Seminarvortrag

über die Enigma

ein Vortrag von

Björn Mross

13. Juni 2002

im
Institut für „Theoretische Informatik“
TU Braunschweig

Mit einem herzlichen
Dankeschön
an
Prof. Dr. Michael Miller
für
die Bereitstellung
seiner
Kryptoanalyse der Enigma
aus seinem
unveröffentlichtem Buch

1. Die Entwicklung

Die ältesten kommerziellen Enigma-Modelle (Enigma – griech. Geheimnis, Rätsel) kamen Anfang der 20er Jahre auf den Markt und hatten das Aussehen einer Schreibmaschine. Sie ermöglichen es, Klartexte zu chiffrieren und Kryptogramme zu dechiffrieren. Einige Modelle können auch als gewöhnliche Schreibmaschinen zur Niederschrift irgendeiner Mitteilung in Klarschrift verwendet werden.

Das „Enigma A"-Modell kann mit einem an der Maschine angebrachten Hebel jederzeit von „Klarschrift" auf „Geheimschrift" umgeschaltet werden. Ein rotierendes Typenrad druckt den Klartext bzw. den Chiffretext direkt auf Papier. Beim Chiffrieren wird der Geheimtext automatisch in Gruppen von je fünf Buchstaben zerlegt, und je zehn Gruppen in eine Zeile geschrieben, so dass in jeder Zeile genau 50 Chiffrebuchstaben stehen. Das Chiffrat besteht dabei nur aus den 26 Buchstaben des internationalen Telegrafenalphabetes, während das Dechiffrat wieder alle Buchstaben, Ziffern, Zeichen und Zwischenräume des Klartextes enthält, wie ein gewöhnlicher Schreibmaschinentext. Die Enigma A wurde 1924 anlässlich des Weltkongresses in Stockholm vorgeführt.
Die praktischen Vorteile der Enigma A und Überlegungen zur Sicherheit der Enigma-Kryptogramme sind von dem deutschen Ingenieur Dr. Arthur Scheribus (erfand die grundlegende Funktionsweise der Enigma) in Fachzeitschriften über Elektrotechnik und Radiotelegrafie veröffentlicht worden.

Beim „Enigma B"-Modell wurde das langsame Typenrad modifiziert, da die Geschwindigkeit der Typenradmechanik für den Fernmeldedienst nicht ausreichte. Der Chiffriermechanismus ist nicht verändert worden.

Das „Enigma C"-Modell, ausgerüstet mit einer Trockenbatterie von 4 Volt Spannung, ist erheblich kleiner und leichter als die Modelle A und B. Allerdings verfügte dieses Modell nicht über eine Schreibvorrichtung. Stattdessen zeigt eine von 26 Glühlampen durch Aufblitzen an, welcher Chiffretextbuchstabe zu notieren ist, wenn eine der 26 Tasten gedrückt wird. Aber auch der Chiffriermechanismus unterscheidet sich wesentlich von dem der Modelle A und B. Erstmals wurde eine sogenannte „Umkehrwalze" eingebaut, wie sie auch in der Wehrmachtsenigma vorzufinden ist.

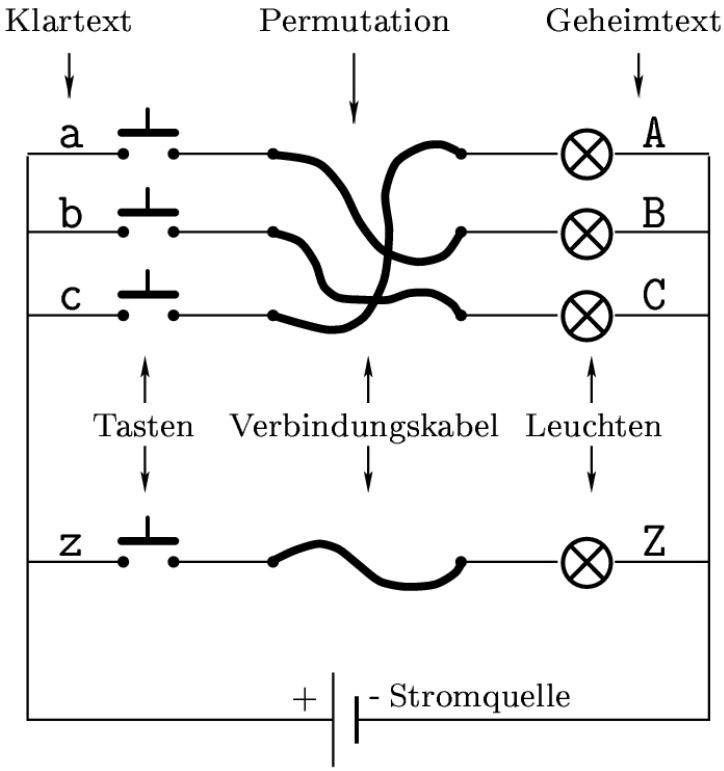
Später wurde noch eine „Enigma D" produziert, die sich von Modell C im Wesentlichen nur dadurch unterscheidet, dass die Umkehrwalze in 26 verschiedenen Stellungen montiert werden kann.

Für militärische Zwecke (ab 1926) wurde das Modell „Enigma I" (eins) (auch „Wehrmachtsenigma" genannt) hergestellt. Dieses Modell basiert auf der Enigma C und unterscheidet sich hauptsächlich durch ein sogenanntes Steckerbrett, mit dem eine zusätzliche Vertauschung der Buchstaben beim Chiffrieren eingestellt werden kann.

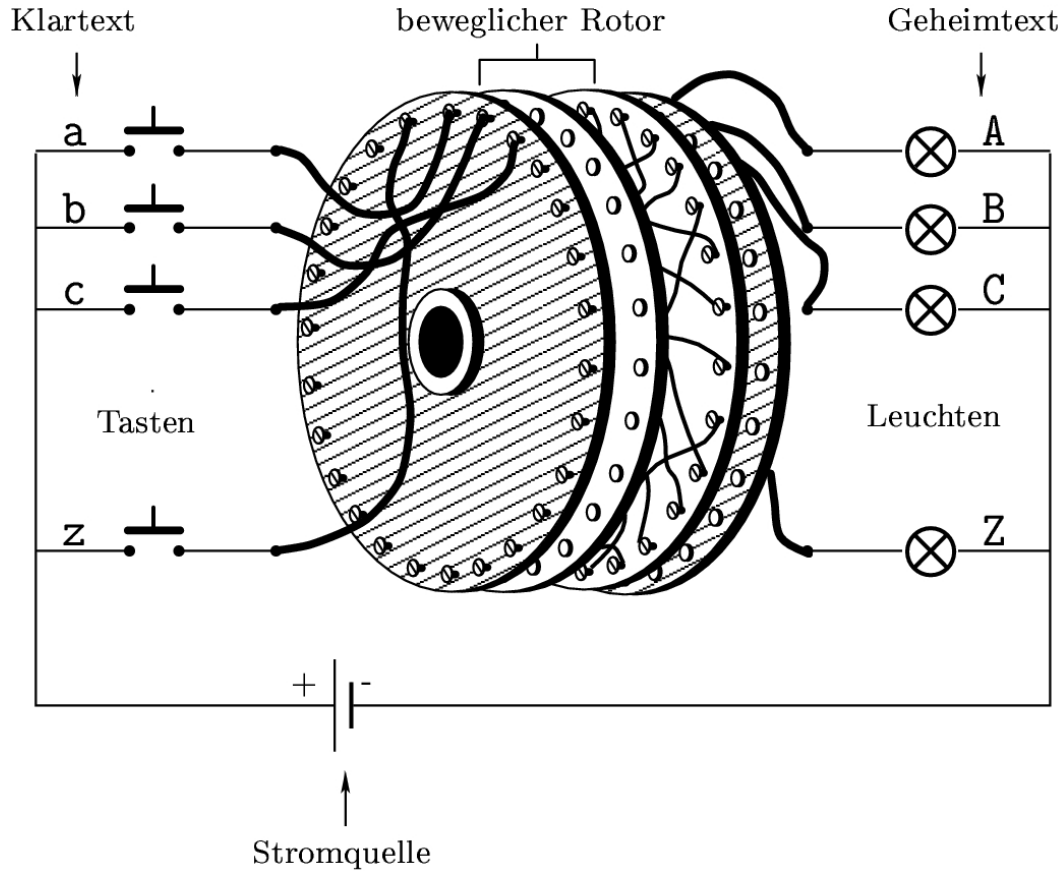
2. Funktionsweise der Enigma

2.1 Rotorchiffrierung

Die Permutation der Buchstaben des Alphabets ist eine sehr naheliegende Art der Chiffrierung und lässt sich mit einer einfachen elektrischen Schaltung, wie sie in folgender Abbildung dargestellt ist, realisieren.

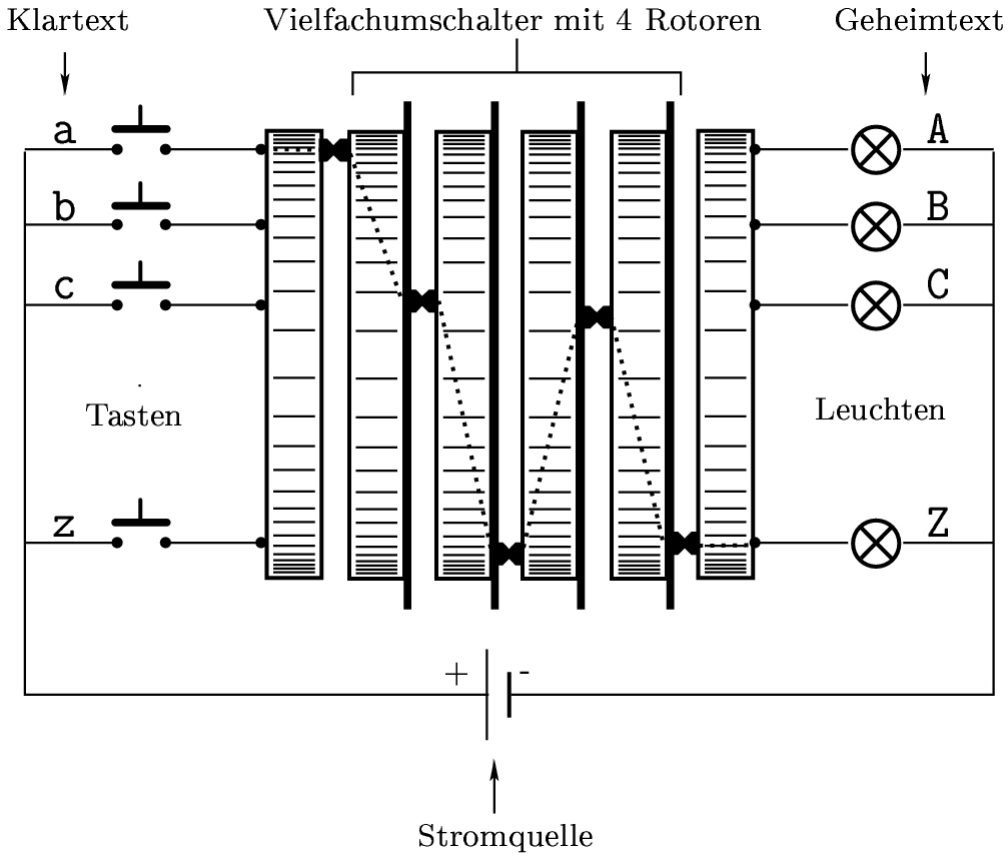


Auf der linken Seite sieht man 26 Tasten, die mit den Buchstaben a, ..., z gekennzeichnet sind, rechts, 26 Leuchten, die mit den Buchstaben A, ..., Z beschriftet sind.
Will man nun eine geheime Nachricht chiffrieren, so geschieht dies, Buchstabe für Buchstabe, indem man die entsprechende Taste für den Klartextbuchstaben drückt. Den dazugehörigen Geheimtextbuchstaben erkennt man am Aufblitzen der entsprechenden Leuchte. Bei der Schaltung in obiger Abbildung würde das Drücken der Taste „c“ zum Aufleuchten der Lampe „A“ führen. Jedoch sollte jedem klar sein, dass diese Art der Chiffrierung leicht zu brechen ist.
Grundlage der Rotorchiffrierung ist es, die unveränderliche Permutation des Alphabets (realisiert mit den Verbindungskabeln) durch eine mechanische Apparatur zu ersetzen, so dass die Verbindungen zwischen Klartext (Schalter) und Geheimtext (Leuchten) nach jedem Buchstaben, der chiffriert wurde, verändert wird. Die Idee, solch eine Mechanik mit sogenannten „Rotoren“ zu realisieren, hat Anfang des zwanzigsten Jahrhunderts zu einer neuen Generation von Chiffriermaschinen geführt.
In folgender Abbildung ist eine einfache Rotor-Chiffriermaschine skizziert.



Die 26 Kontakte, die mit den einzelnen Tasten verbunden werden, sind hier kreisförmig angeordnet. Gegenüberliegend sind, ebenfalls kreisförmig, 26 Kontakte montiert, die mit den Leuchten verbunden sind. Zwischen den Kontakten befindet sich der sog. Rotor, er ist drehbar gelagert und kann 26 verschiedenen Positionen einnehmen. Die Kontakte auf der linken Seite des Rotors sind gemäß einer festen Permutation mit den Kontakten auf der rechten Seite des Rotors verbunden. Eine hier nicht dargestellte Mechanik sorgt dafür, dass der Rotor nach jedem Tastendruck um eine Position weitergedreht wird.

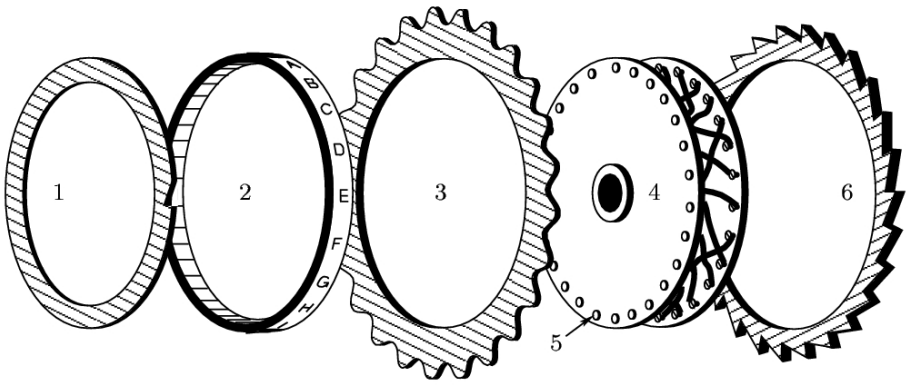
Auch die Kryptogramme dieser einfachen Rotormaschine können mit primitiven Mitteln dechiffriert werden, denn es handelt sich um eine polyalphabetische Chiffre, deren Kryptoanalyse bereits in der Vorlesung behandelt wurde. Um die Sicherheit der Rotorchiffren zu verbessern, hat man Maschinen mit mehreren hintereinandergeschalteten Rotoren gebaut. Bei den meisten Rotor-Chiffriermaschinen (auch bei der Enigma) sind die Rotoren nebeneinander auf einer Achse montiert, und ihre Stellungen werden von einer aufwendigen Mechanik nach jedem Chiffrierschritt verändert. Die folgende Abbildung zeigt die elektrische Schaltung des ersten Enigma Modells.

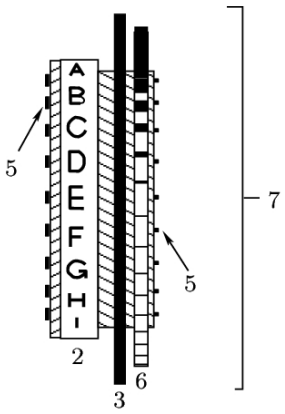


Diese Enigma hat vier Rotoren, die jeweils 26 Positionen einnehmen können. Insgesamt gibt es dann $26 \cdot 26 \cdot 26 \cdot 26 = 456.976$ verschiedene Rotorpositionen, womit die Kryptoanalyse einer solchen Maschine deutlich erschwert wird.
Zum Dechiffrieren eines Kryptogramms kann prinzipiell die gleiche Maschine verwendet werden wie zum Chiffrieren einer Nachricht, wenn man die Leuchten durch Tasten ersetzt und umgekehrt.

2.2 Die Wehrmachstenigma

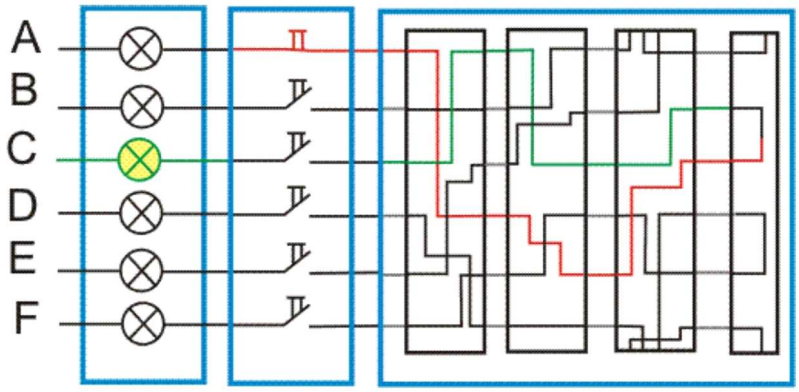
Die Walzen (siehe folgende Abbildung) der Wehrmachtsenigma sind wie oben erwähnt auf einer gemeinsamen Achse montiert und es handelte sich in der Anfangsphase um drei Walzen, welche sich ähnlich wie die Ziffernräder eines mechanischen Kilometerzählers bewegten.





1 Mechanik zum Fortschalten der Walzen
2 Alphabetring
3 Handrad
4 Rotor
5 Kontakte
6 Mechanik zum Fortschalten der Walzen
7 Enigma-Walze

Nach jedem Verschlüsselungsschritt (1 Buchstabe) wird die rechte Walze automatisch um einen Schritt weitergeschaltet. Jedes Mal, wenn diese „schnelle“ Walze eine Umdrehung zurückgelegt hat, sorgt eine einfache Mechanik dafür, dass die mittlere Walze um eine Position weitergedreht wird. Nach jeder Umdrehung der mittleren Walze wird die linke „langsame“ Walze um eine Position verschoben. Die Umkehrwalze (Reflektor) ist nicht beweglich. Damit ergibt sich eine Zykluslänge von $26 \cdot 26 \cdot 26 = 17576$.
Der Reflektor sorgt dafür, dass der Strompfad den Satz der beweglichen Walzen zweifach durchläuft. Siehe folgende Abbildung.



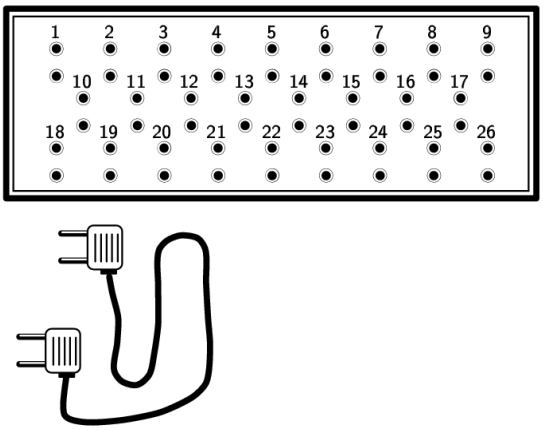
Die Konstruktion hat den praktischen Vorteil, dass die Maschine zum Dechiffrieren in der gleichen Konfiguration wie zum Chiffrieren verwendet werden kann. Eine weitere Folge dieser Konstruktion ist, dass die Substitutionen der Enigma echt involutorisch sind. Dies hat sich später jedoch als die entscheidende Schwachstelle herausgestellt und letztlich die erfolgreiche Kryptoanalyse durch die Polen und Engländer ermöglicht.
Das Außergewöhnliche der Enigma-Walze ist der Alphabetring. Ein Ring, der um den eigentlichen Rotor angebracht und mit den 26 Buchstaben A, ..., Z des Alphabets beschriftet

ist (auch Zahlen 1, 2, …, 26 waren üblich). Dieser Ring ist beweglich montiert, so dass er gegenüber dem eigentlichen Rotor verstellbar ist. Von der Stellung des Rings hängt ab, in welcher Position die nachfolgende Walze weitergeschaltet wird. Ein kleines Beispiel:

- Gehen wir davon aus das sich Zahlen auf dem Ring befinden und die Position 5 auf der ganz rechten (schnellen) Walze eingestellt wurde. Nun würde sich die nächste (mittlere) Walze nach der Eingabe von genau 5 Buchstaben um eine Position weiterdrehen. Daraufhin wären weitere 26 Eingaben nötig, um wieder ein weiterschalten der mittleren Walze auszulösen.
  Analog hierzu: mittlere Walze $\longrightarrow$ langsame Walze
  Der Ring der letzten langsamen Walze hat keine Auswirkung.

Die drei Walzen der Enigma sind leicht austauschbar und können in beliebiger Reihenfolge montiert werden. Um die kryptographische Sicherheit der Maschine zu erhöhen, wurden im Dezember 1938 zwei zusätzliche Walzen eingeführt, so dass für jedes Gerät insgesamt 5 unterschiedliche Walzen vorhanden waren, von denen man drei in beliebiger Reihenfolge montieren konnte.

Ein wesentlicher Unterschied zwischen den militärischen und kommerziellen Enigma-Modellen ist das sogenannte „Steckerbrett“, das eine zusätzliche Permutation der Buchstaben erlaubt. Diese Permutation wird mit losen Kabeln gesteckt (wankte zwischen 6 und 10). Die Zahlen in der folgenden Abbildung stehen für die Position der Buchstaben im Alphabet.



Die Wehrmachtsenigma wurde ausschließlich den Kommandostellen des Heeres bereitgestellt. Unterlagen über die Konstruktion und Funktionsweise der Maschine waren streng geheim. Denn wie erwähnt sind für das Chiffrieren und das Dechiffrieren eines Kryptogramms die gleichen Einstellungen an der Maschine nötig.

3. Sicherheit

3.1 Schlüsselraum

Das Hauptkriterium für die Sicherheit war natürlich der Schlüsselraum, also die Anzahl der möglichen Einstellungen der Maschine.
Folgende Einstellungen der Enigma waren möglich:

- Auswahl, Anordnung und Ausgangsstellung der Rotoren.
  Beim praktischen Einsatz gab es insgesamt 5 verschiedene Rotoren zur Auswahl, von denen man sich 3 aussuchte. Diese konnte man in beliebiger Reihenfolge auf der Achse anordnen und in beliebige Ausgangsstellung bringen.

  $5 \cdot 4 \cdot 3 = 60$ Auswahl und Position der 3 Walzen.

  26^3 = 17.576 verschiedene Ausgangsstellungen der 3 Rotoren.

  $26^3 \cdot 60 = 1.054.560$ mögliche Schlüssel.

- Steckfeldkombinationen:
  Es konnten, z.B. 6 Buchstaben, auf dem Steckfeld nach Belieben substituiert werden.

  Das ergab enorme Auswahlmöglichkeiten:
  $$\frac{26!}{2^6 \cdot 6! \cdot 14!} = 100.391.791.500$$

  26! Dies ist die gesamt mögliche Steckauswahl von den 26 Buchstaben auf dem Steckerfeld.

  Allerdings gibt es Einschränkungen, die folgend erläutert werden:

  2^6 steht für die Möglichkeiten die Buchstaben untereinander zu vertauschen, z.B. A-B, B-A. Dies ist aber nicht möglich, bzw. schon vorhanden, weil das Stecken zweier Buchstaben einen Zyklus bildet.
  Für zwei Elemente gibt es genau 1 Bit (0,1) Möglichkeiten. Somit gibt es für x Paare $xBits = 2^x$ Möglichkeiten.

  6! Bezieht sich auch hier auf die Buchstabenpaare und könnte wie oben für den allgemeinen Fall als x bezeichnet werden. Diese Zahl steht für die Möglichkeit die Paare untereinander zu tauschen: $\begin{matrix} A-B \\ C-D \end{matrix} \longrightarrow \begin{matrix} C-D \\ A-B \end{matrix}$ Das macht auf dem Steckbrett aber keinen Unterschied und wird in dem Aspekt der Sicherheit nicht mit einbezogen.

  14! Es wird Anfangs von 26 Buchstabensubsitutionen ausgegangen und daher 26! Möglichkeiten angenommen. Nun werden aber nur 6 Paare bzw. 12 Buchstaben substituiert und die restlichen bilden weiterhin auf sich selber ab. Die übrigen 14 Buchstaben schränken die Auswahl an Möglichkeiten also um genau 14! ein.

Diese beiden Schlüsselmengen ergeben den gesamten Schlüsselraum, welcher gigantische 105.869.167.644.240.000 Möglichkeiten (über 105 Billiarden) bietet.

Aufgrund dieser riesigen Zahl wurde die Enigma von den Deutschen als sehr sicher eingestuft. Man rechnete mit 14.000 Jahren, die der Feind brauchen würde, um sie zu knacken.

3.2 Geheimhaltung des Schlüssels

Die Geheimhaltung der Schlüssel ist bei vielen Anwendungen der Kryptographie der schwächste Punkt. Auch bei der militärischen Verwendung der Enigma war dies ein großes Problem. Zehntausende von Enigma Maschinen waren über das ganze Land verteilt, und alle mussten mit einem bestimmten Schlüssel versorgt werden. Um sich vor Verrat der Schlüssel durch Überläufer zu schützen, war es notwendig, die Schlüssel regelmäßig und in möglichst kurzen Abständen zu ändern. Das alles musste geheim geschehen, um dem Feind keine Chance zu bieten, die Schlüssel auszuspionieren.

Für jeden Tag gab es eine neue Grundeinstellung der Maschine, die allen Chiffrierern bekannt war (es gab Codebücher, die Tagesschlüssel für einen Monat enthielten). Dieser „Tagesschlüssel“ bestand aus den Positionen der Walzen, der Ringstellung jeder Walze und einer Grundstellung der 3 Walzen. Die Steckerbretteinstellung kam ab ungefähr 1939 zum Tagesschlüssel hinzu.
Damit nicht alle Funksprüche eines Tages mit dem gleichen Schlüssel chiffriert wurden, musste der Absender eines Funkspruchs einen zufälligen „Spruchschlüssel“ wählen. Dieser Spruchschlüssel bestand aus drei Buchstaben, die die Anfangsstellung der Walzen für den folgenden Funkspruch beschrieben. Wegen des störanfälligen Funkverkehrs wurde der Spruchschlüssel verdoppelt. Die resultierenden sechs Buchstaben wurden dann mit dem Tagesschlüssel chiffriert und vor der eigentlichen Nachricht gesendet. Da der Spruchschlüssel vor der Verschlüsselung verdoppelt wurde, war dem Kryptogramm nicht unmittelbar anzusehen, dass zwei Mal die gleichen drei Buchstaben gesendet wurden.

Ein Beispiel um die Bedienung der Enigma zu verdeutlichen:

- Die Walzen wurden anhand des Tagesschlüssels ausgewählt, eingesetzt, und dann auf der Achse in richtiger Reihenfolge montiert. Auf dem Steckerbrett wurden die jeweiligen Buchstaben vertauscht. Der Chiffreur dachte sich nun einen beliebigen Spruchschlüssel aus (z.B. IFX), worauf er später die Rotoren einstellte. Wie oben erwähnt wurde dieser zur Sicherheit zwei Mal hintereinander übertragen (im Bsp. IFXIFX). Nun wurde dieser „doppelte“ Schlüssel mit der Einstellung des Tagesschlüssels chiffriert (als Resultat z.B. RAGXIP). Daraufhin wurde die Enigma auf den Spruchschlüssel eingestellt und die eigentliche Nachricht (z.B. TEST) chiffriert (als Resultat z.B. LIRQ). So wäre in diesem Beispiel die gesendete Nachricht „RAGXIPLIRQ“.

- Zur Dechiffrierung war die Vorgehensweise praktisch gleich. Zuerst Walzen und Steckbrett nach Tagesschlüssel einstellen, dann den Spruchschlüssel ermitteln, indem man die ersten sechs Buchstaben der Nachricht, bei Tagesschlüssel-Stellung, dechiffriert. Nun mussten die Walzen in IFX-Stellung gebracht werden und der Rest der Nachricht konnte entschlüsselt werden.

Aufgrund von Spionage und mathematischen Analysen, die auf der Verdoppelung des Spruchschlüssels basierten, gelang es den polnischen Kryptoanalytikern die Enigma-Kryptogramme zu entschlüsseln und die meisten Funksprüche zu dechiffrieren. Vermutlich ist dies dem deutschen Geheimdienst bekannt geworden, denn das Schlüsselverfahren wurde entsprechend geändert. Seit dem 15. September 1938 bestand der Tagesschlüssel nur noch aus den Walzenpositionen und der Ringstellung. Die Grundstellung der Walzen wurde vom Absender für jeden Funkspruch willkürlich festgelegt und dem Empfänger im Klartext übertragen. Anschließend folgte der verdoppelte und mit der Grundstellung chiffrierte Spruchschlüssel. Am 15. Dezember 1938 wurde die vierte und fünfte Walze ein-

geführt. Ab Kriegsbeginn änderte sich die Ausgangslage der Walzen alle 8 Stunden.
Das neue Schlüsselverfahren erscheint auf den ersten Blick unverständlich, da die Grundstellung der Walzen nun im Klartext übertragen wurde. Dennoch konnten die polnischen Analysen auf diese Art unterbunden werden (siehe Kryptoanalyse).
Am 1. Mai 1940, kurz vor Beginn des Feldzuges in Frankreich, wurde das Schlüsselverfahren erneut geändert, indem die Verdoppelung des Spruchschlüssels aufgehoben wurde.

4. Kryptoanalyse

4.1 Analyse der Spruchschlüssel

Die Polen waren die Ersten, die die Bedeutung der Enigma für die deutsche Seite erkannten. Schon 1928, kurz nachdem das deutsche Heer mit Enigmas ausgestattet war, beschloss man eine Abteilung zur Kryptoanalyse aufzubauen. Die polnischen Mathematiker (hauptsächlich Marian Rejewski) waren gut auf ihre Aufgabe vorbereitet (sie wurden im Studium zusätzlich in Kryptologie ausgebildet), so kannten sie auch den von Friedmann 1925 eingeführten Begriff der Zeichenkoinzidenz. Zur Erinnerung: Der Koinzidenzindex gibt die relative Häufigkeit dafür an, dass zwei zufällig gewählte Buchstaben aus einer Menge gleich sind.

Bei den Analysen der deutschen Kryptogramme fiel ihnen auf, dass bei Funksprüchen, die mit den gleichen sechs Buchstaben begannen, eine deutlich erhöhte Zeichenkoinzidenz auftrat. Das war ein deutliches Zeichen dafür, dass diese Texte mit dem gleichen Schlüssel chiffriert wurden. Es lag also nahe anzunehmen, dass die ersten sechs Zeichen etwas mit dem Schlüssel zu tun hatten. Man hatte festgestellt (bis zu den ersten Erfolgen vergingen 4 Jahre), dass es sich um einen Spruchschlüssel handelte, der mit der gleichen Tageseinstellung zweifach in chiffrierter Form gesendet wurde. Dieses Wissen konnte man in folgender Form nutzen:

Seien $P_1, P_2, ..., P_6$ die Permutationen des 26-Buchstabenalphabets Σ, die bei den ersten sechs Chiffrierschritten von der Wehrmachtsenigma ausgeführt werden. Aufgrund der Konstruktion des Walzensatzes bzw. das Vorhandensein des Reflektors sind diese Permutationen involutorisch, sie erfüllen also die folgenden Eigenschaften:

$$aP_i \neq a \text{ und}$$
$$aP_i = x \Leftrightarrow xP_i = a \qquad \text{wobei } a, x \in \Sigma = \{A, B, ..., Z\} \text{ und } P_i \in \{P_1, ..., P_6\} \text{ sind.}$$

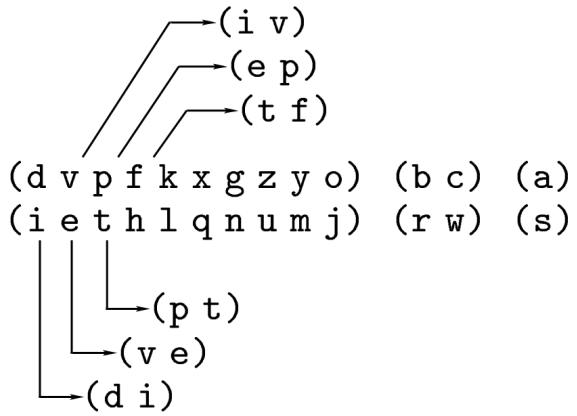
Sei nun $aP_i = x$ und $aP_{i+3} = y$, dann folgt, dass $xP_iP_{i+3} = y$ für $i \in \{1,2,3\}$ ist.

1. AUQ AMN	14. IND JHU	27. PVJ FEG	40. SJM SPO	53. WTM RAO
2. BNH CHL	15. JWF MIC	28. QGA LYB	41. SJM SPO	54. WTM RAO
3. BCT CGJ	16. JWF MIC	29. QGA LYB	42. SJM SPO	55. WTM RAO
4. CIK BZT	17. KHB XJV	30. RJL WPX	43. SUG SMF	56. WKI RKK
5. DDB VDV	18. KHB XJV	31. RJL WPX	44. SUG SMF	57. XRS GNM
6. EJP IPS	19. LDR HDE	32. RJL WPX	45. TMN EBY	58. XRS GNM
7. FBR KLE	20. LDR HDE	33. RJL WPX	46. TMN EBY	59. XOI GUK
8. GPB ZSV	21. MAW UXP	34. RFC WQQ	47. TAA EXB	60. XYW GCP
9. HNO THD	22. MAW UXP	35. SYX SCW	48. USE NWH	61. YPC OSQ
10. HNO THD	23. NXD QTU	36. SYX SCW	49. VII POH	62. YPC OSQ
11. HXV TTI	24. NXD QTU	37. SYX SCW	50. VII POH	63. ZZY YRA
12. IKG JKF	25. NLU QFZ	38. SYX SCW	51. VII POH	64. ZEF YOC
13. IKG JKF	26. OBU DLZ	39. SYX SCW	52. VQZ PVR	65. ZSJ YWG

Die Tabelle zeigt die ersten sechs Buchstaben zu verschiedenen Funksprüchen, die mit der gleichen Tageseinstellung gesendet wurden. Wenn nun für jede Permutationen P_1P_4, P_2P_5 und P_3P_6 die Verknüpfungen der einzelnen Buchstaben herausgeschrieben werden (z.B. b-c-b), bilden sich unterschiedlich lange Zyklen. In Zyklenschreibweise haben sie die folgende Form:

$P_1P_4 = (a)(s)(bc)(rw)(dvpfkxgzyo)(eijmunqlht)$,
$P_2P_5 = (axt)(blfqvcoum)(cgy)(d)(hjpswizrn)(k)$ und
$P_3P_6 = (abviktjgfcqny)(duzrehlxwpsmo)$.

Es ist nun zu ermitteln, wie die Permutationen $P_1, P_2, ..., P_6$ im Einzelnen aussehen. Im Beispiel fällt auf, dass Zyklen gleicher Länge in den P_iP_{i+3} jeweils paarweise auftreten. Das ist kein Zufall, sondern folgt aus der Tatsache, dass der Alphabetumfang $|\Sigma| = 26$ gerade ist (die beiden gleichlangen Zyklen stehen in Verbindung zu einander, näheres folgt noch). Man schreibt nun die Zyklen dieser Paare jeweils untereinander, wobei die Buchstaben des unteren Zyklus in umgekehrter Reihenfolge notiert werden. Ein Satz aus der Gruppentheorie besagt, dass die Transpositionen von P_i senkrecht und die von P_{i+3} diagonal abzulesen sind, wenn die Zyklen, mit dem richtigen Buchstaben beginnend, aufgeschrieben wurden. Die Abbildung veranschaulicht diese Vorgehensweise für P_1P_4.



Es bleibt noch die Beantwortung der Frage, mit welchem Buchstaben beginnend, die einzelnen Zyklen untereinander zu schreiben sind.
Falls man den Tagesschlüssel (Position, Ringstellung und Grundstellung der Walzen) und die Verdrahtungen der Walzen (Permutationen) kennt (für September und Oktober 1932 war der Tagesschlüssel durch Spionage des französischen Geheimdienstes bekannt), kann man alle Möglichkeiten durchspielen und die so gewonnenen Spruchschlüssel ausprobieren, indem man die aufgefangenen Nachrichten dechiffriert. Falls ein sinnvoller Text dabei herauskommt, war die Wahl gut.
Aber auch ohne die Tagesschlüssel gab es noch Hoffnung. Man hatte nämlich herausgefunden, dass die deutschen Chiffrierer sehr einfallslos bei der Wahl der Spruchschlüssel waren. Folgende Tabelle zeigt die dechiffrierten Spruchschlüssel eines Tages.

AUQ AMN → sss	IKG JKF → ddd	QGA LYB → xxx	VQZ PVR → ert
BNH CHL → rfv	IND JHU → dfg	RJL WPX → bbb	WTM RAO → ccc
BCT CGJ → rtz	JWF MIC → ooo	RFC WQQ → bnm	WKI RKK → cde
CIK BZT → wer	KHB XJV → lll	SYX SCW → aaa	XRS GNM → qqq
DDB VDV → ikl	LDR HDE → kkk	SJM SPO → abc	XOI GUK → qwe
EJP IPS → vbn	MAW UXP → yyy	SUG SMF → asd	XYW GCP → qay
FBR KLE → hjk	NXD QTU → ggg	TMN EBY → ppp	YPC OSQ → mmm
GPB ZSV → nml	NLU QFZ → ghj	TAA EXB → pyx	ZZY YRA → uvw
HNO THD → fff	OBU DLZ → jjj	USE NWH → zui	ZEF YOC → uio
HXV TTI → fgh	PVJ FEG → tzu	VII POH → eee	ZSJ YWG → uuu

Die Kombination SYX SCW kommt fünfmal vor, RJL WPX, SJM SPO und WTM RAO jeweils dreimal. Da es sich um Spruchschlüssel unterschiedlicher Sender handelt, ist anzunehmen, dass es sich um einfache stereotype Schlüssel wie zum Beispiel aaa, xyz oder ähnliche handelt. Wenn man unter allen Möglichkeiten der $P_1, P_2, ..., P_6$ nun diejenigen wählt, die diese Annahme bestätigen, wird man in den meisten Fällen die richtige Wahl getroffen haben.
Mit diesem Verfahren ergibt sich für die Permutationen $P_1, P_2, ..., P_6$ die folgende Darstellung:

$P_1 = (as)(br)(cw)(di)(ev)(fh)(gn)(jo)(kl)(my)(pt)(qx)(uz)$
$P_2 = (ay)(bj)(ct)(dk)(ei)(fh)(gx)(ln)(mp)(ow)(qr)(su)(vz)$
$P_3 = (ax)(bl)(cm)(dg)(ei)(fo)(hv)(ju)(kr)(np)(qs)(tz)(wy)$
$P_4 = (sa)(rc)(wb)(iv)(ep)(tf)(hk)(lx)(qg)(nz)(uy)(mo)(jd)$
$P_5 = (yx)(gt)(ca)(jl)(nf)(hq)(rv)(ze)(io)(wu)(sm)(pb)(kd)$
$P_6 = (xb)(lv)(hi)(ek)(rt)(zj)(ug)(df)(oc)(mq)(sn)(py)(wa)$

Besonders bemerkenswert ist es, dass es so gelang, die Spruchschlüssel zu analysieren, ohne die innere Verdrahtung der einzelnen Walzen zu kennen. Vermutlich ist auch dem deutschen Chiffrierdienst diese Schwäche des Schlüsselverfahrens aufgefallen, denn 1933 wurde die Verwendung der Buchstabenwiederholung bei den Spruchschlüsseln ausdrücklich verboten. Den polnischen Analytikern fiel jedoch auf, dass nun verstärkt Spruchschlüssel wie qwe, asd (nebeneinanderliegende Buchstaben auf der Enigma-Tastatur) verwendet wurden, so dass sich eine neue Einbruchsmöglichkeit ergab.

4.2 Analyse der Rotorverkabelungen

Nachdem eine Reihe Spruchschlüssel in chiffrierter und dechiffrierter Form vorlagen, konnte man beginnen, die Verdrahtung der drei Walzen zu analysieren. Auch dazu wurden nur die ersten sechs Zeichen, also die mittlerweile analysierten Spruchschlüssel, der Funksprüche eines Tages benötigt. Man ging dabei von dem Gleichungssystem

$$y_{k_i} = x_{k_i} SP\tilde{P}_i P^{-1} S^{-1}$$

aus, wobei x_{k_i} ein Klartextzeichen aus dem verdoppelten Spruchschlüssel ist, das an i-ter ($i \in \{1,...,6\}$) Position steht, und y_{k_i} ist das entsprechende Geheimtextzeichen. $S = S^{-1}$ ist die unbekannte aber konstante Substitution des Steckerbrettes, P die Substitution der mittleren und langsamen Walze, $\tilde{P}_i$ ist die Substitution der schnellen Walze in i-ter Position. Da sich bei sechs aufeinander folgenden Zeichen in den meisten Fällen nur die schnelle

Walze bewegte, kann man die Substitution P und somit auch P^{-1} als konstant annehmen.

Wenn genügend unterschiedliche Spruchschlüssel für eine Grundstellung vorliegen (das war an Manövertagen meistens der Fall), kann man durch Auflösung des Gleichungssystems die Verdrahtung der schnellen Walze ermitteln. Da die Positionen der Walzen regelmäßig gewechselt wurden, konnten alle Walzen analysiert werden.

Im September 1938 wurden zwei weitere Walzen, die so genannten Griechenwalzen, α und β eingeführt. Gleichzeitig änderte sich auch das Schlüsselverfahren. Da der deutsche Sicherheitsdienst aber weiterhin das alte Schlüsselverfahren verwendete, konnte auch die Verkabelung der neuen Walzen ermittelt werden.
Mit diesem Wissen war es nun möglich, die Wehrmachtsenigma nachzubauen. Im Jahr 1939 bekamen die Briten und Franzosen nachgebaute Enigma Modelle mit fünf Walzen vom polnischen Geheimdienst geliefert.

Um den Funkverkehr mitzuhören, musste man aber auch den Tagesschlüssel rekonstruieren, also die Walzenlage und Ausgangsstellung der Rotoren, die Ringstellung und die Steckerbrettsubstitution.

4.3 Analyse der Walzenlage und Grundstellung

Betrachten wir noch einmal die Zyklenschreibweise der P_iP_{i+3} für $i \in \{1,2,3\}$. Da man diese Permutationen aus den ersten sechs Zeichen eines Funkspruchs ermitteln kann (und sich bei sechs Verschlüsselungsschritten meistens nur die schnelle Walze bewegte), sind sie unabhängig von der Ringstellung. Anders ist es mit der Steckerbrettsubstitution, je nach Einstellung änderten sich die Permutationen P_iP_{i+3}. Da die Steckerbrettsubstitution involutorisch ist, ändern sich aber nicht die Längen der einzelnen Zyklen in den P_iP_{i+3}. Für die Aufteilung der Zykluslängen in den Permutationen P_1P_4, P_2P_5 und P_3P_6 gibt es genau $101^3 = 1.030.301$ Möglichkeiten (101 = Anzahl der Partitionen von 13). Für die Walzenlage (3!) und Rotorstellung gibt es jedoch nur $6 \cdot 26 \cdot 26 \cdot 26 = 105.456$ Möglichkeiten. Die Aufteilung der Zykluslängen in den drei Permutationen P_1P_4, P_2P_5 und P_3P_6 könnte also ausreichend sein, um die Lage und Stellung der Walzen zu charakterisieren (die Permutationen beinhalten mehr mögliche Schlüssel, als die Enigma selbst).
Mit Hilfe der nachgebauten Enigma-Modelle begannen die polnischen Analytiker einen Katalog anzufertigen, der zu allen Grundstellungen die Zyklenpartition der P_iP_{i+3} enthielt. Um diese Arbeit zu beschleunigen, ließ man sich ein Gerät (Zyklometer) anfertigen, welches wesentliche Teile dieser mühseligen Arbeit mechanisierte. Der Katalog war 1937 fertig, und es gelang tatsächlich, die Walzenlage und Grundstellung der Rotoren mit Hilfe des Kataloges zu ermitteln.

4.4 Analyse der Steckerbrettsubstitution

Auf einer nachgebauten Wehrmachtsenigma wurde die mit dem Katalog ermittelte Walzenlage und Grundstellung eingestellt. Die bereits bekannten Spruchschlüssel wurden verdoppelt und chiffriert. Beim Vergleich der so erhaltenen Kryptogramme mit den Originalkryptogrammen konnte man die Steckerbrettsubstitution ablesen.

Beispiel: Originalkryptogramm: x **p** t **v** a
eigene Kryptogramm: x **f** t **b** a

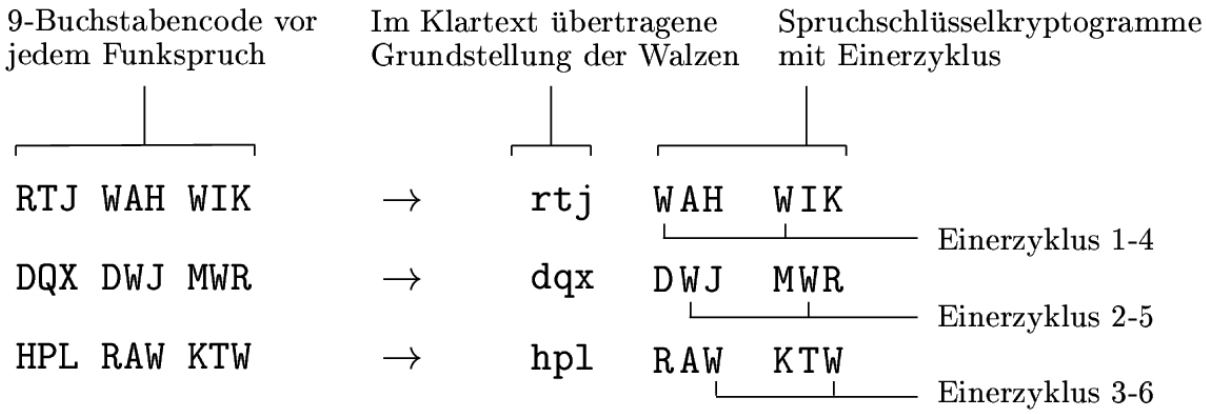
somit war klar, dass $p \to f$ und $v \to b$ substituiert wurde.
Die Ringstellung war für dieses Vorgehen nicht relevant, da bei jeweils sechs Zeichen in den meisten Fällen nur der schnelle Rotor bewegt wurde.

4.5 Analyse der Ringstellung

Da die Ausgangsstellung der Rotoren schon bekannt war, ging es beim Ermitteln der Ringstellung nur noch darum, herauszufinden, in welcher Position die Rotoren fortgeschaltet wurden. Mit Hilfe einer nachgebauten Enigma konnte man dies durch geschicktes Ausprobieren leicht feststellen. Sehr hilfreich war dabei der stereotype Charakter deutscher Funksprüche. So begannen fast alle Nachrichten mit den Buchstaben „ANX“, wobei das X anstelle eines Leerzeichens verwendet wurde, da es kein spezielles Leerzeichen im Alphabet der militärischen Enigma gab.

4.6 Die polnische Kryptographiebombe

Im Herbst 1938 änderten die Deutschen das Schlüsselverfahren. Die Grundstellung der Walzen wurde nun im Klartext übertragen. Anschließend folgte der verdoppelte Spruchschlüssel. Die bisherige Geheimtext-Geheimtext Analyse des Spruchschlüssels war nun nicht mehr anwendbar, da nicht genügend Spruchschlüssel mit der gleichen Grundeinstellung übertragen wurden. Der im Klartext übertragene Drei-Buchstaben Code für die Grundstellung war wertlos, da er die eigentliche Rotorstellung nur verriet, wenn man die Ringstellung kannte, die zusammen mit den Walzenpositionen und der Steckerbrettsubstitution den Tagesschlüssel bildeten.
Auf polnischer Seite entwickelte man nun eine elektromechanische Maschine, mit der es möglich war, die $26^3 = 17576$ Rotorstellungen durchzutesten. Diese Apparatur wurde (vermutlich wegen ihres Aussehens) „Bomba“ genannt. Das maschinelle Durchtesten aller Rotorstellungen war ein mechanisches Problem, das schnell gelöst war. Schwieriger war es, einen Mechanismus zu konstruieren, der die „richtige“ Rotorstellung automatisch erkennt. Man verwendete dazu Spruchschlüssel-Kryptogramme, die sogenannte Einerzyklen aufwiesen. Da genügend Funksprüche abgesetzt wurden, war es unproblematisch, solche zu finden.



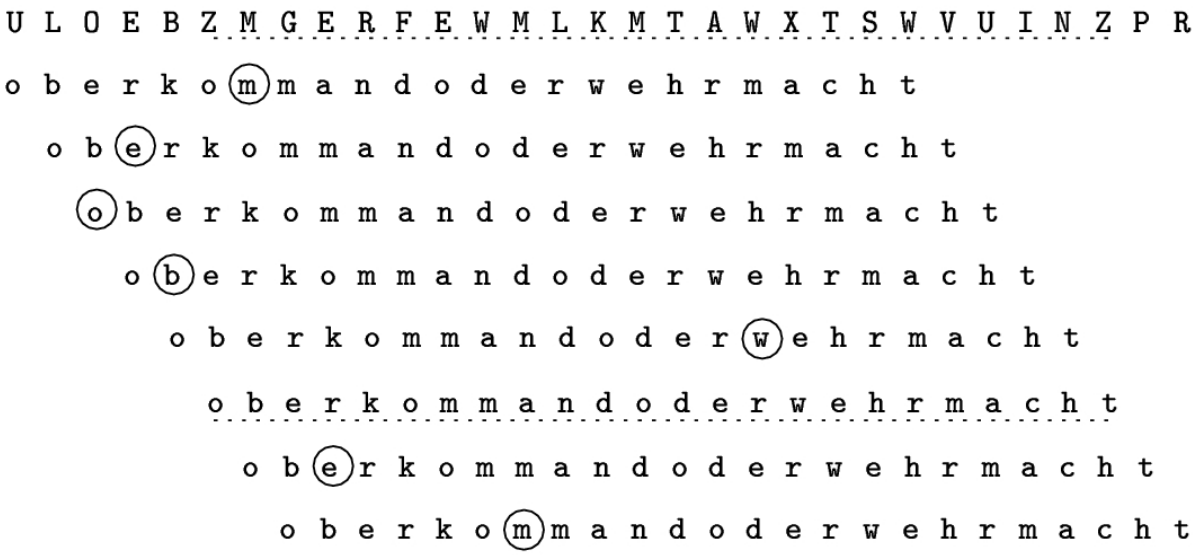
Es wurden drei Spruchschlüssel S_1, S_2, S_3 benötigt, die jeweils an den Positionen 1-4, 2-5 und 3-6 den gleichen Buchstaben enthielten, so wie die Spruchschlüssel in der obigen Abbildung.

Die Maschine zum Testen der Rotorstellungen bestand aus 6 Enigma-Walzensätzen (Walzensatz = 3 Walzen), deren Rotoren mittels eines gemeinsamen Antriebs simultan fortgeschaltet wurden. Auf diese Weise konnte man alle Rotorstellungen auf den 6 Walzensätzen durchtesten.
Zwei Walzensätze wurden gemäß der Grundstellung S_1 (RTJ) eingestellt, zwei gemäß S_2 (DQX) und die letzten beiden gemäß S_3 (HPL). Anschließend wurden die Walzen manuell um so viele Schritte fortgeschaltet, dass die Einerzyklen bei richtiger Ringstellung an allen 6 Rotorsätzen gleichzeitig auftraten.
Die Maschine war so konstruiert, dass die Walzensätze simultan fortgeschaltet wurden. Wenn sich an allen Walzensätzen der gleiche Buchstabe eingestellt hat (welcher Buchstabe das war konnte man wegen der unbekannten Steckerbrettsubstitution nicht sagen), sorgte eine entsprechende Relaisschaltung dafür, dass die Maschine anhielt, so dass man die Rotorstellung ablesen konnte.
Die so ermittelte Rotorstellung musste nicht unbedingt die richtige sein. Die Maschine stoppte aber relativ selten, und man konnte die ermittelten Rotorstellungen mit einer nachgebauten Wehrmachtsenigma testen. Durch Vergleich der Rotorpositionen mit den im Klartext übertragenen Walzenstellungen ergaben sich die gesuchten Einstellungen der Alphabetringe. Das Testen aller 17567 Ringstellungen eines Tagesschlüssels dauerte etwa 2 Stunden.

Ende Juli 1939 zeigten die Polen dem britischen Kryptoanalytiker Alfred Dyllwyn Knox ihre Analysemethoden und Resultate. Es ist anzunehmen, dass auch dem deutschen Chiffrierdienst die polnischen Analysen bekannt waren, denn am 1. Mai 1940, kurz vor dem Einmarsch in Frankreich, wurde das Schlüsselverfahren erneut geändert. Der Spruchschlüssel wurde nur noch einfach chiffriert, wodurch die bisherigen Methoden zur Analyse der Enigma-Kryptogramme unbrauchbar wurden.

4.7 Britische Analyse 1939 bis 1945

Bei dem britischen Analyseansatz der Enigma handelte es sich um eine sogenannte Geheimtext-Klartext-Analyse. Grundlage dafür war ein zusammenhängendes (möglichst langes) Klartext-/Geheimtextpaar. Um ein solches Paar zu finden, suchte man nach langen Worten oder Phrasen, die mit großer Wahrscheinlichkeit in den verschlüsselten Texten vorhanden waren. Wegen der Vorliebe für stereotype Redewendungen im Wehrmachtsjargon war es nicht schwierig, geeignete Textpassagen zu finden.
Anschließend musste man herausfinden, an welcher Stelle diese Textpassagen in den Kryptogrammen versteckt waren. Unter Ausnutzung des involutorischen Charakters der Enigma eignete sich hierfür die „negative Mustersuche“. Diese Vorgehensweise wird nun an einem Beispiel erklärt.
Sei „...ULOEBZMGERFEWMLKMTAWXTSWVUTNZPR ...“ eine Folge von Geheimtextzeichen. Als wahrscheinliches Wort wird hier im Beispiel „oberkommandoderwehrmacht“ angenommen. Da ein Zeichen wegen des involutorischen Charakters der Enigma nie zu sich selbst verschlüsselt wird, führen die meisten Positionen zu einem Widerspruch.

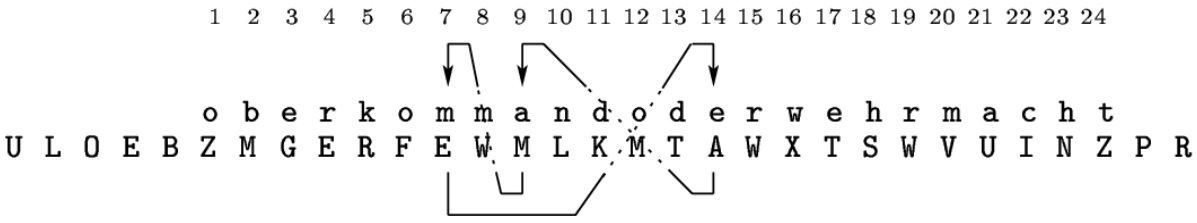


Diese Widersprüche sind in obiger Abbildung durch Kreise um den entsprechenden Buchstaben gekennzeichnet. Letztlich verbleibt nur eine mögliche Position.
Nachdem man auf diese Weise ein geeignetes Klartext-/Geheimtextpaar findet, wäre es theoretisch möglich, alle potentiellen Schlüssel zu testen, dabei gibt es jedoch zwei Probleme:

- Die Anzahl aller möglichen Enigma-Schlüssel ist derart groß, dass auch ein maschinelles Testen nicht in akzeptabler Zeit durchzuführen ist.

- Selbst wenn es gelingt, eine Maschine zu bauen, die alle potentiellen Einstellungen der Enigma durchprobiert, muss man noch dafür sorgen, dass die richtige Einstellung erkannt wird. Natürlich erkennt man den richtigen Schlüssel, wenn man den Geheimtext dechiffriert und dabei kontrolliert, ob der richtige Klartext erscheint. Aber eben dieses Erkennen eines sinnvollen Klartextes war mit den technischen Möglichkeiten der Dreißiger und Vierziger Jahre nicht ohne weiteres zu automatisieren.

Das Verfahren, mit dem es möglich wurde, den richtigen Schlüssel zu ermitteln, stammt von Alan M. Turing. Betrachten wir noch einmal den Klartext und das dazugehörige Kryptogramm aus dem Beispiel oben. In der folgenden Abbildung ist eine „Schleife“ eingezeichnet, die durch die Positionen 14, 9 und 7 geht.



Bei Position 14 wird e zu A verschlüsselt, bei Position 9 wird a zu M verschlüsselt und bei Position 7 wird m zum Anfangsbuchstaben E der Schleife chiffriert. Turing hat erkannt, dass sich solche Schleifen schaltungstechnisch mittels einer geeigneten elektromechanischen Maschine erkennen lassen, also zum automatischen Prüfen der verschiedenen Schlüssel verwendbar sind. Bevor wir uns jedoch ansehen, wie so eine Maschine im Einzelnen funktioniert, betrachten wir die im Beispiel auftretenden Schleifen etwas genauer.

Sei T die Substitution des Steckerbrettes und P_i die Rotorsatzpermutation im i-ten Verschlüsselungsschritt. Mit diesen Bezeichnungen wird die in obiger Abbildung dargestellte Schleife wie folgt beschrieben:

14, 9, 7: $eT = mTP_7$, $mT = aTP_9$, $aT = eTP_{14}$ $\Rightarrow$ $eT = eTP_{14}P_9P_7$

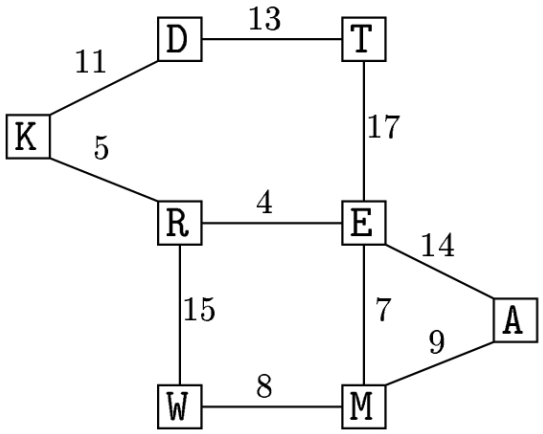
Unter Berücksichtigung der Tatsache, dass die Enigmasubstitutionen involutorisch sind, findet man noch die „Schleifen“:

4, 15, 8, 7: $eT = rTP_4$, $wT = rTP_{15}$, $wT = mTP_8$, $eT = mTP_7$ $\Rightarrow$ $eT = eTP_4P_{15}P_8P_7$

4, 5, 11, 13, 17: $eT = rTP_4$, $rT = kTP_5$, $kT = dTP_{11}$, $dT = tTP_{13}$, $tT = eTP_{17}$ $\Rightarrow$ $eT = eTP_{17}P_{13}P_{11}P_5P_7$

Man sieht hier, dass die Existenz dieser Schleifen unabhängig von der Einstellung des Steckerbrettes ist. Das ist der entscheidende Vorteil dieses Verfahrens, denn wenn es gelingt, durch Betrachtung dieser Schleifen den richtigen Schlüssel zu erkennen, kann man sich zunächst auf die Ausgangsstellung der Rotoren konzentrieren, was dazu führt, dass man nur $26^3 = 17576$ Möglichkeiten durchtesten muss und nicht den gesamten Schlüsselraum. Die Analytiker in Bletchley Park (sitz der britischen Kryptologen, etwa 50 Meilen nördlich von London) hofften, dass die Schleifen dieser relativen Rotorpositionen nur bei sehr wenigen Ausgangstellungen der drei Rotoren auftreten. Diese Hoffnung hat sich bestätigt. So war es möglich, die so gefundenen Ausgangsstellungen der Walzen manuell zu prüfen, um den richtigen Schlüssel zu finden.

In Bletchley Park war es damals üblich, die Schleifen in Form ungerichteter Diagramme darzustellen.

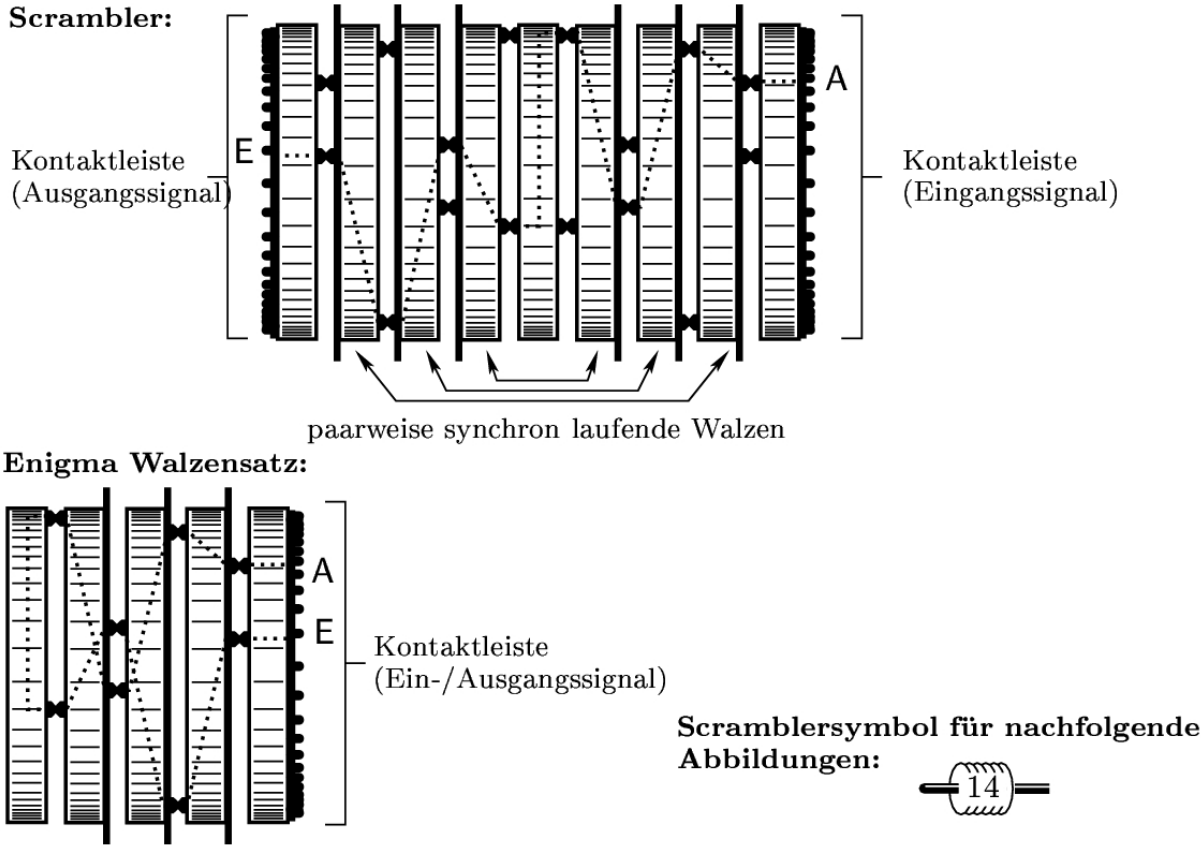


Die Abbildung zeigt das entsprechende Diagramm zu den oben beschriebenen Schleifen.

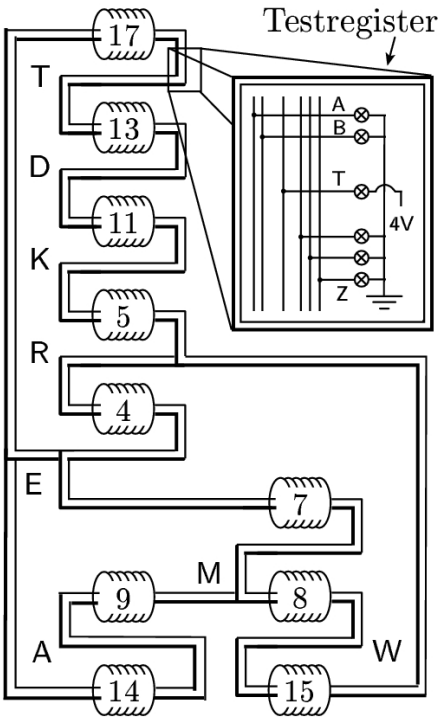
4.8 Die Turing-Bombe

Die Konstruktion einer Maschine, die es ermöglichte den richtigen Schlüssel unter Ausnutzung der Schleifen in einem Klartext-/Geheimtextpaar zu finden, war Alan Turings Aufgabe. Auch der Bau dieser Maschine verlief unter seiner Aufsicht. Die sogenannte

„Turing-Bombe“ unterschied sich wesentlich von der polnischen Dechiffriermaschine „Bomba“, der Name wurde aber dennoch beibehalten.
Die polnische „Bombe“ bestand aus sechs Enigma-Walzensätzen, diese jeweils aus drei Walzen und einer Umkehrwalze, was dazu führte, dass die 26-polige Kontaktleiste des Walzensatzes sowohl für das Eingangssignal als auch für das Ausgangssignal verwendet wurde. Für die britischen Bomben erwies sich das als unpraktisch, und man baute stattdessen sogenannte „Scrambler“ (Vertauscher), die eine 26-polige Steckerleiste für das Eingangssignal und ein 26-polige Steckerleiste für das Ausgangssignal hatten. Ansonsten simulierten diese „Scrambler“ das Verhalten und die Permutationen eines Enigma-Walzensatzes.



In dieser Abbildung sind ein Enigma-Walzensatz und ein „Scrambler“ schematisch dargestellt. Die Turing Bombe bestand aus vielen Scramblern, die gemäß der gefundenen Schleifen mit 26-adrigen Kabeln verbunden wurden. Anschließend wurden die relativen Rotorpositionen an den Scramblern eingestellt. In folgender Abbildung ist dies schematisch dargestellt.



Die Scrambler wurden simultan fortgeschaltet, um alle 17.576 Ausgangspositionen durchzutesten. Wenn die Scrambler sich in der richtigen Position befanden, mussten die Schleifen auch in Form einer elektrischen Verbindung vorliegen, was mit Hilfe eines Testregisters geprüft wurde (siehe obige Abbildung).
An dem Testregister wurde ein beliebiges Kabel unter Spannung gesetzt. In dem Beispiel, das auch in der Abbildung dargestellt ist, wurde das „T“-Kabel gewählt. Da man im allgemeinen Fall aber die Steckerbrettsubstitution nicht kannte, konnte man auch nicht mit Bestimmtheit sagen, welches Kabel Spannung bekam. Man unterscheidet deshalb zwei Fälle:

- Die Steckerbrettsubstitution wurde richtig gewählt, und das T-Kabel war unter Spannung. In diesem Fall erkannte man die richtige Ringstellung daran, dass nur eine Leuchte, nämlich die T-Leuchte, am Testregister aufblitzte, da die im Diagramm aufgezeichneten Schleifen auch physikalisch vorhanden waren und kein Strom in ein anderes Kabel außerhalb der entsprechenden Schleifen gelangte.

- Die Steckerbrettsubstitution wurde falsch gewählt und es wurde ein Kabel außerhalb der Schleifen unter Spannung gesetzt. Die richtige Ringstellung erkannte man nun daran, dass (wenn genügend Schleifen vorhanden waren) alle Leuchten außer der T-Leuchte aufblitzten. Die T-Leuchte bleibt dunkel, da die Schleifen in sich geschlossen waren und kein Strom auf ein Kabel innerhalb der Schleifen gelangte.

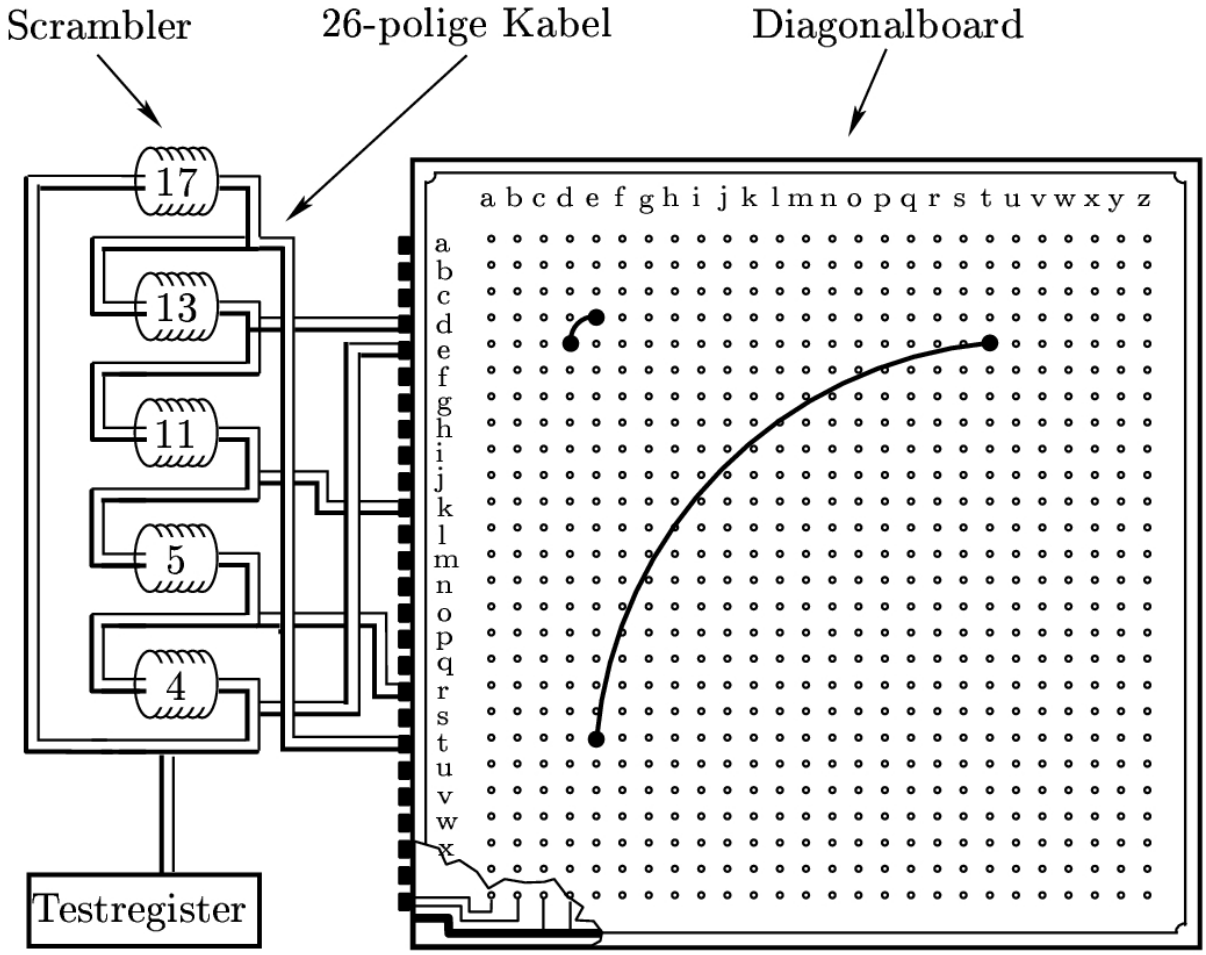
Eine Relaisschaltung brachte die Maschine zum Stillstand, wenn eine Ringstellung gefunden wurde, die die entsprechenden Schleifen aufwies. In diesem Fall wurde die gefundene Ringstellung notiert und die Maschine wieder in Gang gesetzten, um weiter Möglichkeiten zu suchen.

Das Verfahren funktionierte nur, wenn genügend Schleifen vorhanden waren, aber auch dann konnte es vorkommen, dass die Maschine bei „falschen“ Rotorpositionen stehen blieb. Ob es sich bei einer der gefundenen Rotorpositionen um den richtigen Schlüssel handelte, konnte durch versuchsweises Dechiffrieren der reichlich vorhandenen Kryptogramme ermittelt werden.

4.9 Die Turing-Welchman-Bombe

Gordon Welchman verbesserte die Turing-Bombe entscheidend durch das Hinzufügen des sogenannten „Diagonal-Board“. Damit war es möglich, den involutorischen Charakter der Enigma besser auszunutzen. Um die Funktionsweise des Diagonal-Board zu erklären, betrachten wir die T-D-K-R-E-Schleife aus dem obigen Beispiel.

Nimmt man zum Beispiel die Scrambler 11, 5 und 4, so erkennt man, dass (bei richtiger Grundstellung) diese das d-Kabel zwischen den Scramblern 13 und 11 auf das e-Kabel zwischen den Scramblern 4 und 17 schalten. Da die Scrambler involutorisch arbeiten, muss aber auch das e-Kabel auf das d-Kabel geschaltet werden. Das Diagonalboard wurde so an die Turingbombe angeschlossen, dass alle Verbindungen dieser Art mit losen Kabeln gesteckt werden konnten und somit bei *jeder* Rotorstellung vorhanden waren.



Damit erreichte man folgendes:
Bei der richtigen Rotorstellung wurde die Anzeige am Testregister nicht verändert, da die elektrische Verbindung des Diagonalboards, z.B. zwischen e und d, ohnehin schon innerhalb der Scrambler existierten. Bei falscher Wahl der Rotorstellungen sorgten die Verbindungen auf dem Diagonal Board jedoch dafür, dass das Testregister erheblich schneller aufgefüllt wurde, wodurch man auch mit wenigen Schleifen eine erfolgreiche Analyse durchführen konnte. Ferner reichten auch relativ kurze Schleifen, was dazu führte, dass sich der mittlere und langsame Rotor nur mit kleiner Wahrscheinlichkeit bewegten. Auch das war ein gewaltiger Vorteil, denn die Rotorbewegungen hingen von den noch nicht bekannten Ringstellungen ab. Diese ringstellungsabhängige Rotorbewegung wurde von der Turing-

Welchman-Bombe nicht weiter berücksichtigt. Falls keine Analyse gelang, musste mit verschiedenen Ringstellungen experimentiert werden, was viel Zeit beanspruchte.

Die erste Bombe wurde von Alan Turing AGNUS getauft, sie war im Sommer 1940 betriebsbereit und brauchte ca. 11 Minuten für einen Durchlauf. Auch in technischer Hinsicht war diese Bombe ein Meisterwerk. Im Frühjahr 1941 waren acht Bomben betriebsbereit, gegen Ende 1941 zwölf, im August 1942 dreißig, im März 1943 sechzig und kurz vor Kriegsende waren 200 Turing-Welchman-Bomben im Einsatz. Den Briten gelang es, fast alle Funksprüche der deutschen Wehrmacht zu dechiffrieren, die in den Äther gesendet wurden. In Bletchley Park wurde ein riesiges Archiv für die aufgefangenen Funksprüche angelegt. Ferner wurden alle gewonnenen Informationen unter militärischen Gesichtspunkten ausgewertet und an die entsprechenden Heeresstellen weitergeleitet.

4.10 Die Hilfe der Amerikaner

Am 1. Februar 1942 kam dann der Rückschlag, in deutschen U-Booten wurde eine neue Enigma-Maschine mit 4 Rotoren verwendet. Man kannte wenigstens die Verdrahtung des hinzugekommenen festen Rotors. Dieser war schon längere Zeit in der Maschine, aber in Ruhestellung. Eines Tages hatte jemand den Rotor versehentlich benutzt, woraufhin der Empfänger nur unverständlichen Text erhielt. Bei der erneuten Übertragung machte sich jener unachtsame Chiffreur nicht die Mühe, neue Rotorstellungen zu benutzen und so konnten die Engländer, die beide Nachrichten empfangen hatten, aus der Differenz die Verdrahtung des neuen Rotors bestimmen. Dies änderte jedoch nichts daran, dass der Materialaufwand zur Dechiffrierung um Faktor 26 steigen würde. Wie 1938 die Polen sahen sich nun die Engländer nicht mehr in der Lage, mit eigenen Mitteln weiter zu kommen. Selbst wenn man die nötigen Bomben hätte bauen können, sie wären zu langsam gewesen. Zu diesem Zeitpunkt arbeitete man zwar an der Entwicklung einer elektronischen Variante der Bomben, auf englischer Seite konnte sie aber nie zum funktionieren gebracht werden.

In der Folge musste die Zusammenarbeit mit den Amerikanern verstärkt werden. Diese konnten im September 1942 schließlich mitteilen, dass sie eine neue bessere Bombe entwickelt hatten, sie verfügten über die nötigen Ressourcen.

Ab 1943 beherrschten die Engländer zusammen mit den Amerikanern endlich die Enigma. Einige Schlüssel wurden allerdings nie gebrochen. Das lag hauptsächlich an der seltenen Verwendung, beispielsweise des U-Boot-Schlüssels für "taktische Trainingsaufgaben".

5. Abschlußbetrachtung

Die Verschlüsselungssysteme des Deutschen Reichs im zweiten Weltkrieg waren die besten, die man weltweit bis dahin entwickelt hatte. Die deutschen Ingenieure leisteten bei der Erweiterung der Enigma hervorragende Arbeit. Aber auch auf alliierter Seite wurden innerhalb weniger Jahre großartige Leistungen vollbracht, die in Friedenszeiten Jahrzehnte der Entwicklung bedurft hätten.

Es gibt zwei Hauptfaktoren, die die deutschen Chiffriersysteme zu Fall brachten. Der Erste, nämlich die Fehler ausführender Personen bei der Schlüsselverwendung und der Nachrichtenübertragung, ist praktisch nie auszuschließen. Der andere jedoch, einem System bedingungslos zu vertrauen, selbst nach eindeutigen Hinweisen die Wahrscheinlichkeit eines

Versagens mit Null anzusetzen, sollte in Zukunft ausgeschlossen werden. Insbesondere, als festgestellt wurde, dass der Feind offenbar gewisse Nachrichten kannte.

Die Dechiffrierung der Enigma durch die Alliierten ist ein Phänomen. Ohne die französischen Informationen hätten die Polen vermutlich nicht genug Zeit gehabt, die Enigma zu brechen. Andererseits wären die Engländer ohne die Vorarbeit der Polen kaum in der Lage gewesen, so weit zu kommen. Und ohne die Amerikaner schließlich wäre man ab 1942 wieder blind gegenüber den U-Booten gewesen. Obwohl Misstrauen das Verhältnis dieser Länder untereinander prägte, konnte nur durch die Beiträge aller, das deutsche Enigma-System beherrscht werden.

Der Verlauf des 2. Weltkrieges wurde entscheidend durch die erfolgreiche Kryptoanalyse der Alliierten geprägt. Möglicherweise hat diese Leistung entscheidend dazu beigetragen, den Abwurf einer Atombombe über Deutschland zu vermeiden.