriegs ins Leben gerufen: Operation Fortitude.[[137]](#footnote-137) Diese Gründete sich auf verschiedenste Desinformations-Kampagnen und diverse Verschleierungsmethoden, wobei eine der Entscheidendsten wohl das sogenannte Double Cross System darstellte. Mit Hilfe eines deutschen Doppelagenten[[138]](#footnote-138) und vor allem durch den Einbruch von BP in die Funkverschlüsselung der deutschen Abwehr (Geheimdienst)[[139]](#footnote-139) gelang es den Briten einreisende deutsche Agenten rechtzeitig zu fassen und sie vor die Wahl zu stellen für das Vereinigte Königreich als Doppelagenten zu arbeiten oder sich freiwillig in die „Schlinge des Henkers“ zu begeben.[[140]](#footnote-140) Ganz nach erwarten der britischen Intellegence wählten fast alle Agenten die erste Möglichkeit und wurden unter Beobachtung des MI5 „umgedreht“.[[141]](#footnote-141) Nicht zuletzt durch gezielte von den Alliierten gesäte Falschmeldungen, von den Double Cross Agenten übermittelt, gelang es die eigentliche Truppenstärke der Invasionstruppen zu verschleiern und die deutschen Verbände vom eigentlichen Invasionsort fernzuhalten.[[142]](#footnote-142) Für dieses Vorhaben war es von größter Bedeutung, die Auswirkung der durch die Doppelagenten verbreiteten Falschmeldungen zu überprüfen und zu ermitteln, welchen Agenten mehr vertraut wurde als anderen um gegebenenfalls Meldungen so anzupassen, dass sie den Deutschen glaubwürdiger erschienen.[[143]](#footnote-143) Laut Rohwer wären die massiven Täuschungsoperationen der Alliierten rund um die Landung in der Normandie ohne die ständige Kontrolle deren Wirkung durch Ultra, kaum möglich gewesen.[[144]](#footnote-144)

Doch Ultra diente im Zuge der Operation Overlord nicht nur als Kontrollinstanz für den Erfolg der Verbreiteten Falschmeldungen, auch gelang es durch die Mühen der Codebrecher in BP ein überaus umfassendes Bild der deutschen Verteidigungsaufstellungen und Vorbereitungsmaßnahmen zu gewinnen.[[145]](#footnote-145) Durch die Ultra Informationen gelang es die Positionen der deutschen Verbände aufzudecken und die vollständige Truppenstärke der Wehrmacht in Erfahrung zu bringen. [[146]](#footnote-146) Vermutlich rettete ein einziger entschlüsselter Funkspruch das Leben von etwa 15.000 alliierten Fallschirmjägern, welche sonst die ursprüngliche Landezone angepeilt hätten und mitten in den deutschen Truppenverbänden gelandet wären. [[147]](#footnote-147)

Ein Weiteres Beispiel für die kritische Relevanz eines einzelnen Funkspruchs lässt sich in der ersten Phase der Nordafrikaschlacht finden. General Archibald Wavell der Oberbefehlshaber des Kommandos Naher Osten gelang es durch einen einzelnen Funkspruch aus BP 25 italienische Flugzeuge in einem einzelnen Angriff abzuschießen[[148]](#footnote-148). Folgt man Smith dann zeigte sich besonders in Nordafrika die Relevanz der „Ultra“ Funkaufklärung, welche ab 1942 konstant Informationen über die Vorhaben des Kommandanten des Deutschen Afrikakorps Erwin Rommels[[149]](#footnote-149) lieferte und die Schwachstellen seiner Strategien aufzeigte.[[150]](#footnote-150)

Auch der Überfall der Wehrmacht auf Norwegen und Dänemark im Zuge der Operation Weserübung im April 1940[[151]](#footnote-151) konnte durch die Informationen aus BP genau verfolgt werden[[152]](#footnote-152). Bei der Luftschlacht um England soll Ultra ebenfalls eine wichtige Rolle gespielt haben, so war es etwa in einigen Fällen möglich, die Bombardierungsziele der Luftwaffe anzugeben und rechtzeitig Warnungen herauszugeben.[[153]](#footnote-153) Immer wieder, sollen die Ultra Informationen Alliierte Befehlshaber rechtzeitig in Alarmbereitschaft versetzt haben und Angriffszeile sowie strategische Absichten der Befehlshaber der Achsenmächte aufgedeckt haben. Nicht selten half Ultra die „Order of Battle“ und die logistische und materielle Situation des Feindes aufzudecken.[[154]](#footnote-154) So wurde etwa der Oberbefehlshaber der britischen Mittelmeerflotte Admiral Cunningham durch BP rechtzeitig über die Pläne einer Bevorstehenden Italienischen Flottenvorstoßes nach Kap Matapan (Griechenland) im Jahre 1941 informiert und konnte so seine Ressourcen Optimal einsetzten[[155]](#footnote-155) und die Schlacht dank „Ultra“ gewinnen. [[156]](#footnote-156)

Aus diesen Informationen wird ersichtlich, dass die Arbeit in BP zwar nicht alleine Schlachten gewonnen hat, jedoch in vielen Fällen die Entscheidung der zuständigen Alliierten Kommandeure wesentlich beeinflusst hat und zu kleineren Siegen maßgeblich beigetragen hat. Oft ergab sich aus den vielen kleineren Informationsschnipseln ein größeres Bild, welches den Alliierten half, die strategische Situation besser einzuschätzen und ihre Ressourcen entsprechend zu verteilen.

Nachdem nun also die Problemfrage auf ihre Unterschiedlichen Aspekte untersucht wurde und beide Betrachtungsweisen anhand von Beispielen analysiert und belegt wurden, ist es möglich eine Antwort auf besagte Problemfrage mittels eines abschließenden Fazits zu ermitteln, welches sich auf die bis jetzt herausgearbeiteten Fakten stützt und diese unter einer zeitgenössischen Betrachtung evaluiert und gewichtet.

**Fazit**

Um ein

* Ringstellung Email überarbeiten
* Entschlüsselung Polen Bomba genauer erklären 🡪 possible errors
* Was wussten die deutschen (monarch)
* Enigma beeinflusst operation dunkirk nicht (<https://www.ifz-muenchen.de/heftarchiv/1979_3_1_rohwer.pdf> S.340)
* Coventry
* Wintherbotham einer der bekanntesten autoren schreibt das die enigma den krieg fast alleine gewonnen hat (<https://www.nytimes.com/1974/12/29/the-ultra-secret.html>) 🡪 wird von anderen autoren oft als schlecht recherschiert oder überspitzt dargstellt (<https://d1wqtxts1xzle7.cloudfront.net/5035877/Ultra-libre.pdf?1390839789=&response-content-disposition=inline%3B+filename%3DNSA_OSS_Released_Document.pdf&Expires=1692965110&Signature=eN-TAirR3hNxiq9JXoLsJh6GZba92ksz9sc~fAjFLQvVD9s5X06DtsLl2ndLLHyrIBjyNKVdUyvI27asvoAHOpZPMRvTGlMknUE9e3YIlZR0VPMRriUAUke5F0omrp2yVvxKygfo2ijhd0Im9iaX6pf3w0eyUSH4N5IsEbvM2y9NSsph4aL~QwP2HATljHjNUD0pzEz87TACcD3TiCo2fY3c7Rxw38syeIla-J-a3JZE~hHCmaMQTcA6y-OYQbdO9Hm4YJXtiT8URCrxlEZ-XYjn-hAmMi4fdyaVaT-FCebBlRLwqeAVwPNL-5nmjpWfiPa57ghafwzn03VgjFfLAw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA> S.5, <https://www.rafmuseum.org.uk/documents/research/RAF-Historical-Society-Journals/Journal-17-Dr%20Noble-Frankland-on-writing-official-history.pdf> S.17)
* Man verließ sich zu sehr auf Ultra 🡪 schwer Folgen ([https://www.hamfu.ch/\_upload/Die\_Funkaufklaerung\_und\_ihre\_Rolle\_im\_zweiten\_Weltkrieg.pdf S.23](https://www.hamfu.ch/_upload/Die_Funkaufklaerung_und_ihre_Rolle_im_zweiten_Weltkrieg.pdf%20S.23))
* Nach vielen U-Boot verlusten 1944 fragt man sich ob die maschine noch sicher ist monarch 142
* Wenn der Gegner in der Überzahl ist (Im Luftraum) dann bringt auch die beste Intelligence nicht (Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.350)
* David Kahn sagt dass im Falle eines längeren Krieges dieser ohnenhin durch die Atombombe beendet worden wäre Seizing the Enigma The Race to Break the German U-boat Codes, 1939-1943 S.278
* Order of Battle wurde durch Ultra klar (Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.364)
* Die deutschen haben viele U-Boote verloren, nicht aufgrund von radartechnologie, sondern aufgrund von ultra <https://web.archive.org/web/20140611025626/http://www.nsa.gov/public_info/_files/european_axis_sigint/volume_2_notes_on_german.pdf>
* Die nordatlantikschlacht wurde nicht nur BP gewonnen (The U-Boat problems did not stem simply from the fact that the Admiralty knew their locations and intentions.) 🡪 The Secrets of Station X: How the Bletchley Park codebreakers helped win the war S.192
* The contribution made by the codebreakers to the allied victory is truly incalculable. Bletchley Park did not win the war. No single organisation could make that claim. Certainly not of a war that was fought all too often by soldiers killing and dying by the bullet or bayonet. But Bletchley Park’s contribution to the allied victory was enormous. The Secrets of Station X: How the Bletchley Park codebreakers helped win the war S.191

It does affect the position of the internal wiring, relative to the alphabet on the outer ring, but that doesn’t interest the cryptanalyst, as that alphabet on the outer ring are just letters, but the cryptanalyst wants to know the internal wiring.

1. <https://www.theguardian.com/world/2022/mar/08/vitaly-gerasimov-second-russian-general-killed-ukraine-defence-ministry-claims>

   <https://www.youtube.com/watch?v=j2Bvc12476k>

   <https://www.businessinsider.com/ukraine-says-killed-russia-general-vitaly-gerasimov-intercepted-fsb-call-2022-3> [↑](#footnote-ref-1)
2. <https://www.wsj.com/articles/death-of-russian-generals-in-ukraine-expose-vulnerabilities-in-moscows-military-tactics-11647441273>

   <https://www.nytimes.com/2023/01/04/world/europe/ukraine-russia-cellphones.html> [↑](#footnote-ref-2)
3. <https://www.businessinsider.com/russia-general-killed-after-ukraine-intercepted-unsecured-call-nyt-2022-3>

   <https://www.nytimes.com/2022/03/16/us/politics/russia-troop-deaths.html> [↑](#footnote-ref-3)
4. <https://www.nytimes.com/2023/01/02/world/europe/ukraine-russia-himars-makiivka.html> [↑](#footnote-ref-4)
5. <https://www.nytimes.com/2023/01/04/world/europe/ukraine-russia-cellphones.html>

   <https://t.me/mod_russia/23167> [↑](#footnote-ref-5)
6. <https://mediarep.org/bitstream/handle/doc/15199/GFM_11_56-70_Koenig_Telegraphie_Telefonie_Funk.pdf?sequence=1> S.60

   <https://link.springer.com/content/pdf/10.1007/978-3-658-39561-2_6.pdf> [↑](#footnote-ref-6)
7. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S. 177 [↑](#footnote-ref-7)
8. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.4 [↑](#footnote-ref-8)
9. <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjAgoiRwJL-AhWKRvEDHTc1A2oQFnoECBQQAQ&url=https%3A%2F%2Fjournals.wlb-stuttgart.de%2Fojs%2Findex.php%2Fwlbf%2Farticle%2Fdownload%2F313%2F332%2F842&usg=AOvVaw26KfRXXwedhdvUxAkZ0ta9> S. 28

   Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.178 [↑](#footnote-ref-9)
10. Historische Notizen zur Informatik S.47 [↑](#footnote-ref-10)
11. Historische Notizen zur Informatik S.49 [↑](#footnote-ref-11)
12. Historische Notizen zur Informatik S.49 [↑](#footnote-ref-12)
13. Historische Notizen zur Informatik S.49 [↑](#footnote-ref-13)
14. Seizing the Enigma - The Race to Break the German U-boat Codes S.37,38

    https://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/4a\_ZylRot/Enigma.html [↑](#footnote-ref-14)
15. <https://www.cdvandt.org/Enigma%20DE452194C1.pdf> S.1 [↑](#footnote-ref-15)
16. [https://www.hamfu.ch/\_upload/Die\_Funkaufklaerung\_und\_ihre\_Rolle\_im\_zweiten\_Weltkrieg.pdf S.4](https://www.hamfu.ch/_upload/Die_Funkaufklaerung_und_ihre_Rolle_im_zweiten_Weltkrieg.pdf%20S.4)

    Historische Notizen zur Informatik S.50 [↑](#footnote-ref-16)
17. <https://www.hamfu.ch/_upload/Die_Funkaufklaerung_und_ihre_Rolle_im_zweiten_Weltkrieg.pdf> S.4 [↑](#footnote-ref-17)
18. <https://www.ifz-muenchen.de/heftarchiv/1979_3_1_rohwer.pdf> S.331 [↑](#footnote-ref-18)
19. <https://www.kryptowissen.de/enigma.html>

    <https://entwickler.de/javascript/geheime-botschaften-durch-verschlusselung>

    [https://www2.informatik.uni-hamburg.de/TGI/lehre/vl/WS0910/IuG/ProSem\_WiSe\_2009.pdf](https://www2.informatik.uni-hamburg.de/TGI/lehre/vl/WS0910/IuG/ProSem_WiSe_2009.pdf%20) S.100 [↑](#footnote-ref-19)
20. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.179 [↑](#footnote-ref-20)
21. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.178 [↑](#footnote-ref-21)
22. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.178 [↑](#footnote-ref-22)
23. [https://www.hamfu.ch/\_upload/Die\_Funkaufklaerung\_und\_ihre\_Rolle\_im\_zweiten\_Weltkrieg.pdf S.4](https://www.hamfu.ch/_upload/Die_Funkaufklaerung_und_ihre_Rolle_im_zweiten_Weltkrieg.pdf%20S.4)

    <https://www.ifz-muenchen.de/heftarchiv/1979_3_1_rohwer.pdf> S.332 [↑](#footnote-ref-23)
24. <https://www.hamfu.ch/_upload/Die_Funkaufklaerung_und_ihre_Rolle_im_zweiten_Weltkrieg.pdf> S.4 [↑](#footnote-ref-24)
25. <https://www.dohrau.ch/downloads/enigma.pdf> S. 18 [↑](#footnote-ref-25)
26. <https://www.dohrau.ch/downloads/enigma.pdf> S.14 [↑](#footnote-ref-26)
27. <http://www.softdoc.de/mr/de/downloads/files/EnigmaTechnischeDetails.pdf> S.10

    <https://imsc.uni-graz.at/fripertinger/CodesUndKrypt19/s_CK19.pdf> S.1-2 [↑](#footnote-ref-27)
28. [https://web.archive.org/web/20220331013314/http://www.intelligenia.org/downloads/rotors1.pdf S.2](https://web.archive.org/web/20220331013314/http://www.intelligenia.org/downloads/rotors1.pdf%20S.2)

    <https://imsc.uni-graz.at/fripertinger/CodesUndKrypt19/s_CK19.pdf> S. 2 [↑](#footnote-ref-28)
29. <https://www.dohrau.ch/downloads/enigma.pdf> S.30 [↑](#footnote-ref-29)
30. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S. 183 [↑](#footnote-ref-30)
31. https://www.geo.de/wissen/weltgeschichte/zweiter-weltkrieg-operation-enigma-der-stille-kampf-der-30178208.html [↑](#footnote-ref-31)
32. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.179 [↑](#footnote-ref-32)
33. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.180 [↑](#footnote-ref-33)
34. <https://www.ifz-muenchen.de/heftarchiv/1979_3_1_rohwer.pdf> [↑](#footnote-ref-34)
35. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.180 [↑](#footnote-ref-35)
36. <https://www.ifz-muenchen.de/heftarchiv/1988_1_3_borodziej.pdf> S.85,88 [↑](#footnote-ref-36)
37. Historische Notizen zur Informatik S.173

    Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.182 [↑](#footnote-ref-37)
38. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.183 [↑](#footnote-ref-38)
39. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.195 – 196

    Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 335 [↑](#footnote-ref-39)
40. <https://www.tu-chemnitz.de/urz/stammtisch/rsrc/enigma.pdf> S.20, Die Funkaufklärung und ihre Rolle im 2. Weltkrieg S. 8 [↑](#footnote-ref-40)
41. Historische Notizen zur Informatik S.173 [↑](#footnote-ref-41)
42. <https://www2.informatik.uni-hamburg.de/TGI/lehre/vl/WS0910/IuG/ProSem_WiSe_2009.pdf#page=95>, <https://www.hamfu.ch/_upload/Die_Funkaufklaerung_und_ihre_Rolle_im_zweiten_Weltkrieg.pdf> s.8 [↑](#footnote-ref-42)
43. https://www2.informatik.hu-berlin.de/~oependox/files/Ausarbeitung-Enigma.pdf [↑](#footnote-ref-43)
44. <https://www2.informatik.hu-berlin.de/~oependox/files/Ausarbeitung-Enigma.pdf> S.10 [↑](#footnote-ref-44)
45. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 336,

    https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/ [↑](#footnote-ref-45)
46. Historische Notizen zur Informatik S. 176, <https://www.hamfu.ch/_upload/Die_Funkaufklaerung_und_ihre_Rolle_im_zweiten_Weltkrieg.pdf> S.8 [↑](#footnote-ref-46)
47. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 333 [↑](#footnote-ref-47)
48. <https://imsc.uni-graz.at/fripertinger/CodesUndKrypt19/s_CK19.pdf> S. 5 [↑](#footnote-ref-48)
49. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.97 [↑](#footnote-ref-49)
50. [https://www2.informatik.uni-hamburg.de/TGI/lehre/vl/WS0910/IuG/ProSem\_WiSe\_2009.pdf](https://www2.informatik.uni-hamburg.de/TGI/lehre/vl/WS0910/IuG/ProSem_WiSe_2009.pdf%200) S.100-101

    <https://www2.informatik.hu-berlin.de/~oependox/files/Ausarbeitung-Enigma.pdf> S.10 [↑](#footnote-ref-50)
51. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 335 [↑](#footnote-ref-51)
52. <https://cryptocellar.org/pubs/enigma-modern-breaking.pdf> S.2 [↑](#footnote-ref-52)
53. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S .98, Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S. 188-193 [↑](#footnote-ref-53)
54. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des S.190-191 [↑](#footnote-ref-54)
55. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.191 [↑](#footnote-ref-55)
56. <https://www.archives.gov/files/publications/prologue/1997/fall/turing.pdf> S.208

    Historische Notizen zur Informatik S.302 [↑](#footnote-ref-56)
57. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.194 [↑](#footnote-ref-57)
58. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.99-100 [↑](#footnote-ref-58)
59. Historische Notizen zur Informatik S.303 [↑](#footnote-ref-59)
60. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.195 [↑](#footnote-ref-60)
61. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.100 [↑](#footnote-ref-61)
62. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.100 [↑](#footnote-ref-62)
63. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.100 [↑](#footnote-ref-63)
64. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.197 [↑](#footnote-ref-64)
65. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.197-199 [↑](#footnote-ref-65)
66. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.199 [↑](#footnote-ref-66)
67. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.199 [↑](#footnote-ref-67)
68. Historische Notizen zur Informatik S.181 [↑](#footnote-ref-68)
69. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.200 [↑](#footnote-ref-69)
70. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.204 [↑](#footnote-ref-70)
71. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.210 [↑](#footnote-ref-71)
72. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.102 [↑](#footnote-ref-72)
73. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.101 - 102 [↑](#footnote-ref-73)
74. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S .102 Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S. 210 [↑](#footnote-ref-74)
75. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.211 – 216 [↑](#footnote-ref-75)
76. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S. 217 [↑](#footnote-ref-76)
77. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S. 217 [↑](#footnote-ref-77)
78. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.339-340 [↑](#footnote-ref-78)
79. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.218

    *Enigma – The battle for the code*. Cassell Military Paperbacks, London 2004, S. 357 [↑](#footnote-ref-79)
80. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S. 107 [↑](#footnote-ref-80)
81. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.220-221 [↑](#footnote-ref-81)
82. https://en.wikipedia.org/wiki/Ultra#cite\_ref-8 [↑](#footnote-ref-82)
83. Die Funkaufklärung und ihre Rolle im 2. Weltkrieg S.5 Vgl. Fig. 6 [↑](#footnote-ref-83)
84. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.326 [↑](#footnote-ref-84)
85. <https://de.wikipedia.org/wiki/Enigma_(Maschine)#Geschichtliche_Konsequenzen>, https://historyhub.info/british-signals-intelligence-and-the-shortening-of-world-war-two/ [↑](#footnote-ref-85)
86. https://web.archive.org/web/20200708021120/https://de.wikipedia.org/wiki/Enigma\_(Maschine)#Geschichtliche\_Konsequenzen [↑](#footnote-ref-86)
87. <https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/ultra_secret.pdf> S. 3 [↑](#footnote-ref-87)
88. https://historyhub.info/british-signals-intelligence-and-the-shortening-of-world-war-two/ [↑](#footnote-ref-88)
89. <https://www.rafmuseum.org.uk/documents/research/RAF-Historical-Society-Journals/Journal-17-Dr%20Noble-Frankland-on-writing-official-history.pdf> S. 17 [↑](#footnote-ref-89)
90. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.110 [↑](#footnote-ref-90)
91. http://deutscher-historischer-jahrweiser.de/marine/geleitzug-konvois.htm [↑](#footnote-ref-91)
92. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.224 [↑](#footnote-ref-92)
93. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.224 [↑](#footnote-ref-93)
94. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.224 [↑](#footnote-ref-94)
95. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.110 [↑](#footnote-ref-95)
96. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.110-111 [↑](#footnote-ref-96)
97. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.111 [↑](#footnote-ref-97)
98. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.346 [↑](#footnote-ref-98)
99. Seizing the Enigma The Race to Break the German U-boat Codes, 1939-1943 Preface [↑](#footnote-ref-99)
100. <file:///C:/Users/liamw/Downloads/Seizing%20the%20Enigma%20%20The%20Race%20to%20Break%20the%20German%20U-boat%20Codes,%201939-1943%20(%20PDFDrive%20).pdf> Preface [↑](#footnote-ref-100)
101. <file:///C:/Users/liamw/Downloads/Evaluate%20the%20extent%20to%20which%20Bletchley%20Park.pdf> S.3 [↑](#footnote-ref-101)
102. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 356-357 <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.111 [↑](#footnote-ref-102)
103. Ultra and the Battle of the Atlantic S.11 [↑](#footnote-ref-103)
104. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.111-112 [↑](#footnote-ref-104)
105. Ultra and the Battle of the Atlantic S.11 [↑](#footnote-ref-105)
106. <file:///C:/Users/liamw/Downloads/Evaluate%20the%20extent%20to%20which%20Bletchley%20Park.pdf> S.3-5 [↑](#footnote-ref-106)
107. Ultra and the Battle of the Atlantic S.5 [↑](#footnote-ref-107)
108. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.225

     <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.3 [↑](#footnote-ref-108)
109. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges [↑](#footnote-ref-109)
110. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 329 [↑](#footnote-ref-110)
111. https://www.spiegel.de/geschichte/verschluesselungstechnologie-a-946499.html [↑](#footnote-ref-111)
112. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.3, Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 330 [↑](#footnote-ref-112)
113. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.3 [↑](#footnote-ref-113)
114. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S. 6 [↑](#footnote-ref-114)
115. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.342 [↑](#footnote-ref-115)
116. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 334 [↑](#footnote-ref-116)
117. <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S.110 [↑](#footnote-ref-117)
118. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.334, <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S. 110 [↑](#footnote-ref-118)
119. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.340, Ultra and the Battle of the Atlantic S.7, Die Funkaufklärung und ihre Rolle im 2. Weltkrieg S.10 [↑](#footnote-ref-119)
120. Die Funkaufklärung und ihre Rolle im 2. Weltkrieg S. 8, Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.333, <https://monarch.qucosa.de/api/qucosa%3A18268/attachment/ATT-0/> S. 139 [↑](#footnote-ref-120)
121. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.333 [↑](#footnote-ref-121)
122. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.357 [↑](#footnote-ref-122)
123. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 341 [↑](#footnote-ref-123)
124. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.227-228 [↑](#footnote-ref-124)
125. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.227 [↑](#footnote-ref-125)
126. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 351 [↑](#footnote-ref-126)
127. https://www.geo.de/wissen/weltgeschichte/zweiter-weltkrieg-operation-enigma-der-stille-kampf-der-30178208.html [↑](#footnote-ref-127)
128. Vgl. http://chris-intel-corner.blogspot.com/2013/07/soviet-codebreakers-of-wwii.html [↑](#footnote-ref-128)
129. Die Schlacht von Stalingrad S.5 [↑](#footnote-ref-129)
130. Die Schlacht von Stalingrad S. 3 [↑](#footnote-ref-130)
131. Die Schlacht von Stalingrad S.18 [↑](#footnote-ref-131)
132. Die Schlacht von Stalingrad S. 16 [↑](#footnote-ref-132)
133. Die Schlacht von Stalingrad S.18 [↑](#footnote-ref-133)
134. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 360 [↑](#footnote-ref-134)
135. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.230 [↑](#footnote-ref-135)
136. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.365 [↑](#footnote-ref-136)
137. OPERATION FORTITUDE: THE CLOSED LOOP D-DAY DECEPTION PLAN S.1 [↑](#footnote-ref-137)
138. OPERATION FORTITUDE: THE CLOSED LOOP D-DAY DECEPTION PLAN S. 3 [↑](#footnote-ref-138)
139. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S. 365, Double Cross: The True Story of the D-Day Spies S. 6 [↑](#footnote-ref-139)
140. Double Cross: The True Story of the D-Day Spies S. 8 (Zitat übersetzt) [↑](#footnote-ref-140)
141. OPERATION FORTITUDE: THE CLOSED LOOP D-DAY DECEPTION PLAN S.3-4, Double Cross: The True Story of the D-Day Spies S. 8 [↑](#footnote-ref-141)
142. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.365 [↑](#footnote-ref-142)
143. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.365, OPERATION FORTITUDE: THE CLOSED LOOP D-DAY DECEPTION PLAN S.2,12 [↑](#footnote-ref-143)
144. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.366 [↑](#footnote-ref-144)
145. https://austria-forum.org/af/AustriaWiki/Enigma\_%28Maschine%29 [↑](#footnote-ref-145)
146. The Secrets of Station X: How the Bletchley Park codebreakers helped win the war S.172 [↑](#footnote-ref-146)
147. https://www.geo.de/wissen/weltgeschichte/zweiter-weltkrieg-operation-enigma-der-stille-kampf-der-30178208.html [↑](#footnote-ref-147)
148. The Secrets of Station X: How the Bletchley Park codebreakers helped win the war S.134 [↑](#footnote-ref-148)
149. <https://macau.uni-kiel.de/servlets/MCRFileNodeServlet/macau_derivate_00000492/0171_17.pdf> S.1 [↑](#footnote-ref-149)
150. The Secrets of Station X: How the Bletchley Park codebreakers helped win the war S.193 [↑](#footnote-ref-150)
151. War Hitler ein Feldherr? S.54 (https://books.google.de/books?hl=en&lr=&id=-8TFF5EQJx4C&oi=fnd&pg=PA9&dq=zweiter+weltkrieg+einfall+in+norwegen+und+dänemark+weserübung&ots=b8H-qjhKSs&sig=k\_0x4NN5j1WMZRRz7CKoH7XqRWk&redir\_esc=y#v=onepage&q&f=false) [↑](#footnote-ref-151)
152. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.202 [↑](#footnote-ref-152)
153. Geheime Botschaften Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet S.202, The Secrets of Station X: How the Bletchley Park codebreakers helped win the war S.192 [↑](#footnote-ref-153)
154. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.364 [↑](#footnote-ref-154)
155. Der Einfluß der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges S.349 [↑](#footnote-ref-155)
156. The Secrets of Station X: How the Bletchley Park codebreakers helped win the war S.88 [↑](#footnote-ref-156)