

# Codebrechen im 2. Weltkrieg: Die Entschlüsselung der Enigma- und Lorenzmaschine

Seminar: Geschichte der Rechnerarchitektur

Andreas Lorenz  
ge69dal@mytum.de

Mariia Borysova  
ga92zad@mytum.de

## ABSTRACT

Das Thema dieser Seminararbeit sind die Verschlüsselungstechniken der Enigma und der Lorenz-Schlüsselmaschine während des Zweiten Weltkrieges, sowie deren Entschlüsselung durch polnische Codeknacker, wie Marian Rejewski, und britische, wie Alan Turing, Gordon Welchman, John Tiltman und Bill Tutte. Bei der Entschlüsselung wird besonders auf die Entwicklung der Turing-Bombe und des Colossus eingegangen, welche den Ablauf zur Chiffrierung einzelner Nachrichten automatisieren. Zudem werden sowohl die zeitlichen Umstände und Geschichte der beiden Maschinen beschrieben sowie die Auswirkungen, die diese Maschinen auf den Krieg hatten.

Die Arbeit basiert auf mehreren Büchern und Onlinequellen über die Verschlüsselung und Entschlüsselung der Enigma und der Lorenz-Maschine.

## CCS Concepts

•**Social and professional topics** → **Historical people; History of hardware**; •**Security and privacy** → *Cryptanalysis and other attacks*; •**Theory of computation** → *Computational complexity and cryptography*; •**Mathematics of computing** → Probability and statistics;

## Keywords

Zweiter Weltkrieg, Enigma, Lorenz-Schlüsselmaschine, Arthur Scherbius, Colossus, Rotoren, Alan Turing, Marian Rejewski, Rotoren, Bomba, Zygaliski-Lochblätter, Turing-Bombe, Diagonal board, John Tiltman, Bill Tutte, Kryptologie

## 1. EINFÜHRUNG

Während des Krieges spielt die Verfügbarkeit einer zeitnahen und zuverlässigen Kommunikation zwischen den Einheiten eine besonders wichtige Rolle. Das ermöglicht es, die Aktionen von Truppen, die an verschiedenen Orten stationiert sind und verschiedene Funktionen ausführen, zeitnah zu koordinieren, um ein gemeinsames Ziel zu erreichen - den Sieg in einer bestimmten Schlacht und im gesamten Krieg.

Mit der Erfindung der Funkkommunikation im späten 19. Jahrhundert ist der Informationsaustausch schneller und einfacher geworden. Da Funksignale jedoch von jeder Person einfach mit einem Empfänger abgefangen werden können, ist eine verschlüsselte Übertragung wichtig, da sonst geheime Informationen in den falschen Händen fatale Folgen hätten. Eine abgefangene Nachricht in unverschlüsselter Form wäre dasselbe, als würde man zum Feind kommen und ihm persönlich über die eigenen Pläne Bericht erstatten.

Um zu Vermeiden, dass der Feind diese Nachrichten mitlaß, mussten diese also verschlüsselt übertragen werden. Desweiteren musste die Verschlüsselung auch sämtlichen Versuchen feindlicher Codeknacker widerstehen können, sodass der Feind auch beim Abfangen einzelner Nachrichten keine Möglichkeit hat, den Aufbau der benutzten Verschlüsselungstechnik herauszufinden, da sonst die Funktion der Verschlüsselung verloren ginge und die entschlüsselten Nachrichten dem Feind viele Vorteile bieten würden.

Die Wissenschaft, die sich sowie mit der Verschlüsselung, als auch mit der Entschlüsselung beschäftigt, heißt Kryptologie (aus dem griechischen Wort *"versteckt"*). Die Kryptologie hat bereits einen sehr langen Entwicklungsweg von primitiven Methoden aus dem 3. Jahrtausend v. Chr. bis hin zu modernen Computertechnologien hinter sich. Besonders während des Zweiten Weltkrieges spielte die Kryptologie eine sehr wichtige Rolle. Eine der bekanntesten kryptografischen Maschinen, die das deutsche Militär je gebaut hat, ist die Enigma. Obwohl die Enigma so berühmt war, gab es eine zweite Verschlüsselungsmaschine, nämlich die Lorenzmaschine, die im Krieg genauso wichtig war.

Während die tragbare Enigma hauptsächlich im Außendienst eingesetzt wurde, diente die etwas größere und schwere Lorenz-Maschine der Kommunikation auf hoher Ebene. Unter anderem nutzte auch Adolf Hitler diese zur Verschlüsselung geheimer Nachrichten.

In diesem Artikel werden sowohl der Aufbau und die Funktionsweise dieser Maschinen erläutert, als auch die Methoden, die die Geheimdienste der Alliiertenmächte für ihre Entschlüsselung benutzten.

## 2. ENIGMA

### 2.1 Geschichte

Der Name *Enigma* wird aus dem Griechischen mit *Rätsel* übersetzt und die Geschichte einer der berühmtesten Chiffriermaschinen beginnt 1918. In diesem Jahr hat der deutsche Erfinder Arthur Scherbius [Abbildung 1] das Patent für eine Chiffrier-Rotormaschine mit dem Mehrfach-Rotorverfahren bekommen [29].

Nach ein paar Jahren und einer Reihe von Verbesserungen der Erfindung wurde im Jahr 1923 die erste Maschine aus der Enigma Familie gebaut. Sie wurde *Handelsmaschine* [Abbildung 2] genannt. Das erste Modell hat den kodierte Text direkt auf Papier gedruckt, wie eine gewöhnliche Schreibmaschine. Es gab die Möglichkeit, zwischen der Kodierung, Dekodierung und dem üblichen Druckmodus auszuwählen. Die Handelsmaschine war nicht nur groß und schwer, son-



Figure 1: Arthur Scherbius (1878-1929) [34]

den auch extrem teuer in der Produktion [23].

Deswegen wurde in den späteren Enigmas der Druckmechanismus durch ein Glühlampenfeld ersetzt. Die erste solche Maschine, Enigma A, wurde im Jahr 1924 gebaut. 1926 wurde Enigma durch das Hinzufügen der Umkehrwalze weiter verbessert, dadurch gab es in der Enigma D schon keinen Unterschied mehr zwischen der Verschlüsselung und Entschlüsselung. Diese Version ist ein Basismodell für alle spätere Enigmas geworden [23].

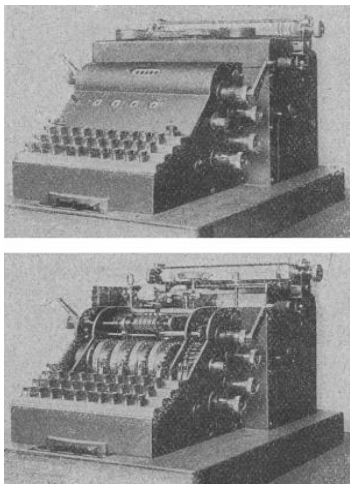


Figure 2: Handelsmaschine [23]

Im Jahr 1925 beginnt die militärische Geschichte der Enigma.

Diese beginnt mit einer schockierenden Entdeckung während des Ersten Weltkriegs. Die Briten haben die Mehrheit der deutschen Nachrichten für die Marine erfolgreich entziffert und gelesen. Deswegen sind die Deutschen zu dem Schluss gekommen, dass die ständige Wechslung des Codes nicht mehr genug war. Sie brauchten ein ganz neues System, das sogar bei der Aneignung sicher bleiben konnte [18].

Enigma war dafür perfekt geeignet. Erstens, war man nicht in der Lage nur mit einer Maschine, aber ohne passende, ständig wechselnde Einstellungen die Nachricht zu entziffern. Zweitens, war die Kodierungsvorschrift komplett von dem Menschen unabhängig, was die Anzahl von Fehlern deutlich reduzierte. Der Operator sollte nur die Maschine entsprechend einstellen, den Text eingeben, Ergebnisse einle-

sen und sie dann per Rundfunk senden [18]. Drittens, glaubte man, dass Enigma unknackbar war [19].

Am 15. Juli 1928 begann die Arbeit der Enigma bei der deutschen Armee. Sie war aber etwas anders als die kommerzielle Enigma: hatte z.B. ganz andere innere Verdrahtung von den Rotoren [18]. Bei der kommerziellen Enigma waren die Kontakte auf dem Eingangsring in QWERTZ Reihenfolge, wie auf der Tastatur, belegt. Die militärische hatte wiederum die Alphabetische Reihenfolge [3]. Im Jahr 1923 entstand die endgültige Version der militärischen Enigma, *Enigma I*, die nur für das Militär zur Verfügung stand [23].

Für verschiedene Armee-Einheiten wurden verschiedene Modelle der Maschine entwickelt [15]. Z.B., Enigma-G für die Abwehr und Enigma M4 für die Kriegsmarine [23].

Im Folgenden wird Enigma I [Abbildung 3], das Basismodell für alle militärischen Enigmas, im Detail betrachtet.

## 2.2 Aufbau

Enigma ist eine elektromechanische Verschlüsselungsmaschine, es hat die Größe von ungefähr 28 x 35 x 15 Zentimeter und wiegt etwa 12 Kilogramm [6]. Die 5 wichtigsten Elemente der Maschine sind Walzensatz (3 Rotoren, Reflektor, Stator), Tastatur, Glühlampenfeld zur Anzeige von Ergebnissen, Steckerbrett und Batterie [7].



Figure 3: Die Aufbau von der Enigma I [5]

### 2.2.1 Rotoren

Drehbare Walzen, auch *Rotoren* genannt, sind die wichtigsten Bestandteile für die Verschlüsselung des Textes. Ein Rotor ist eine Scheibe mit einem Durchmesser von ungefähr 10 Zentimetern [31].

Jede Walze hat 26 Kontakte auf den beiden Seiten, die den 26 Buchstaben des lateinischen Alphabets entsprechen. Im Inneren des Rotors sind die Kontakte auf zufälligerweise miteinander verbunden. Der elektrische Strom kommt durch den Kontakt auf einer Seite herein, dann fließt er durch den Draht innerhalb des Rotors und geht in einem Kontakt auf der anderen Seite hin [Abbildung 4.d] [7].

Damit wird ein Buchstabe durch den anderen ersetzt und eine sehr einfache Art der Verschlüsselung, elementare Er-

satzchiffre, erzeugt. Die Position der Walze wird mit einer Zahl oder einem Buchstaben gekennzeichnet [Abbildung 5.a] [7]. Enigma I enthält insgesamt 3 Rotoren mit unterschiedlichen inneren Verbindungen [Abbildung 4.c] [31].

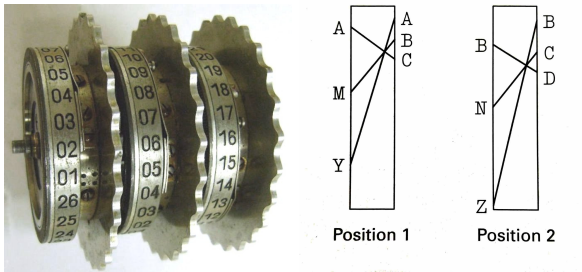
Nach jedem Tastendruck wird der ganz rechte Rotor um eine Position gedreht. Zusätzlich verfügt das Gerät über einen eingebauten Mechanismus, mit dem eingestellt werden kann, wann die restlichen der zwei Rotoren gedreht werden [31]. Dafür haben die Rotoren einen Ring mit einer V-förmige Kerbe auf einer Seite [Abbildung 4.a] und einen Zahnkranz mit 26 Zähnen auf der anderen [Abbildung 4.b] [7]. Diese Einstellung nennt man Ringstellung [31].

Mit ihrer Hilfe erzeugt die Enigma eine polyalphabetische Verschlüsselung. Das bedeutet, dass wegen der Rotor-drehung für jeden nacheinander folgenden Buchstaben ein anderes Alphabet benutzt wird und die Ereignisse nach der mehrfachen Kodierung des gleichen Buchstabens nicht unbedingt gleich sein müssen [31].



(a) Die Kerbe [31]

(b) Der Zahnkranz [31]



(c) Walzensatz aus 3 zusammen- (d) Innere Verkabelung von  
gesetzten Rotoren [31] dem Rotor[7]

Figure 4: Rotoren

### 2.2.2 Reflektor und Stator

Die Eintrittswalze, auch *Stator* genannt, ist in der Enigma fixiert und dient, zur Leitung des Stroms von der Tastatur zu den Rotoren und zurück von den Rotoren zu den Lampen [7].

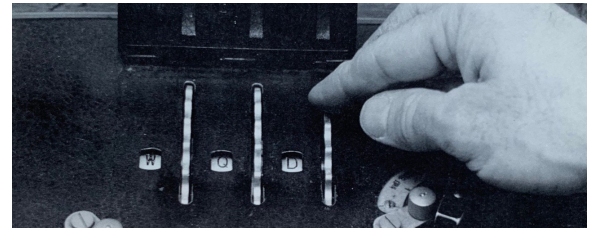
Die Umkehrwalze, auch *Reflektor* genannt, ist nach dem 3. Rotor, ohne die Fähigkeit zu drehen, in der Maschine eingestellt. Seine Aufgabe ist es, die 26 Kontakte paarweise miteinander zu verknüpfen. Der Strom, der in einen der Kontaktpunkte des Reflektors fließt, tritt also an einem anderen Kontaktpunkt aus, und verbindet 2 Buchstaben miteinander [7].

Damit kann man einen symmetrischen Code bekommen und muss nicht zwischen der Kodierung und Dekodierung unterscheiden. Das macht den Prozess der Entschlüsselung viel leichter, aber der Nachteil liegt darin, dass bei solchen

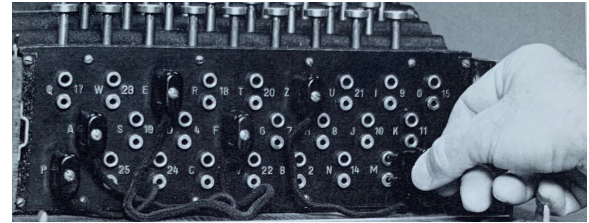
Verfahren ein Buchstabe nie in sich selbst kodiert werden kann [31].

### 2.2.3 Steckerbrett

Im Gegensatz zur kommerziellen Enigma, hatte das militärische Modell noch ein Element [7], dass im Jahr 1930 hinzugefügt wurde [6], das *Steckerbrett* [Abbildung 5.b]. Es hat 26 Buchsen, die paarweise miteinander mit Kabeln verbunden werden können. Diese Verbindung dient zum Vertauschen von Buchstaben vor dem Eintritt und nach dem Ausgang aus dem Walzensatz [7].



(a) Walzstellung [18]



(b) Steckerbrett [18]

Figure 5: Elemente von der Enigma

### 2.2.4 Funktionsweise

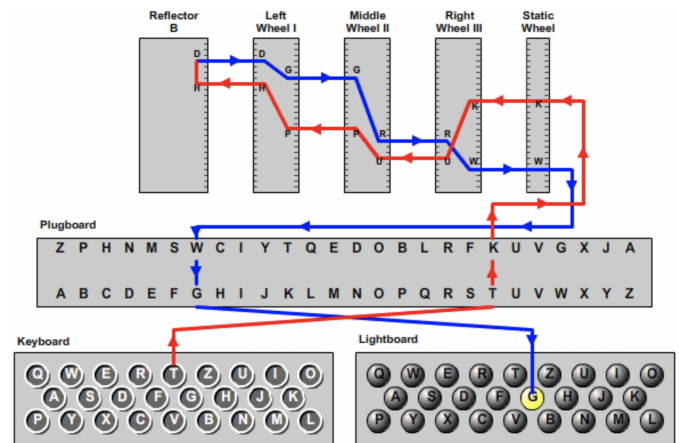


Figure 6: Funktionsweise der Enigma [9]

Jetzt kann man die ganze Funktionsweise der Maschine sehen [Abbildung 6]. Der Chiffrieroperator drückt die Taste *T*, damit wird der Stromkreis geschlossen und Kodierungsvorschritte angefangen.

Auf dem Steckerbrett ist *T* mit *K* verbunden, deswegen wird *T* durch *K* vor dem Eintritt des Walzensatzes vertauscht. Dann kommt der Strom in den Stator herein, wo



das Signal zu den Rotoren geleitet wird. Aufgrund der internen Verdrahtung wird  $K$  durch  $U$  im rechten (schnellen) Rotor vertauscht, dann  $U$  durch  $P$  im mittleren und  $P$  durch  $H$  im linken (langsamen).

Jetzt kommt der Strom in den Reflektor, wo  $H$  mit  $D$  vertauscht wird. Das Signal fließt jetzt durch den Walzensatz zurück und der Buchstabe wird immer wieder verändert. Endlich kommt der Strom wieder zum Steckerbrett, wo  $W$  mit  $G$  verbunden ist und auf dem Glühlampenfeld leuchtet  $G$  als Endergebnis.

Hier ist besonders gut die Aufgabe des Reflektors sichtbar: wenn man  $T$  drückt, wird  $G$  als Endergebnis angezeigt und umgekehrt bekommt man  $G$  aus  $T$  [9].

### 2.2.5 Schlüsselraum

Um den Schlüsselraum von Enigma zu berechnen, muss man 4 Einstellungen betrachten:

- *Die Walzenlage*

Ab dem Jahr 1938 konnte man 3 aus 5 verfügbaren Walzen wählen [3], insgesamt ergeben sich 60 mögliche Permutationen.

- *Die Walzenstellung*

Es war möglich für jeden Rotor eine aus 26 Startpositionen zu wählen, also insgesamt 17.576 Möglichkeiten.

- *Die Ringstellung*

Diese Einstellung war nur für den rechten und mittleren Rotor sinnvoll, insgesamt 676 Kombinationen.

- *Die Steckerverbindungen*

Ab 1939 sollte man genau 20 Buchstaben auf dem Steckerbrett miteinander verbinden [3], insgesamt 150.738.274.937.250 Kombinationen [31].

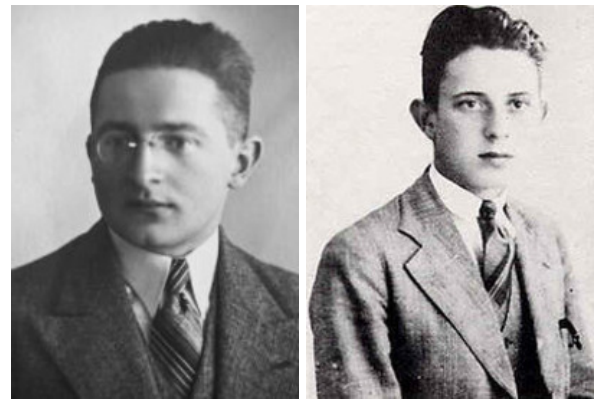
Insgesamt bekommt man mehr als  $1,07 \cdot 10^{23}$  verschiedene Möglichkeiten Enigma einzustellen, was einem 77-Bit Schlüssel entspricht [31]. Wenn eine Mannschaft aus 1000 Kryptoanalytikern 4 Schlüssel pro Minute, den ganzen Tag, jeden Tag prüfen wird, dann braucht sie 1,8 Milliarde Jahren, um alle Möglichkeiten durchzugehen [18].

### 2.2.6 Schlüsseltafel

Um die Möglichkeit zu haben, Nachrichten auszutauschen, sollen die Maschinen bei den zwei Chiffrieroperatoren gleich angepasst werden. Für diesen Zweck wurden sogenannte Schlüsseltafeln entwickelt, die für einen ganzen Monat ausgeteilt wurden. Sie beinhaltete die Einstellungen für die Maschine (Walzenlage, Ringstellungen, Steckerverbindungen) für jeden Tag des Monats [18]. Die Grundstellungen wurden jeden Tag um Mitternacht geändert [2].

## 2.3 Entschlüsselung: Polen I

Polnische *Biuro Szyfrow* (BS), Chiffrierbüro, hat sich mit der Entzifferung von deutschen Codes schon seit 1920 erfolgreich beschäftigt. Aber mit dem Erscheinen von Enigma in 1926 hat sich die Situation verschlechtert und das Büro konnte nicht mehr die geheimen Nachrichten der Deutschen lesen. 1929 wurde ein Kurs in der Kryptologie für Mathematiker organisiert. Nur 3 Studenten, *Marian Rejewski* [Abbildung 7.a], *Jerzy Rozycki* [Abbildung 7.b] und *Henryk Zygałski* [Abbildung 7.c] haben ihn erfolgreich abgeschlossen [6].



(a) Marian Rejewski  
(1905 - 1980) [23]

(b) Jerzy Rozycki  
(1909 - 1942) [23]



(c) Henryk Zygałski  
(1908 - 1978) [23]

Figure 7: Mitarbeiter von Biuro Szyfrow

Im Jahr 1932 haben sie die Arbeit als Stammmitarbeiter bei Biuro Szyfrow angefangen, wo sie sich mit der Entzifferung von Enigma beschäftigt haben. Zu ihrer Verfügung stand ein kommerzielles Modell von Enigma, die aber andere innere Verdrahtungen von Rotoren als militärische Maschine hatte. Weitere Hilfe hat Polen von Frankreich bekommen [6].

Der französische Geheimdienst hat die geheimen Dokumente von einem Spion mit dem Codename *Asche*, Hans-Thilo Schmidt, aus der deutschen Chiffrierstelle gekauft. Unter anderem haben die Polen Gebrauchsanweisungen, Schlüsselanweisungen und Schlüsseltafeln für ein paar verschiedene Monaten bekommen [20]. Bis zum Ende des Jahres hat Rejewski mit Hilfe der Permutationstheorie die interne Verkabelung der militärischen Enigma rekonstruiert [6].

Die Schwachstelle lag aber nicht bei der Konstruktion der Maschine, sondern bei der Methode, mithilfe deren man die Nachrichten verschlüsselt hat. Es war zu aufwendig für jede einzelne Nachricht neue Grundstellungen zu wählen, deswegen wurden die sogenannten *Spruchschlüssel* eingeführt. Die Kodierungsvorschrift sah folgendermaßen so aus:

1. Der Operator sollte mithilfe der Grundstellungen aus der Schlüsseltafel die Maschine geeignet einstellen (Walzenlage, Walzenstellung, Ringstellung, Steckerverbindungen).
2. 3-Buchstaben-Gruppe (Spruchschlüssel) beliebig wäh-



len und sie doppelt mit der Enigma kodieren (z.B., Walzenstellung *CLM*, Gruppe *HPU*, Kodierung: *HPU HPU* -> *JDK ZEP*)

3. Die Nachricht mit dem Spruchschlüssel *HPU* kodieren und *JDK ZEP* am Anfang der Nachricht hinzufügen.

Die Verdopplung hat man benutzt, um sicher zu sein, dass der Spruchschlüssel richtig durchgegeben wurde. Diese Eigenschaft, die zu der Sicherheit von Enigma dienen sollte, wurde von Polen für die Entzifferung benutzt [3].

Auf jeden Fall wäre es sinnvoller gewesen ein unabhängiges Verfahren für die Verschlüsselung des Spruchschlüssels zu nutzen, wie es ab dem Jahr 1941 für das 4-Rotoren für die Marine eingeführt wurde. So konnte der Feind keine Schlussfolgerungen über den inneren Aufbau der Maschine aus dem Schlüssel ziehen [3].

Polen haben gewusst, dass nach der Dekodierung an der 1. und 4., sowie 2. und 5., 3. und 6. Position die gleichen Buchstaben stehen werden. Daraus konnten sie mithilfe der mathematischen Umformungen bestimmte Abhängigkeiten zwischen den Buchstaben und Positionen von Rotoren ableiten. Wenn es genug Funksprüche (von 50 bis 100) für denselben Tag gab, konnten die Grundstellungen des Tagesschlüssels rekonstruiert werden [3].

Polen haben ein Gerät, *Zyklometer* [Abbildung 8] gebildet, dass die Wiederherstellung von Walzenlagen und Einstellungen beschleunigt hat. *Zyklometer* bestand aus 2 zusammengesetzten Enigma-Walzensätzen [18]. Dank ihm wurde nach einem Jahr der Arbeit, 1937, der Katalog aufgestellt, mit welchem man den Tagesschlüssel in 10-20 Minuten knacken konnte [3].

Diese Methode hat erfolgreich bis zum 15. September 1938 funktioniert, bis die Deutschen die Kodierungsvorschriften geändert haben. Damit war der Katalog nicht mehr gültig [3].



Figure 8: Zyklometer [23]

## 2.4 Entschlüsselung: Polen II

Mit der neuen Vorschrift sollte der Operator die Walzenstellung nicht aus der Schlüsseltafel einlesen, sondern sich auch selbst ausdenken und als Klartext am Anfang der Nachricht schicken. Wenn es eine Nachricht gab, die mit z.B. *RTJ WAH WIK* angefangen hat, wusste man, dass *RTJ* die zufällig gewählte Walzenlage war und *WAH WIK* mit *RTJ* die doppelt verschlüsselte Spruchschlüssel, gefolgt von dem mit dem Spruchschlüssel kodierte Text [3].

Um mit dieser Methode umgehen zu können, wurde ein neues Gerät entwickelt, das *Bomba* oder auch *Bomba kryptologiczna* [Abbildung 9] genannt wurde [3]. Es war eine

elektromechanische Maschine, die aus 6 paarweise zusammengesetzten Enigma-Walzensätzen bestand. *Bomba* konnte 17.576 verschiedene Kombinationen pro ungefähr 2 Stunden durchgehen [20].



Figure 9: Bomba kryptologiczna [23]

Die Maschine hat die Suche nach dem Muster *123123* im Spruchschlüssel durchgeführt. In jedem Paar wurde ein Walzensatz um 3 Positionen weiter versetzt im Vergleich zu den anderen, da bekannt wurde, dass nach der Entschlüsselung an der um 3 versetzte Position der gleiche Buchstabe stehen muss. Um die Maschine nutzen zu können, sollte man zuerst genug Sprüche sammeln. Es wurde nach solchen Sprüchen gesucht, wo an der 1. und 4., sowie 2. und 5., 3. und 6. Position der gleiche Buchstabe steht. Wie z.B. *W* in

RTJ | WAH WIK  
DQX | DWJ MWR  
HPL | RAW KTW

*Bomba* war gegen die Steckerverbindungen empfindlich, deswegen sollte man solchen Buchstaben finden, der nicht mit einem anderen auf dem Steckerbrett verbunden war. Bei der Verwendung von 5 bis 8 Stecker Paaren lag diese Wahrscheinlichkeit bei ungefähr 50%. Wenn man aber nicht *W* für alle 3 Sprüche benutzt hat, wie es im Beispiel, sondern jedes Mal einen anderen Buchstaben, senkte das die Wahrscheinlichkeit auf 12,5% [3].

Zuerst soll die Maschine geeignet eingestellt werden [Abbildung 10]. Das erste Paar der Walzensätze bekommt die Walzenstellungen *RTJ* und *RTJ* um 3 Positionen versetzt, also *RTJ+3*, zweites *DQX* und *DXQ+3* und drittes entsprechendes *HPL* und *HPL+3*. Dann sollte man ständig den Testbuchstaben *W* eingeben und warten, bis die Maschine gleichzeitig die Koinzidenz der Buchstaben in jedem der drei Paaren signalisierte, also ein Muster *123123* gefunden wurde. Dann sollte man das Ergebnis manuell mit einer Enigma überprüfen. Bis Dezember 1938 existierten nur 3 Rotoren, aus welchen sich insgesamt 6 Möglichkeiten für die Walzenlage ergaben. Deswegen wurden 6 Bombas gebaut, eine für jede Walzenlage [3].

Zu dieser Zeit wurde noch eine Methode für die Entzifferung entwickelt: *Zygalski Lochblätter* [Abbildung 11]. Dieses

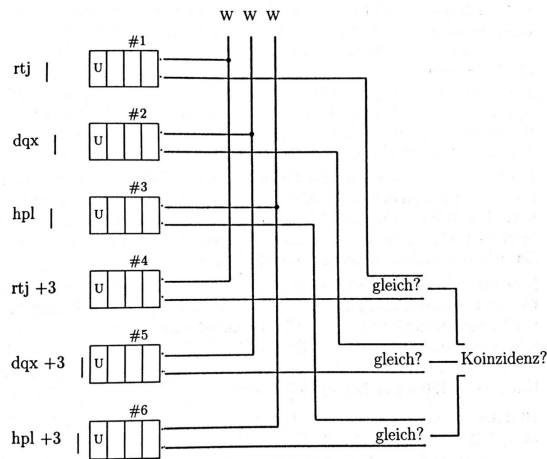


Figure 10: Funktionsweise von Bomba [3]

Verfahren hat auch eine Schwachstelle bei der Doppelkodierung benutzt. Jedes Blatt hatte die Fläche von ungefähr 60 Zentimetern und war in 51 x 51 Quadrate durch wiederholtes Alphabet (A bis Z und A bis Y) nach der Länge und Breite aufgeteilt. Jedes Blatt hat für den schnellen (rechten) Rotor die Positionen von 2 anderen Rotoren im Hinblick auf die bestimmten Abhängigkeiten zwischen den Buchstaben fixiert. Dafür sollte man die Löcher an bestimmten Positionen machen. Dann sollten 4 Blätter über einer Lichtquelle aufeinandergelegt werden. Die Löcher, in welchen es Licht gab, haben den möglichen Walzenstellungen und Ringstellungen entsprochen. Die Methode war gegen die Steckerverbindungen unempfindlich. Man brauchte aber 26 Blätter für jede Walzenlage, also 156 insgesamt und jedes Blatt sollte ungefähr 1000 Löcher an ganz bestimmten Positionen haben. Ihre Herstellung dauerte viel länger als die Herstellung von Bombas [18].

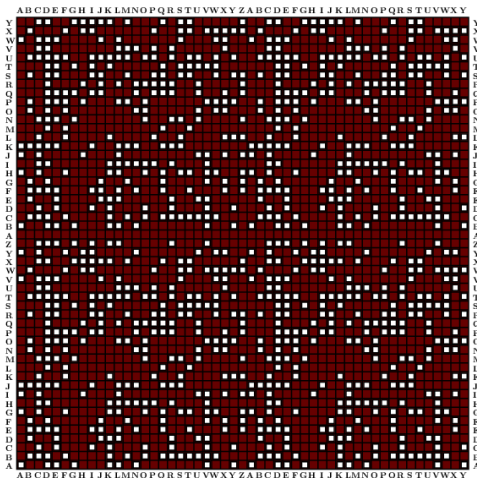


Figure 11: Zygalski-Lochblätter [36]

Am 15. Dezember 1938 haben die Deutschen zwei neue Walzen IV und V eingeführt. Obwohl Rejewski die innere Verdrahtung schnell rekonstruiert hatte, gab es schon 60 statt 6 mögliche Walzenlagen. Das bedeutete, dass man 60

Bombas brauchte, um alle Walzenlagen gleichzeitig überprüfen zu können. Das Budget von Biuro Szyfrow wurde 15 Mal überschritten. Man brauchte auch 1.560 Zygalski-Lochblätter, aus welchen zu diesem Zeitpunkt insgesamt nur 52 hergestellt wurden [18].

Im Januar 1939 haben die Deutschen angefangen 10 Paare auf dem Steckerbrett gleichzeitig zu verbinden. Die Wahrscheinlichkeit, einen ungesteckerten Buchstaben zu finden, ist drastisch gesunken. Das hat Bomba fast unbrauchbar gemacht [18]. Endlich haben die Deutschen im April 1940 auf die Doppelverschlüsselung verzichtet, was die beiden Methoden gleichzeitig nutzlos gemacht hat [3].

## 2.5 Entschlüsselung: Großbritannien

Am 25. Juli 1939 fand in Pyry, im Süden Warschaus, zwischen den Polen, Briten und Franzosen ein Treffen statt. Während des Treffens haben Briten als auch Franzosen polnische Repliken von Enigma mit allen 5 Rotoren bekommen. Polen haben auch die Bombas und Lochblätter gezeigt und ihre Funktionsweise den Verbündeten erklärt [18]. Ab diesem Zeitpunkt hat sich schon Großbritannien statt Polen mit der Entzifferung von der Enigma beschäftigt.

Alan Turing [Abbildung 12], junger Mitarbeiter von *Government Code and Cypher School*, wollte ein Verfahren erfinden, dass von der Doppelverschlüsselung, als auch von den Steckerverbindungen unabhängig war. Und das hat er mit der Methode, die man als Klartext-Geheimtext-Kompromittierung kennt, geschafft. Grundlage der Methode ist die Suche nach einem wahrscheinlichen Wort (*Crib*) im kodierten Text [3].



Figure 12: Alan Turing (1912 - 1954) [25]

Das deutsche Militär hat sich gewöhnlich sehr stereotyp ausgedrückt. Z.B., wenn eine Nachricht am frühen Morgen abgefangen wurde, konnte sie wahrscheinlich eine Wettervorhersage sein. Daraus konnte man eine Vermutung anstellen, dass die Nachricht genau das Wort "Wettervorhersage" enthält. Jetzt kommt die Besonderheit der Umkehrwalze ins Spiel, nämlich dass ein Buchstabe nie in sich selbst kodiert werden kann. Damit kann die wahrscheinliche Position des Wortes im kodierten Text gefunden werden [Abbildung 13] [13].

Z.B. an der ersten Position geht S in sich selbst, also das kann nicht die Position des Wortes sein, an der zweiten bricht

V die Regel und so weiter. An Position 4 gibt es aber keine Widersprüche, deswegen kann man vermuten, dass das Wort genau hier steht.

- ...QFZWRWIVTYRESXBFOGKUHQBAISEZ...
1. WETTERVORHERSAGEBISKAYA
  2. WETTERVORHERSAGEBISKAYA
  3. WETTERVORHERRAGEBISKAYA
  4. WETTERVORHERSAGEBISKAYA
  5. WETTERVORHERSAGEBISKAYA
  6. WETTERVORHERSAGEBISKAYA

Figure 13: Crib

Jetzt kann Crib dem kodierten Text zugeordnet und alle Paare durchnummeriert werden [Abbildung 14].

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B	A	I	S	E
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A

Figure 14: Zuordnung von Crib dem kodierten Text [13]

Daraus folgt, dass bei einer aus allen möglichen Einstellungen von Enigma der Buchstabe R in W kodiert wird und umgekehrt. Diese Einstellung wird als Position 1 benannt. Dann dreht sich ein Rotor oder wahrscheinlich auch mehrere Rotoren um eine Position, W geht jetzt in E und E in W (Position 2). Dann wieder Drehung, I in T (Position 3) und so weiter. Alle diese Übergänge können als ein Diagramm dargestellt werden, wo die Quadrate die Walzen und die Zahlen die Positionen repräsentieren [Abbildung 15] [13].

Jetzt nimmt man an, dass Enigma auf eine ganz bestimmte Weise konfiguriert ist (beliebige, aber bestimmte Walzenlage, Walzenstellungen, Ringstellungen und Steckerverbindungen). Dann behauptet man, dass K auf dem Steckerbrett mit E verbunden ist. Im Folgenden wird das Diagramm [Abbildung 15] betrachtet. Dieses Diagramm wird *Menu* benannt [13].

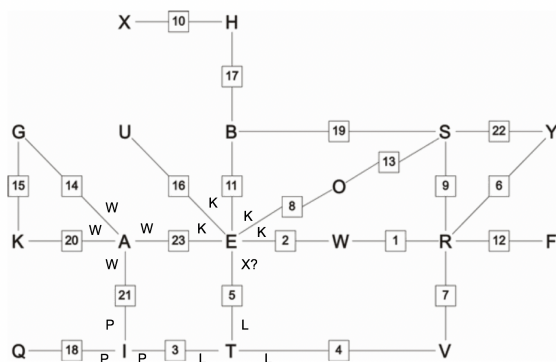


Figure 15: Crib und Text als Diagramm [12]

Wenn K mit E verbunden ist, dann kommt das Signal als E in die Walzen an Position 23. Das Signal fließt durch alle

Walzen und verlässt den Stator als W. Aus dem Diagramm folgt, dass W auf dem Steckerbrett mit A verbunden ist, deswegen fließt das Signal wieder als W an Position 21. Nach der Kodierung von W im Walzensatz bekommt man den Buchstaben P, der auf dem Steckerbrett mit I verbunden ist. So geht man weiter und es tritt ein Problem beim Verlassen des Walzensatzes an der Position 5 ein. Nach der Kodierung bekommt man X als Ergebnis und das Diagramm zeigt, dass X mit E verbunden ist [13].

Aber hier liegt der Widerspruch, da am Anfang behauptet wurde, dass E auf dem Steckerbrett mit K verbunden ist. Die Konstruktion der Maschine lässt nur zwei Buchstaben gleichzeitig miteinander verbinden, deswegen kann E nur entweder mit K oder mit X ein Paar erzeugen. Daraus folgt, dass unsere Behauptung über die Steckerverbindung für die früher gewählten Einstellungen falsch ist [13].

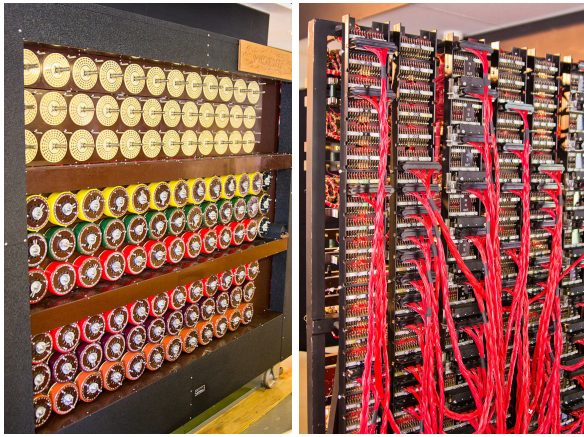
Jetzt muss man eine andere Behauptung finden (wie z.B. E mit H) und sie überprüfen. Wenn alle Möglichkeiten überprüft werden, dreht man den Rotor und beginnt wieder von vorne. Wenn das Diagramm mindestens 4 Schleifen enthält, gibt es nicht so viele Möglichkeiten, die keinen Widerspruch erzeugen. Im Allgemeinen müssen nur alle Behauptungen für alle möglichen Einstellungen der Maschine überprüft werden [13].

Und das war genau die Aufgabe der Maschine, die in der Mitte 1940 im *Bletchley Park* gebaut wurde [18]. Heutzutage ist sie als *Turing-Bombe* bekannt. Sie wog eine Tonne und hatte die Größe von ungefähr 2,1 x 2 x 0,6 Meter. An der Vorderseite hatte sie 108 Trommeln [Abbildung 16.c], die in drei 12 x 3 Arrays angeordnet waren. Jede Trommel hat die gleiche Transformation wie entsprechender Enigma Rotor dargestellt. Und drei Rotoren eines Triplets haben genau einen vollen Walzensatz dargestellt [Abbildung 16.a]. Die Rotoren und der Reflektor hatten zwei konzentrische Kreise mit 26 Anschlüssen anstelle eines Kreises in der Enigma. So wurden die Sätze miteinander verbunden und wurden *double-ended scrambler* genannt [13]. Jede Bombe bestand aus 12 Enigmas und diagonal boards. Damit konnte man alle 60 Walzenlagen mit 5 Bomben darstellen [18].

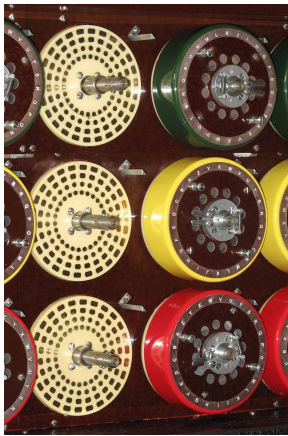
Zu den mehreren Kopien von Enigma wurde ein Testregister hinzugefügt, ein Satz von 26 Relais. Die Bombe hat alle Positionen der Rotoren nacheinander geprüft und in jeder der Positionen hat das Register die Spannung an den 26 Kontakten, die dem Glühlampenfeld von der Enigma entsprechen, betrachtet. Wenn also nur ein Kontakt oder alle, außer einer, gleichzeitig beleuchtet werden, hat man die Positionen von Rotoren bekommen, bei welchen es keinen Widerspruch gab. Die Arbeit der Maschine wurde dann unterbrochen, diese Kombination war eine wahrscheinliche Lösung und sollte manuell überprüft werden, weil es auch die falschen Unterbrechungen gab [18].

Am Anfang hat man die Basiseinstellungen für Bombe gewählt: Rotoren I, II und III, Positionen AAA. Es wurde erwartet, dass sich innerhalb von Crib der mittlere Rotor nicht dreht, deswegen wurden die Ringstellungen einfach ignoriert. Die Position der Bombe stellt die eine aus 26 möglichen Steckerverbindungen für den ersten Buchstaben von Crib dar. Die Spannung fließt durch den Walzensatz des ersten Paares aus dem Menu, den Reflektor, wieder den Walzensatz und dann durch den Walzensatz, der das zweite Paar von Buchstaben aus der Schleife testet. Der zweite Walzensatz wird in Bezug auf den ersten Walzensatz um die Zahl versetzt, die die Differenz zwischen den beiden Paa-





(a) Nachbau der Turing-Bombe im Bletchley Park Museum [41] (b) Die Kabel für die Verkabelung von Menus, die diagonal board enthalten [41]



(c) Trommel [41]

Figure 16: Turing-Bombe

ren im Text darstellt. So fließt der Strom weiter, bis er alle Paare aus dem Crib durchgeht und wieder in erstes Paar ein- kommt. Am Ende fließt er durch das Testregister und prüft die Spannung [18].

Wenn nicht nur die Walzen richtig eingestellt, sondern auch die Verbindung auf dem Steckerbrett richtig gewählt wurde, wird die Spannung nur an einem Testpunkt ange- zeigt. Wenn die Rotoren richtig eingestellt waren, die Ver- bindung aber falsch gewählt, wird die Spannung an allen, außer einem Punkt, angezeigt. Alle anderen Fälle bedeuten, dass die Position von Rotoren falsch ist und provozieren ke- ine Unterbrechung der Arbeit [18].

Die Bombe hat theoretisch funktioniert, in der Praxis brauchte man aber lange Crips mit vielen Schleifen, um die notwendige Anzahl von Möglichkeiten eliminieren zu können und nicht zu viele Unterbrechungen zu provozieren. Hier hat die Methode von *Gordon Welchman* [Abbildung 17], *diagonal board* [Abbildung 16.b], geholfen [18].

Diagonal board ist eine 26 x 26 Matriz. Kontakte in dia- gonal board haben die Paare auf solche Weise erstellt [Ab- bildung 18]: der Kontakt in der Reihe *E* und Spalte *A* ist mit dem Kontakt in der Reihe *A* und Spalte *E* diagonal ver- bunden. So kann man elektrisch die Aussage darstellen, dass wenn *A* mit *E* gesteckt ist, dann ist auch *E* mit *A* gesteckt.



Figure 17: Gordon Welchman (1906-1985) [42]

Diagonal board wurde mit dem double-ended scrambler und dem Testregister verbunden [40].

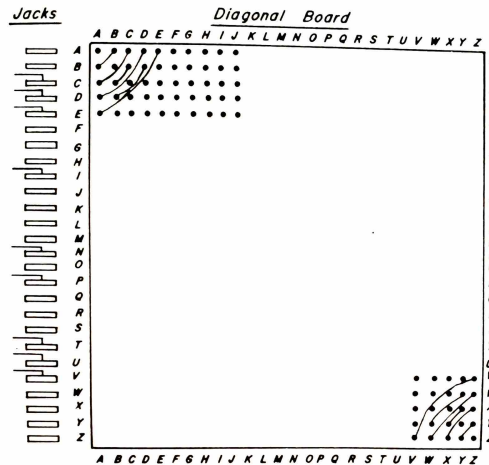


Figure 18: Diagonal board [40]

Es wird behauptet, dass *E* mit *A* verbunden ist. Wenn der Strom den Kontakt in Reihe *X* und Spalte *Y* auf dem board erreichen kann, folgt daraus, dass die Verbindung zwis- chen *X* und *Y* die logische Ableitung aus der Behauptung über die Verbindung von *E* mit *A* ist. Dann fließt der Strom zum Kontakt in der Reihe *Y* und Spalte *X* (*Y* ist mit *X* verbunden) wegen der Verbindung auf dem board und er existiert die Wahrscheinlichkeit, dass der Strom über die 26- polige Buchse, die der Reihe *Y* zugeordnet ist, wieder in die Scrambler kommt. Diese Methode hat die Anzahl von nutz- losen Unterbrechungen deutlich reduziert und die kürzeren Crips mit weniger Schleifen erlaubt [40].

Die Bombe brauchte etwa 12 Minuten für einen Durch- lauf. Am Anfang 1941 haben schon 8 Bomben funktioniert, bis zum Ende des Kriegs gab es insgesamt schon 200 Ma- schinen [3]. Das Heer und die Luftwaffe Enigma wurde end- lich geknackt und die Briten konnten ständig die deutschen

Nachrichte lesen.

Jetzt sollte man in der Lage sein, mit den weiteren Verbesserungen der Maschine umzugehen. Die Deutschen haben nicht gewusst, dass die Maschine kompromittiert wurde, sie hatten aber Angst, dass die Daten aufgrund verstärkter Kommunikation auslaufen können [19]. Das deutsche Militär hat bis zum Ende des Krieges nicht gewusst, dass die Enigma geknackt wurde [2]. Als Problem ist geblieben, die Enigma mit 4 Rotoren für die Kriegsmarine [Abbildung 19], die deutlich komplizierter als gewöhnliche Enigma war. Im Jahr 1942 haben die Briten auch diese Aufgabe gelöst und konnten mit relativer Regelmäßigkeit auch die Nachrichten der Marine ablesen [19].



Figure 19: Enigma M4 für die Kriegsmarine [23]

## 2.6 Ultra

Die Information über die Entzifferung der Enigma hatte die höchste Geheimhaltungsstufe beim britischen Militär, die sogar höher als Top Secret war [15]. Zuerst hatte die Operation den Namen *Boniface* bekommen, aber später wurde der Name *Ultra* für alle entzifferten Funksprüche von der Enigma eingeführt [19].

Der Premierminister von Großbritannien *Winston Churchill* [Abbildung 20] hat in 1940 befohlen, dass er täglich alle entzifferten Enigma Nachrichten bekommen muss.



Figure 20: Winston Churchill (1874 - 1965) [11]

Dass war aber wegen der Anzahl von Nachrichten sehr unpraktisch, deswegen hat er ab dem Jahr 1941 täglich ein

paar Dutzend der wichtigsten Nachrichten zusammen mit den Berichten über die Ergebnisse von Bletchley Park erhalten. Sie wurden in einer speziellen Box, welche nur von Churchill persönlich geöffnet werden konnte, geliefert [19].

Die Entzifferung von Enigma und dessen Einfluss auf den Zweiten Weltkrieg war ein großes Geheimnis bis zu den frühen siebziger Jahren. Der Grund war, dass Großbritannien Tausende von den Enigma Kopien für die Benutzung in den ehemaligen Kolonien gesendet hat [19]. Mehr als 10.000 Leute haben nur in Bletchley Park gearbeitet und sie alle haben das Geheimnis über Ultra gehalten [15]. Anfang der siebziger Jahre wurde Enigma nicht mehr gebraucht [19].

1974 wurde in Großbritannien eine Reihe von Artikeln veröffentlicht, in denen zum ersten Mal Ultra Secret erwähnt wurde. Dann folgten Dutzende von Büchern und Archiven in den Vereinigten Staaten und Großbritannien [19]. Insgesamt gab es 572 Bände mit 420.000 entzifferten Funksprüchen und Fernschreiben [3]. Dadurch hat die breite Öffentlichkeit von der Geschichte der Enigma und die Auswirkung ihrer Entzifferung auf den Ausgang des Krieges erfahren. Mithilfe des Knackens haben die Verbündete nicht nur viele Leben gerettet, sondern beispielsweise auch Atlantikschlacht gewonnen [19].

## 3. LORENZ SCHLÜSSELMASCHINE

### 3.1 Einführung

Etwas unbekannter als die Enigma, aber dennoch eine der wichtigsten Verschlüsselungsmaschinen während des Zweiten Weltkrieges war die Lorenzschlüsselmaschine. Die Lorenzschlüsselmaschine wurde von den Oberstenbefehlshabern, unter anderem auch Adolf Hitler, genutzt, um Nachrichten zu verschlüsseln.

Im Auftrag des deutschen Militärs wurde die Lorenzmaschine von der Firma C. Lorenz Ag in Berlin entwickelt und diente der Wehrmacht zur geheimen Kommunikation. Das erste Modell Schlüsselzusatz 40, kurz SZ40, wurde 1940 entwickelt und durch die Nachfolgemodelle SZ42a, SZ42b und SZ42c kryptographisch verbessert. Die Maschine selbst unterlag strengster Geheimhaltung, darum wurde nie ein Patent angemeldet und nahezu alle Exemplare nach Ende des Krieges zerstört. Im Deutschen Museum wird eine der weltweit letzten Originalmaschinen, die während des Krieges nicht zerstört wurden, ausgestellt [38].



Figure 21: Lorenz-Schlüssel-Zusatz SZ 42 mit Fernschreiber [16]



Die Lorenzmaschine nutzte zur Chiffrierung eine Addition eines pseudozufälligen Schlüssels zu einem Zeichen. Dazu musste diese als Zusatzgerät an einen Fernschreiber angeschlossen werden, welcher dann mithilfe von elektrischen Impulsen die verschlüsselte Nachricht überträgt [Abbildung 21]. Den Vorteil, den diese Art der Verschlüsselung gegenüber der Enigma hatte und warum sie so wertvoll für die deutschen Oberbefehlshaber war, war die maschinelle automatisierte Verschlüsselung und die Datenübertragung durch Fernschreiber, welche im Vergleich zu Morsecode stark erhöht war.

Ein weiterer Vorteil bestand darin, dass der Originaltext auf Empfängerseite durch nochmalige Addition des gleichen Schlüssels aus der empfangenen Nachricht gewonnen werden konnte [38].

Die Briten erfuhren bereits durch die Gefangennahmen von deutschen Kryptologen und von enzifferten Enigma-Funksprüchen von der neuen Innovation, aber schafften es bis 1941 nicht die chiffrierten Nachrichten zu entschlüsseln. Erst durch einen Fehler eines deutschen Nachrichtensoldaten konnten die Codeknacker einer geheimen Einrichtung bei Bletchley Park die Lorenzschlüsselmaschine entschlüsseln ohne diese jemals gesehen zu haben [8].

### 3.2 Aufbau

Die Lorenzmaschine war gegenüber der Enigma deutlich größer. Ihre Maße betrugen 50cm x 45cm x 45cm. Insgesamt bestand die Maschine aus 12 Nockenrädern [22].

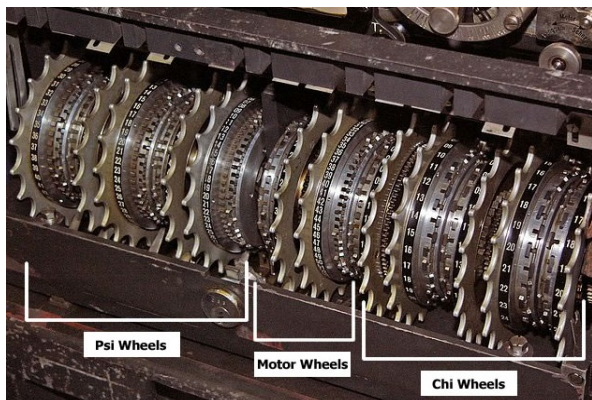


Figure 22: Nockenräder der Lorenzmaschine [38]

Jede dieser Nocken kann wie bei einer Binärzahl zwei Zustände annehmen: "aktiv" oder "inaktiv", was auch als "1" bzw "0" interpretiert werden kann [Abbildung 23]. Jedes Nockenrad variiert dabei in der Länge, was der Anzahl an Nocken auf einem Rad entspricht [33].

Die einzelnen 12 Räder lassen sich nochmals in drei Gruppen unterteilen, die in Tabelle 24 und Abbildung 22 dargestellt sind. Dabei unterscheiden sich die einzelnen Rotorguppen neben ihrer Nockenanzahl auch noch in der Häufigkeit der Drehungen sowie in ihrer Funktion, was im Folgenden erläutert wird [38].

Im Gegensatz zur Enigma, besaß die Lorenzmaschine keine eigene Tastatur, sondern musste an einen Funkschreiber angeschlossen werden.

### 3.3 Verschlüsselung

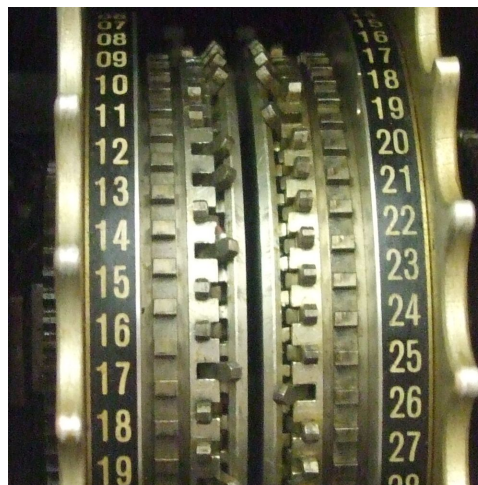


Figure 23: Nockenräder C3 und C4 [28]

Rad	Anzahl	Rad	Anzahl	Rad	Anzahl
A <sub>1</sub>	41	B <sub>1</sub>	61	C <sub>1</sub>	43
A <sub>2</sub>	31	B <sub>2</sub>	37	C <sub>2</sub>	47
A <sub>3</sub>	29			C <sub>3</sub>	51
A <sub>4</sub>	26			C <sub>4</sub>	53
A <sub>5</sub>	23			C <sub>5</sub>	59

Figure 24: Rotoren der SZ42 und zugehörige Nockenanzahl

Bei der Verschlüsselung wird der zu übertragende Klartext über die Tastatur eingegeben und mit einem "pseudo-zufälligen" Schlüssel exklusiv verodert [Abbildung 26]. Das Ergebnis kann daraufhin als verschlüsselter Text versandt werden.

Jedes Zeichen das über die Tastatur eingegeben wird, kann mit fünf Bits codiert werden. Dazu verwendete man den Baudot Code [Abbildung 25], der mit 5 Bits bis zu 56 Zeichen mithilfe von Umschalttasten darstellen konnte.

Diese fünf Bits eines Klartextbuchstabens werden in der Lorenzmaschine mit den fünf Bits des Schlüssels Bit für Bit "exklusiv-verodert". Der Schlüssel wiederum wird durch Veroderung der 5 Rädern aus Gruppe A mit den 5 Rädern aus Gruppe C generiert. Das resultierende Ergebnis aus Schlüssel und Originalbuchstabe bildet dann den chiffrierten Buchstaben, der gesichert übertragen werden kann.

Um einen möglichst zufälligen Schlüssel erzeugen zu können, haben die Rotorengruppen der SZ42 neben den unregelmäßig gezahnten Rädern auch verschiedene Bewegungsmuster. Die Räder der A Gruppe schalten nach jedem verschlüsselten Zeichen, während sich die Räder der C Gruppe nur in Abhängigkeit der Veroderung der ihnen vorrausgestellten Räder (von den Briten auch "Motorwheels" bezeichnet) bewegen. Ergab die XOR-Verknüpfung der B1- und B2-Räder eine 1, bewegten sich alle Rotoren der C Gruppe um eine Position, während sich bei einer 0 nichts änderte. B1 wiederum drehte sich wie auch die A Gruppe nach jedem Zeichen, wogegen sich B2 nur bewegte, wenn B1 einen Impuls erzeugte hat.

Die Verschlüsselung lässt sich wie folgend verallgemeinern [33]:



CODE ELEMENTS					LETTERS FIGURES
5	4	3	2	1	
		•	•	•	A
•	•	•	•	•	B
	•	•	•	•	C
•		•	•	•	D
		•	•	•	E
•	•	•	•	•	F
•	•		•	•	G
•		•	•	•	H
	•	•	•	•	I
	•		•	•	J
•	•	•	•	•	K
•		•	•	•	L
•	•	•	•	•	M
	•	•	•	•	N
•	•		•	•	O
•		•	•	•	P
•	•	•	•	•	Q
	•	•	•	•	R
	•	•	•	•	S
•		•	•	•	T
	•	•	•	•	U
•	•	•	•	•	V
•		•	•	•	W
•	•	•	•	•	X
•		•	•	•	Y
•		•	•	•	Z
	•	•			CARRIAGE RETURN
		•	•		LINE FEED
•	•	•	•	•	LETTERS
•	•	•	•	•	FIGURES
	•	•			SPACE
	•				ALL-STAR NOT USED

Figure 25: Baudot-Code [38]

Sei  $N$  der Klartext,  $S$  der Schlüssel und  $Z$  die verschlüsselte Nachricht. Dann kann die Verschlüsselung wie folgend formalisieren:

$$N \oplus S = Z$$

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Figure 26: XOR - Verknüpfung

Da die XOR-Verknüpfung selbstinvers ist, lässt sich die Formel umstellen zu:

$$Z \oplus S = N$$

Dies bedeutet, dass wenn auf der Empfängerseite nochmals der selbe Schlüssel aufaddiert wird, sich die Verschlüsselung gegenseitig aufhebt und der Empfänger als Resultat den Klartext bekommt. Eine verschlüsselte Nachricht kann also mithilfe einer Lorenzmaschine auch wieder entschlüsselt werden. Dafür ist es erforderlich, dass die Rotoren der beiden Maschinen gleich eingestellt wurden (auch bezeichnete als gleicher "Grundschlüssel") und im selben Startzustand (auch "SSpruchschlüssel") befanden [30]. Die Nocken der Räder wurden nur relativ selten verändert. Vor Sommer 1944 wurden die Nocken der C-Räder nur monatlich oder quartalsweise geändert, die der A-Räder monatlich und alleine die Nocken der beiden Kommandoräder täglich anders. Sender und Empfänger tauschten sich dazu im Bedarfsfall kurz aus und stellten dann zeitgleich auf den mithilfe geheimer Grundschlüsselblätter ihnen bekannten neuen Tagesschlüssel um. Im Gegensatz zur Nockeneinstellung änderte sich die Anfangsstellung der Räder, also der Spruchschlüssel bei jeder Nachricht. Um den richtigen Startzustand unter den  $1,6 \cdot 10^{19}$  möglichen Startzuständen zu finden, musste die richtige Einstellung mithilfe von 12 Geheimbuchstaben zu Beginn einer Nachricht gesendet werden. Jedem Geheimbuchstabe ist für jedes Rad eine Anfangsstellung zugeordnet, welche der Empfänger mithilfe einer Ablesetafel ablesen konnte und somit den richtigen Spruchschlüssel hatte [33].

Beispiel der Verschlüsselung und Entschlüsselung:

Gruppe A:	01010
Gruppe C:	00110
XOR - Verknüpfung	01100
Buchstabe "M":	11100
Schlüssel:	01100
verschlüsselter Buchstabe	10000

Figure 27: Buchstabe "M" wird zu "T" verschlüsselt

Angenommen der Buchstabe "M" soll verschlüsselt werden und die Lorenzmaschine ist so eingestellt, dass die Rotoren der A Gruppe den Wert "01010" ergeben und die Räder der C Gruppe den Wert "00110".

Zuerst müssen die Werte der beiden Rädergruppe exklusiv verodert werden. In unserem Beispiel ergäbe dies den Wert "01100", also den Schlüssel. Als nächstes wird der Schlüssel erneut mit dem Buchstaben M verodert, welcher im Baudot-Code als "11100" dargestellt wird. Das Ergebnis dieser Verschlüsselung ist "10000", was dem Buchstaben "T" entspricht [Abbildung 27].

Zur Entschlüsselung wird genau die selbe Vorgehensweise auf Empfängerseite wiederholt und der Originalbuchstabe "M" erscheint.

### 3.4 Entschlüsselung

Im Folgenden wird erläutert, wie die Briten es schafften, die Lorenzschlüsselmaschine zu knacken, ohne diese jemals gesehen zu haben.

Ab 1940 wurde die Lorenzmaschine von den Deutschen zur Verschlüsselung der Funksprüche eingesetzt. Die Briten wussten bereits aus den entzifferten Enigmafunksprüchen und der neuen Gefangennahmen von deutschen Kryptologen von einer neuen Erfindung namens "Sägefisch". Trotzdem konnten die britischen Codeknacker kein Muster in den abgefangenen Verschlüsseltexten erkennen und bezeichneten die Lorenzmaschine fortan "Tunny" (Tunfisch, in Anlehnung zum deutschen Begriff "Sägefisch").

Am 30. August 1941 gelang es einer britischen Abhörstelle eine ca. 4000 Zeichen lange Nachricht der Deutschen abzufangen, die von Athen nach Wien geschickt wurde. Da der Empfänger in Wien die Nachricht nicht korrekt lesen konnte, forderte er den Sender auf, diese zu wiederholen. Dabei sind dem Nachrichtensoldaten in Athen jedoch zwei Fehler unterlaufen [39]:

1. Bei der zweiten Nachricht wurde der bereits verbrauchte Spruchschlüssel verwendet mit dem die erste Nachricht verschlüsselt wurde. Dies war aus Sicherheitsgründen verboten, denn jeder Schlüssel musste nach einmaligen Benutzen verworfen werden, was jedoch hier nicht geschah.
2. Vermutlich aus Bequemlichkeit oder Frust die Nachricht wiederholt in den Funkschreiber eintippen zu müssen, verkürzte der Nachrichtensoldat den Text geringfügig. So schrieb er beispielsweise statt "SSPRUCHNUMMER" nur "SSPRUCHNR". Somit hatten die Briten nun zwei unterschiedliche Texte.

Durch diesen Fehler waren sie jetzt im Besitz einer sogenannten "depth", also zwei unterschiedlichen Geheimtexten, denen zwei nahezu identische Klartexte zugrundeliegen, die beide mit einem identischen Schlüssel verschlüsselt wurden (Im deutschen: "Klartext-Klartext-Kompromiss") [30].

John Tiltman [Abbildung 28], einer der besten Dechiffrierer in Bletchley Park (eine geheime militärische Dienststelle zur Entschlüsselung von Nachrichten), erhielt nun die Aufgabe, sich um Tunny zu kümmern. Tiltman stellte die Hypothese auf, dass es sich dabei um eine Maschine handeln musste, die das Prinzip eines binären Addierens eines Schlüssels auf den zu übermittelnden Text verwendete. Die entscheidende Frage war nun, wie das Gerät die zur Verschlüsselung benötigten Zufallsmuster generierte. Obwohl die britische Funkaufklä-

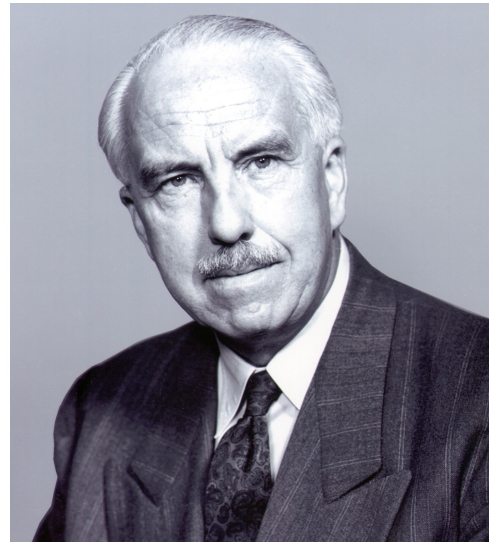


Figure 28: John Tiltman [1]

rung weitere abgefangene Nachrichten in größerer Zahl nachlieferte, kamen die Codeknacker zunächst nicht voran. Erst mithilfe der depth vom 10. August 1941 schafften es Tiltman und seine Kollegen erste Erkenntnisse zu ziehen. Wenn die Hypothese stimmte würden sich durch die exklusive Verodierung der beiden abgefangenen Funksprüche die benutzten Schlüssel gegenseitig aufheben [39].

Seien  $Z$  und  $Z'$  die Geheimtexte,  $S$  der gemeinsame Schlüssel und  $N$  und  $N'$  die unterschiedlichen Originalnachrichten, dann lässt sich ihre Vermutung wie folgend formalisieren:

$$Z = N \oplus S \text{ bzw. } Z' = N' \oplus S$$

Verknüpft man nun  $Z$  und  $Z'$  mit der XOR-Verknüpfung und setzt die obige Formeln ein, erhält man:

$$Z \oplus Z' = N \oplus S \oplus N' \oplus S = N \oplus N'$$

Das Resultat war eine Verknüpfung der beiden Nachrichten. Wenn nun die Hypothese stimmte, könnte man durch geschicktes Einsetzen von Wörtern die Originaltexte rekonstruieren. Zuerst fingen sie an häufige Wörter für alle möglichen Stellen des Textes einzusetzen. Falls das Wort an der richtigen Stelle war, würde die Verodierung mit dem Resultat einen deutschen Begriff ergeben, da sich der Text der das Wort an dieser Stelle enthält, wegfallen würde. Folgender Term veranschaulicht nochmals die zu Grunde liegende Forme [39]:

$$N \oplus N' \oplus N = N'$$

Erste Erfolge bestätigten die Hypothese und es gelang den Briten innerhalb von zwei Wochen nicht nur die kompletten Originaltexte zu entschlüsseln, sondern auch den benutzten Schlüssel zu rekonstruieren. Für weiteres musste nur der Klartext  $N$  mit dem Geheimtext  $Z$  exklusiv verodert werden:

$$Z \oplus N = S$$

Trotz des Erfolges waren sie noch weit davon entfernt die Lorenzmaschine zu entschlüsseln. Um nämlich regelmäßig Nachrichten mitlesen zu können, mussten die Codeknacker

es zuerst schaffen, den logischen Aufbau des Schlüssels zu verstehen.

Obwohl sie den Schlüssel hatten, konnten sie kein Muster



Figure 29: William Thomas „Bill“ Tutte [27]

bezüglich dessen Aufbaus erkennen. Im Oktober 1941 überreichten sie den Schlüssel an einen jungen Mathematiker namens Bill Tutte mit den Worten: „See what you can make of these“ (Schau mal, was du damit anstellen kannst) [Abbildung 29] [21]. Bill Tutte war gerade mal 24 Jahre alt und hatte sein Studium an der Cambrage University abgeschlossen als er diese Aufgabe bekam. Er erinnerte sich an den sog. „Kasiski-Test“, welchen sie im Studiums besprochen haben. Mit diesem Test kann man die Länge eines Schlüssels finden, falls er ein Muster aufweist, dass sich nach einer bestimmten Periode wiederholt.

Zu Beginn sucht man im verschlüsselten Text nach allen Buchstabenfolgen mit Mindestlänge von zwei, die sich wiederholen und notiert den Abstand zu der identischen Folgen. Der Abstand (entspricht der Anzahl der Buchstaben) zwischen dem ersten Buchstaben der einen Folge und dem ersten Buchstaben der anderen Folge wird notiert. Anschließend wird für alle Abstände eine Primfaktorzerlegung durchgeführt. Wenn man nun das Ergebnis gemeinsame Teiler besitzt, hat man die Länge des Schlüssels oder ein Vielfaches davon gefunden.

Tutte modifizierte den Test für seine Anwendung etwas, indem er von jedem Zeichen das jeweils erste Bit in ein Raster eintrug. „0“ stellte er mit einem Punkt dar und „1“ mit einem Kreuz. Falls die Zeilenlänge der Schlüssellänge entspricht, würde sich in den Spalten ein Muster ergeben. Bei seinen ersten Versuchen konnte er kein Muster erkennen. Als er aber die Zeilenlänge 41 wählte, bildeten sich in den Spalten Wiederholungen von Bits. Im Beispiel aus Grafik 30 kann man erkennen, dass sich Rechtecke aus Punkten und Kreuzen bilden [37]. Bill Tutte hatte mit seiner Methode die Länge des ersten Rades gefunden. Nachdem er bewiesen hatte, dass es möglich war den Aufbau der Räder zu rekonstruieren, wurden auch andere Codeknacker darauf aufmerksam

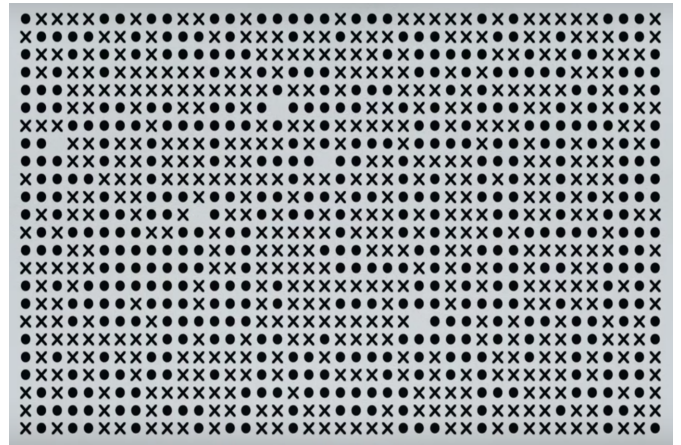


Figure 30: Tutes modifizierter Kashiki-Test für Rad A1 [26]

und gemeinsam erarbeiteten sie die restlichen Räder, ohne die eigentliche Maschine jemals gesehen zu haben. Dabei erkannte er, dass der Schlüssel aus zwei Schlüsseln bestand, wobei sich einer davon nicht regelmäßig änderte. Also stellte er die folgende Formel auf:

A ist der Wert der A Gruppe (Tutte nannte sie Chi-Wheels”), B der Wert der Gruppe C (eng. ”Psi-Wheels”) und S der resultierende Schlüssel

$$S = A \oplus C$$

Zusätzlich erstellte Tutte noch eine Skizze der Lorenzmaschine, in der er sogar die Funktion der Räder der B Gruppe (engl. ”Motorwheels”) darstellte [32].

Die letzte Frage, die noch zu beantworten war, um konstant die Nachrichten der Deutschen mitlesen zu können, ohne dabei auf depths angewiesen zu sein, war: Wie kann man die richtig Anfangsstellung der einzelnen Räder herausfinden, mit der Annahme, dass man bereits den Aufbau der Rotoren rekonstruiert hat?

Da sich die Anfangsstellung der Räder bei jeder Nachricht ändert und es insgesamt, wie bereits erwähnt,  $1,6 \cdot 10^{19}$  mögliche Startzustände gab, würde es mit einfachem Brute-Force selbst mit modernen Rechnern Jahre dauern.

Tutte erkannte, dass wenn man die Anfangsstellung der ersten beiden Räder findet, sich die restlichen Anfangsstellungen davon ableiten ließen. Desweiteren entwickelte er eine Methode, die die richtige Anfangsstellung der Rotoren A1 und A2 lieferte. Seine Methode beruhte auf einer statistischen Analyse des Aufbaues eines Geheimtextes [37]. Dabei stellte er für den i-ten Geheimbuchstaben die Formel:

$$Z_i = A_i \oplus C_i \oplus N_i$$

auf. Bildet man nun die Delta-Funktion des Geheimtextes, indem man zu jedem Zeichen das vorherige Zeichen aufaddiert, ergibt sich:

$$Z_i \oplus Z_{i+1} = (A_i \oplus A_{i+1}) \oplus (C_i \oplus C_{i+1}) \oplus (N_i \oplus N_{i+1})$$

Er erkannte, dass sich die Räder der C Gruppe nur bei ca jedem zweiten Zeichen bewegten und wenn sie sich bewegten nur zu etwa 50% von von einer 0 zu einer 1, bzw umgekehrt, änderten. Allgemein ließen sich diese Aussagen zusammenfassen, indem er bewies, dass zu 70% der Term  $C_i \oplus C_{i+1}$



eine 0 ergab. Das Addieren einer 0 wiederum beeinflusst das Ergebnis nicht, d.h zu 70% kann der Anteil der C Gruppe vernachlässigt werden. Desweiteren erkannte er, dass die Delta-Funktion des Orginaltext aus ungefähr 60% Nuller bestand. Diese Beobachtung lässt sich auf verschiedene Faktoren zurückzuführen, wie z. B. auf die deutsche Sprache, die bestimmte Zeichen wiederholte (BSP: "Schlüssel" das doppel s) oder auf die Wahl das Baudot-Codes, der für die ersten beiden Impulse von häufig vorkommenden Silben die gleiche Darstellung festlegt (BSP: "DE"). Bill Tutte veralgemeinerte seine Beobachtungen, indem er bewies, dass zu 55% die folgende Ungleichung gilt:

$$Z_i \oplus Z_{i+1} = A_i \oplus A_{i+1}$$

Er stellte anhand seiner Anaylse fest, dass die richtige Anfangsstellung diejenige ist, die die höchste Übereinstimmung mit dem Delta des Geheimtextes hat.

Tuttes Methode reduzierte die Anzahl der Vergleiche um die Startstellung der ersten beiden Räder zu finden auf ein Minimum von  $1271 \cdot \text{Länge der Nachricht}$ . Jedoch war seine Methode mit Stift und Papier in der Praxis noch nicht anwendbar, da man für eine 4000 Zeichen lange Nachricht bis zu 5084000 Vergleiche durchführen müsste. Als Bill Tutte Max H. A. Newman, einer der führenden Kryptologen sowie Pionier der elektronischen digitalen Datenverarbeitung, schüchtern von seiner Methode erzählte, erkannte Newman das Potential des Algorithmuses und schlug vor, die ganze Methodik zu automatisieren. Das war die Geburt des ersten Großrechners "Colossus".

## 4. COLOSSUS

### 4.1 Einführung

Bereits 1943 wurde "Heath Robinson", der Vorgänger des Colossus, von Max Newman konstruiert. Heath Robinson konnte mithilfe von Tuttes Methodik die Anfangsstellung der Räder A1 und A2 finden, indem die Maschine den Geheimtext mit allen möglichen Anfangsstellungen der ersten beiden Räder exklusiv-veroderte und zählte wie viele Punkte sich dabei ergaben. Dazu las die Maschine mit einer maximal Geschwindigkeit von 2000 Zeichen pro Sekunde die Einstellung der Räder und den Geheimtext ein und gab das Ergebnis der Startstellung als Lochkarte zurück. Mithilfe der Startstellung der ersten beiden Räder konnten Codeknacker dann per Hand die Startzustände der restlichen Räder berechnen. Es war nun möglich innerhalb von einer Woche ca. 3 Nachrichten zu entschlüsseln. Trotz der anfänglichen Erfolge war Heath Robinson sehr anfällig für Fehler, da er zwei Lochstreifen, die der verschlüsselten Nachricht und die der Räder, gleichzeitig einlesen musste, was ab einer Geschwindigkeit von 1000 Zeichen pro Sekunde zu Synchronisierungsproblemen führte. Da das britische Militär möglichst schnell und zuverlässig Nachrichten entschlüsseln wollte, musste eine Weiterentwicklung erfunden werden [4]. Im selben Jahr noch wurde eine Maschine namens "Colossus" von Tommy Flowers entworfen [Abbildung 31].



Figure 31: Thomas „Tommy“ Harold Flowers [14]

Colossus war eine schnellere und zuverlässigere Version des Heath Robinson. Anders als bei Robinson, verwendet dieser nämlich Takte um die einzelnen Schritte zu synchronisieren. Schon im Dezember 1943 wurde das erste Exemplar "Colossus Mark 1" gebaut und konnte ab Januar 1944 erste Erfolge erzielen. Im Gegensatz zu seinem Vorgänger konnten mit dieser bei einer Geschwindigkeit von 5000 Zeichen pro Sekunde bis zu 100 Nachrichten pro Woche entschlüsselt werden. Flowers optimierte diesen am 1 Juni 1944 nochmals, indem er Parallelverarbeitung nutzte, um im "Colossus Mark II" die Geschwindigkeit auf unglaubliche 25.000 Zeichen pro Sekunde zu steigern. Colossus gilt seitdem als erster großer Elektronenrechner [10].

### 4.2 Aufbau

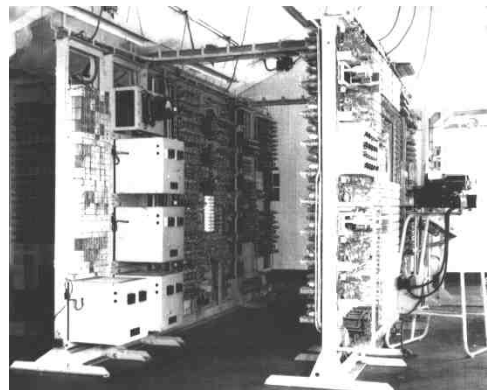


Figure 32: Colossus [8]

Colossus bestand aus acht Regalen, die jeweils 2,3 Meter hoch und unterschiedlich breit waren, und einem Lochstreifenleser [Abbildung 32]. Die wichtigsten Komponenten des Colossus waren [Abbildung 34] [8]:

- Master control panel: Dies war das Hauptbedienfeld. Nach dem Lesen eines "Start"- oder "Stop"-Befehls, setzte bzw. resetete es die Zähler und Zwischenspeicher und schrieb das Ergebnis.

- Lochstreifenleser: Die verschlüsselte Nachricht konnte mit einer Geschwindigkeit von bis zu 5000 Zeichen pro Sekunde eingelesen werden. Dazu musste zuerst die Darstellung des Textes im Baudot-Code auf eine Lochkarte gedruckt werden, bevor sie eingelesen werden konnte.
- Optical reader system: Dies war für das Lesen des Lochstreifens zuständig und ein Teil des Lochstreifenlesers. Sogenannte Fotozellen haben dabei optisch die Löcher auf dem Lochstreifen eingelesen
- Thyatron rings: bestanden aus gasgefüllten Elektronenröhren, die als 1 Bitspeicher dienten
- Shift registers: dienten als 5 bit Zwischenspeicher, die nach jedem Takt einmal ausgelesen wurden. Sie dienten vorallem zur Berechnung der Delta-Funktion
- Counter and counter control circuits: hier wurde die Anzahl an Übereinstimmungen der  $\Delta Z$  und  $\Delta C$  gezählt. Zusätzlich konnte hier auch eingestellt werden, das Ergebnisse erst ab einer bestimmten Anzahl von Übereinstimmungen ausgegeben wird.
- Span counters: falls ein Abschnitt einer Nachricht fehlerhaft war, beispielsweise wegen einer schlechten Übertragung, konnte man diesen mithilfe der Span counters überspringen. Dazu musste der jeweilige Bereich in den Zählern gesetzt werden.
- Relay buffer store and printer logic: hier wurde das Ergebnis gespeichert und nach Beendigung des Prozesses ausgegeben

Wie bereits erwähnt, beruhte die Colossus Funktion auf Tutes Beweis, dass bei richtiger Starteinstellung der Räder A1 und A2 die Delta-Funktion dieser eine 55% Übereinstimmung mit der Deltafunktion des Geheimtextes hatte. Um nun die Anfangsstellung der ersten beiden Räder zu finden, bildete Colossus für alle 1271 möglichen Startzustände die Deltafunktion der ersten beiden Räder und zählte an wie vielen Stellen diese mit der Deltafunktion übereinstimmte. Die richtige Anfangsstellung ist dann diejenige, die die höchste Übereinstimmung besitzt. Colossus Mark II konnte sogar zusätzlich die Startposition der restlichen Rotoren der A Gruppe und die der C Gruppe berechnen [35]. Dabei simulierten die Thyatrons die Räder. Dies bot den Vorteil, dass die Werte der A Gruppe nicht manuell eingelesen werden mussten und somit das Synchronisationsproblem umgangen werden konnte. Des Weitern nutze man eine große Anzahl an Elektronenröhren zur Verwirklichung der Boolean-Operation. Diese dienten vorallem zur Umsetzung der And- und OR-Gattern, da sich alle anderen notwendigen Gatter, wie z. B. XOR daraus ableiten ließen. Colossus I enthielt 1500 Elektronenröhren und Colossus II sogar 2500. Nach Beendigung der Berechnungen wurde das Ergebnis dann auf den "Relay buffer store" gespeichert und beim Einlesen der nächsten Werte als Lochstreifen ausgegeben [8].

### 4.3 Funktionsweise

Im Prinzip hatte der Colossus zwei Hauptabläufe von Operationen:

Der erste bestand darin, den Geheimtext als Lochstreifen

einzulesen. Hierbei war es wichtig, dass am Anfang des Streifens ein Startzeichen eingefügt wurde und am Ende ein Stopzeichen. Nachdem das Startzeichen eingelesen wurde, wurde sofort Tutes Methodik Zeichen für Zeichen ausgeführt und das Ergebnis zu den "Counter Circuits" weitergeleitet. Der erste Schritt musste getackt werden um so mögliche Synchronisationsproblemen zu vermeiden. Dazu wurden sogenannte "Sprocket Holes" [Abbildung 33] auf dem Lochstreifen der verschlüsselten Nachricht zwischen Spur zwei und drei gestanzt. Der Zweck der "Sprocket Holes" war, dass während des Lesens des Lochstreifens ein bestimmter Takt eingehalten wurde. In diesem Fall waren es 40 Mikrosekunden pro "Sprocket".

Der zweite Ablauf von Operationen fing an, nachdem ein "Stop"-Zeichen von den Fotozellen gelesen wurde. Nach dem "Stopp-Puls" wurde als erstes mithilfe von Schaltungen der Kontrollfluss des ersten Ablaufes unterbrochen, sodass die Lochstreifen nicht mehr eingelesen werden und das Endergebniss nicht mehr verändert wird. Des Weitern musste das Ergebnis der Berechnung von den Countern in die Relais zwischengespeichert werden. Nachdem dieser Wert gesichert wurde, mussten noch alle Zähler und Zwischenspeicher (Thyatronen) für den nächsten Durchlauf zurückgesetzt werden. Dieser Vorgang dauerte ungefähr 100 Millisekunden. Wenn nach Beendigung des ersten Ablaufes wieder ein "Start-Puls" von den Fotozellen gelesen wurde, wurde der Kontrollfluss wieder zurückgesetzt und der erste Ablauf wiederholt [8].

Dieser Ablauf wiederholte sich solange, bis man für alle Startzustände diesen Ablauf durchgeführt hatte und man einen Kandidaten gefunden hatte.

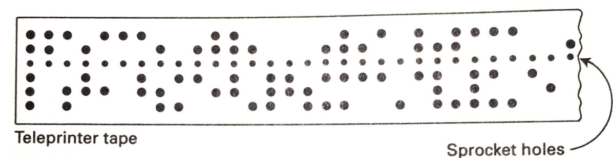


Figure 33: Lochstreifen mit eingestanzten "Sprocketholes" [17]

### 4.4 Folgen

Rechtzeitig zum "D-Day" am 6. Juni 1944 konnte Colossus II fertiggestellt werden. Der D-Day gilt als Anfang vom Ende des 2ten Weltkrieges, als 150000 amerikanische, kanadische und britische Soldaten im Morgengrauen des 6. Juni an der Küste von Frankreich ankamen [Abbildung 35]. Die Schlacht an der Westfront dauerte bis zum 12ten September 1944 bevor die Alliierten Truppen es schafften diese Schlacht für sich entscheiden zu können [43].

Einen entscheidenden Vorteil für die Alliierten bot Colossus. Colossus erlaubte einen Einblick in die strategische Planung der deutschen Befehlshaber und ermöglichte somit eine Gegenschlag vorzubereiten. Nach der Invasion in Frankreich wurden in Bletchley Park täglich über 10 Nachrichten entschlüsselt.

Nach Ende des Krieges jedoch wurde Colossus nicht mehr gebraucht und alle 10 Exemplare bis 1960 abgebaut. Heutzutage existiert noch ein Nachbau im National Museum of Computation in Bletchley Park [24].

## 5. FAZIT

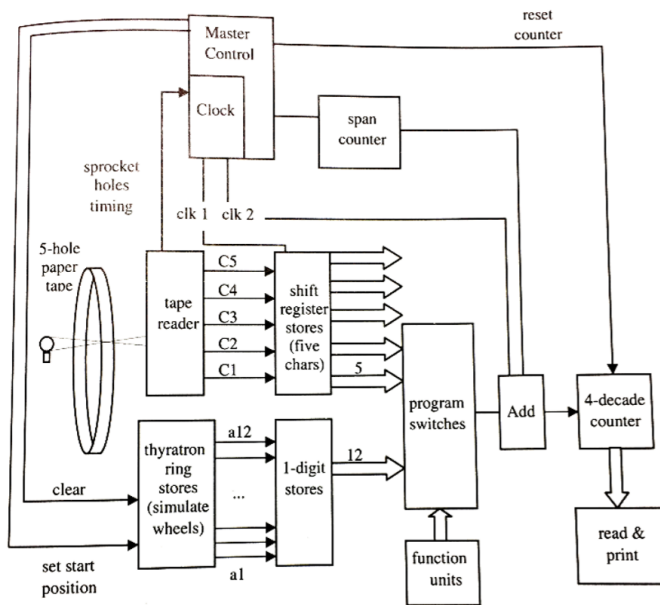


Figure 34: Aufbau des Colossus [32]



Figure 35: Beobachtungsposten am Atlantikwall [43]

Trotz unterschiedlicher Funktionsweisen haben Enigma und die Lorenzmaschine mehr Gemeinsamkeiten als man denkt. Beide wurden vom deutschen Militär als Verschlüsselungsmaschinen benutzt, beide konnten durch einen Anwendungsfehler deutscher Soldaten geknackt werden und auch beide besaßen eine solche Relevanz, dass Sir Harry Hinsley, ein offizieller Historiker des britischen Geheimdienstes im Zweiten Weltkrieg meinte, dass die Entschlüsselung der Krieg „um nicht weniger als zwei Jahre und wahrscheinlich um vier Jahre“ verkürzt hat [2].

Die Geschichte der beiden Maschinen sowie ihre Fehler bilden für die heutige Kryptografie eine wichtige Grundlagen in der Entwicklung moderner Verschlüsselungsverfahren. Anhand dieses Beispiels erkennt man, dass obwohl beide Maschinen aus heutiger Sicht veraltet scheinen, sie trotzdem noch eine gewisse Relevanz besitzen und Grundbausteine der modernen Kryptografie sind.

## 6. REFERENCES

[1] Alchetron. John tiltman.

- <https://alchetron.com/John-Tiltman>, 2018. Zuletzt eingesehen: 10.06.2019.
- [2] J. A. Anderson. *After Digital. Computation as Done by Brains and Machines*. Oxford University Press, Oxford, 2017.
- [3] F. L. Bauer. *Entzifferte Geheimnisse: Methode und Maximen der Kryptologie Zweite, erweiterte Auflage*. Springer-Verlag Berlin Heidelberg New York, Berlin, Deutschland, 1997.
- [4] F. L. Bauer. *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*. Springer, Berlin, 2000.
- [5] Bonhams. Enigma machine. markierung auf dem bild sind von mariia borysova gemacht. <https://www.bonhams.com/auctions/22795/lot/2/>.
- [6] E. by Ralph Erskine and M. Smith. *Action this Day*. Bantam Press, London, Great Britain, 2001.
- [7] R. Churchhouse. *Codes and ciphers: Julius Caesar, the Enigma, and the Internet*. Cambridge University Press, The Edinburgh Building, Cambridge, UK, 2002.
- [8] B. J. Copeland. Colossus: Breaking the german 'tunny' code at bletchley park. <http://www.codesandciphers.org.uk/lorenz/colossus.htm>. Zuletzt eingesehen: 10.06.2019.
- [9] L. Dade. How enigma machines work. <http://enigma.louisedade.co.uk/howitworks.html>, 2006.
- [10] A. David. Was the manchester baby conceived at bletchley park? [https://www.bcs.org/upload/pdf/ewic\\_tur04\\_paper3.pdf](https://www.bcs.org/upload/pdf/ewic_tur04_paper3.pdf), 2007. Zuletzt eingesehen: 10.06.2019.
- [11] O. T. Day. Winston churchill. <https://www.onthisday.com/people/winston-churchill>.
- [12] G. Ellsbury. The turing bombe - cribs and menus. markierung auf dem bild sind von mariia borysova gemacht. <http://www.ellsbury.com/bombe1.htm>.
- [13] G. Ellsbury. The turing bombe - cribs and menus. <http://www.ellsbury.com/bombe1.htm>, 1998.
- [14] T. H. Flowers. [https://de.wikipedia.org/wiki/Tommy\\_Flowers#/media/Datei:Tommy\\_Flowers.jpg](https://de.wikipedia.org/wiki/Tommy_Flowers#/media/Datei:Tommy_Flowers.jpg), 2013. Zuletzt eingesehen: 10.06.2019.
- [15] H. W. Franke. *Die geheime Nachricht: Methoden u. Technik d. Kryptologie; d. Geschichte um d. unknackbaren Code*. Umschau-Verlag, Frankfurt am Main, Deutschland, 1982.
- [16] Garrethe. Lorenz cipher machine. [https://de.wikipedia.org/wiki/Lorenz-Schl%C3%BCsselmaschine#/media/Datei:Lorenz\\_Cipher\\_Machine.jpg](https://de.wikipedia.org/wiki/Lorenz-Schl%C3%BCsselmaschine#/media/Datei:Lorenz_Cipher_Machine.jpg), 2007. Zuletzt eingesehen: 10.06.2019.
- [17] F. H. Hinsley. *Codebreakers. The inside story of Bletchley Park*. Oxford University Press, Oxford, 2001.
- [18] D. Kahn. *Seizing the enigma: the race to break the German U-Boat codes, 1939-1943*. Houghton Mifflin Company, Boston, USA, 1991.
- [19] D. Kahn. *The Codebreakers: The Story of Secret Writing*. Scribner, New York, USA, 1996.
- [20] W. Kozaczuk. *ENIGMA. How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two. Translated by Christopher Kasparek*. University Publications of America, USA, 1985.



- [21] C. Mathematics. <https://www.cambridgemaths.org/blogs/a-network-to-catch-a-fish-in/>. Zuletzt eingesehen: 10.06.2019.
- [22] C. Museum. Lorenz sz-40/42. <https://www.cryptomuseum.com/crypto/lorenz/sz40/index.htm>. Zuletzt eingesehen: 10.06.2019.
- [23] C. Museum. Enigma cipher machines. <https://www.cryptomuseum.com/crypto/enigma/index.htm>, 2009.
- [24] national museum of computing. Colossus decrypts to be revealed after 75 years. <https://www.tnmoc.org/news-releases/2019/2/5/colossus-decrypts-to-be-revealed-after-75-years>, 2019. Zuletzt eingesehen: 10.06.2019.
- [25] NSA. Alan turing. <https://www.nsa.gov/About-Us/Current-Leadership/Article-View/Article/1621551/alan-turing/>.
- [26] U. of Waterloo. [https://www.youtube.com/watch?time\\_continue=5&v=GBsfWSQVtYA](https://www.youtube.com/watch?time_continue=5&v=GBsfWSQVtYA), 2014. entnommen an der Stelle 7:27 und zuletzt eingesehen: 10.06.2019.
- [27] U. of Waterloo. <https://uwaterloo.ca/math/news/undergraduate-scholarship-honouring-professor-william-tutte>, 2017. Zuletzt eingesehen: 10.06.2019.
- [28] OS. Spring-cäsar-räder (nr. 3 und 4) des lorenz-schlüssel-zusatzes. [https://de.wikipedia.org/wiki/Lorenz-Schl%C3%BCsselmaschine#/media/Datei:Lorenz\\_machine\\_Psi\\_wheels\\_3\\_and\\_4.jpg](https://de.wikipedia.org/wiki/Lorenz-Schl%C3%BCsselmaschine#/media/Datei:Lorenz_machine_Psi_wheels_3_and_4.jpg), 2017. Zuletzt eingesehen: 10.06.2019.
- [29] D.-I. M. Präse. *Chiffriermaschinen und Entzifferungsgeräte im Zweiten Weltkrieg: Technikgeschichte und informatikhistorische Aspekte*. PhD thesis, Technische Universität Chemnitz, 2004.
- [30] J. A. Reeds. *Breaking Teleprinter Ciphers at Bletchley Park*. Wiley-IEEE Press, New Jersey, 2015.
- [31] D. Rijmenants. Technical details of the enigma machine. <http://users.telenet.be/d.rijmenants/en/enigmattech.htm>, 2004.
- [32] U. H. R. Rojas. *The First Computers History and Architectures*. Massachusetts Institute of Technology, Massachusetts, 2000.
- [33] T. Sale. The colossus. <http://www.rutherfordjournal.org/article030109.html#section07>, 2009. Zuletzt eingesehen: 10.06.2019.
- [34] T. C. Sanger. The evolution of enigma. <http://thomascsanger.com/tag/arthur-scherbius/>, 2018.
- [35] singingbanana. Lorenz: Hitler's unbreakablecipher machine. <https://www.youtube.com/watch?v=GBsfWSQVtYA>. Zuletzt eingesehen: 10.06.2019.
- [36] A. M. Society. The polish attack on enigma ii: Zygalski sheets. <http://www.ams.org/publicoutreach/feature-column/fc-2013-12>.
- [37] W. T. Tutte. Fish and i. <https://www.ee.iitb.ac.in/~hn/matroids-evolving-notes/tutte.pdf>. Zuletzt eingesehen: 10.06.2019.
- [38] VirtualColossus.co.uk. The lorenz machine. <https://lorenz.virtualcolossus.co.uk/lorenz.html>. Zuletzt eingesehen: 10.06.2019.
- [39] Virtualcolossus.co.uk. The first break. <https://www.virtualcolossus.co.uk/firstbreak.html>, 2009. Zuletzt eingesehen: 10.06.2019.
- [40] G. Welchman. *The Hut Six Story. Breaking the Enigma Codes*. M M Baldwin, Kidderminster, UK, 1998.
- [41] Wikipedia. Bombe. <https://en.wikipedia.org/wiki/Bombe>.
- [42] Wikipedia. Gordon welchman. [https://en.wikipedia.org/wiki/Gordon\\_Welchman](https://en.wikipedia.org/wiki/Gordon_Welchman).
- [43] wissen.de. D-day: Der 6. juni 1944. <https://www.wissen.de/d-day-der-6-juni-1944>. Zuletzt eingesehen: 10.06.2019.