Die Mathematik der Enigma

Maturaarbeit am Gymnasium Kirschgarten Basel
auf Basis der Abschlussarbeit an der Rudolf Steiner Schule Basel

Jérôme Dohrau

unter der Betreuung von Prof. Dr. Hanspeter Kraft

18. September 2008

Inhaltsverzeichnis

Vorwort

Das Thema für meine Abschlussarbeit stand als Erstes fest. Schon relativ früh wusste ich, dass ich ein mathematisches Thema behandeln wollte. Nachdem ich einige Themen in Erwägung gezogen hatte, entschied ich mich, eine Arbeit über die Enigma, eine elektromechanische Chiffriermaschine, zu schreiben.

Die Suche nach einem geeigneten Mentor führte mich zu Herrn Prof. Dr. Hanspeter Kraft an der Universität Basel, der sofort einwilligte und mir schon bei unserem ersten Treffen einen umfassenden Überblick über die für meine Arbeit notwendigen mathematischen Kenntnisse bot. Damit war der Einstieg in die Arbeit getan. Nun galt es, mich rund 7 Monate in mein Thema zu vertiefen.

An dieser Stelle möchte ich all den Menschen einen grossen Dank aussprechen, die mich während dieser Zeit in meiner Arbeit unterstützt haben. Dieser Dank richtet sich in erster Linie an meinen Mentor, Herrn Prof. Dr. Hanspeter Kraft, für seine ausgezeichnete Betreuung, die interessanten Gespräche und die Zeit, die er sich immer wieder für mich genommen hat. Ein besonderer Dank geht auch an meinen Mathematiklehrer, Herrn Michael Schröter, der mich als Kontaktperson zur Schule bei meiner Abschlussarbeit begleitete und Korrektur gelesen hat.

Kapitel 1

Einleitung

Man findet relativ viel Literatur über die Chiffriermaschine Enigma. In den meisten Büchern werden hauptsächlich die Funktionsweise und der historische Hintergrund der Enigma behandelt. In einigen Büchern werden auch die mathematischen Aspekte der Enigma beschrieben. Dabei werden oft Tatsachen ohne grosse Erklärungen hingestellt, oder nur unvollständig beschrieben.

Ziel meiner Abschlussarbeit ist es, dem Leser einen Einblick in die Funktionsweise der Enigma zu geben. Insbesondere möchte ich die mathematischen Zusammenhänge der Enigma behandeln. Dazu werde ich im Verlaufe meiner Arbeit die mathematischen Grundlagen der Enigma herausarbeiten und im Detail erklären. Ferner will ich aufgrund dieser Analysen zeigen, wieso es Alan Turing gelungen war, die Enigma-Verschlüsselung zu „knacken“. Die zum Verständnis meiner Arbeit notwendigen mathematischen Grundkenntnisse aus der elementaren Zahlentheorie und der Gruppentheorie werden im Anhang erklärt.

Nebst der mathematischen Behandlung meines Themas werde ich auch kurz auf die historischen Zusammenhänge eingehen und den engeren und weiteren historischen Kontext beschreiben.

Kapitel 2

Kryptologie

Die *Kryptologie* ist die Wissenschaft, die sich mit der sicheren Übermittlung oder Speicherung von Nachrichten oder anderen beliebigen Daten befasst. Bis ins 20. Jahrhundert wurde die Kryptologie fast ausschliesslich zur Geheimhaltung von Nachrichten, vor allem im militärischen Bereich, eingesetzt. Mit dem Einzug des Computers und des Internets wurde die Kryptologie dann auch für zivile Anwendungen zunehmend wichtiger.

Die Kryptologie lässt sich in zwei Hauptbereiche aufteilen: *Kryptographie* und *Kryptoanalyse*. Der wesentliche Unterschied zwischen diesen beiden Bereichen liegt darin, dass sich die Kryptographie mit der Entwicklung und Anwendung kryptologischer Verfahren befasst und die Kryptoanalyse die Stärken und Schwächen solcher Verfahren untersucht.

2.1 Kryptographie

Ursprünglich war die Kryptographie die Wissenschaft der Verschlüsselung von Informationen; doch heutzutage ist das Gebiet der Kryptographie viel umfangreicher. Die Ziele der modernen Kryptographie werden im nächsten Abschnitt beschrieben.

2.1.1 Ziele der Kryptographie

Im Wesentlichen gibt es fünf Anforderungen, die an ein kryptographisches Verfahren gestellt werden können.

Geheimhaltung Durch die *Geheimhaltung* soll erzielt werden, dass nur berechtigte Personen in der Lage sind, Daten zu lesen oder Informationen über deren Inhalt zu erlangen.

Dazu werden sogenannte Verschlüsselungsverfahren entwickelt, die es einer unbefugten Person in der Praxis unmöglich machen soll, durch die

verschlüsselten Daten auf den unverschlüsselten Inhalt zu schliessen. Viele Verfahren sind jedoch nur in der praktischer Anwendung sicher. Das heisst, dass der zur Entschlüsselung notwendige Zeitaufwand so gross ist, dass er entweder nicht zu bewältigen ist, oder die Geheimhaltung nach Bewältigung dieses Zeitaufwands nicht mehr gewährleistet sein muss.

Um sich das Prinzip der Geheimhaltung veranschaulichen zu können, kann man sich einen Briefkasten vorstellen. Es ist jeder Person möglich, einen Brief in diesen Briefkasten zu werfen; aber nur eine Person hat den passenden Schlüssel zu diesem Briefkasten und kann die Briefe herausnehmen und lesen.

Authentifizierung Man kann bei der *Authentifizierung* zwischen den Bereichen der Datenauthentifizierung und der persönlichen Authentifizierung unterscheiden.

Durch die *Datenauthentifizierung* soll der Ursprung der Daten eindeutig nachgewiesen werden können. Die *persönliche Authentifizierung* dient dazu, dass zwei Kommunikationspartner sich so ausweisen können, dass der eine sicher sein kann, dass der andere auch derjenige ist, für den er sich ausgibt.

Als Veranschaulichung des Prinzips kann man sich bei der Authentifizierung einen abschliessbaren Schaukasten vorstellen. Zu diesem Schaukasten hat nur eine Person den Schlüssel. Das bedeutet, dass alles, was in diesem Schaukasten zu sehen ist, von dieser Person stammen muss.

Integrität Unter dem Begriff *Integrität* versteht man, dass Daten nicht verändert werden können, ohne dass es bemerkt wird. Der Empfänger muss also in der Lage sein, festzustellen, ob die Daten während der Übermittlung durch Dritte verändert wurden.

Die Integrität lässt sich gut mit einem versiegeltem Brief vergleichen: Wird der Inhalt des Briefs verändert, so muss er dazu aufgemacht werden. Durch das Aufmachen wird das Siegel zerstört; die Änderung wird dadurch bemerkbar.

Verbindlichkeit Die *Verbindlichkeit* soll verhindern, dass der Absender einer Nachricht bestreiten kann, die Daten jemals abgeschickt zu haben. Dies erscheint im ersten Moment vielleicht gleichwertig mit der Authentifizierung, doch der Unterschied zwischen der Verbindlichkeit und der Authentifizierung liegt darin, dass bei der Verbindlichkeit nicht nur überprüft werden kann, ob die Daten vom angegebenen Absender stammen, sondern der Absender auch noch zu einem späteren Zeitpunkt gegenüber Dritten nachgewiesen werden kann.

Zur Veranschaulichung der Verbindlichkeit, kann man diese mit einer von einem Notar beglaubigten Unterschrift eines Kaufvertrags vergleichen. Weder Käufer noch Verkäufer können abstreiten, den Vertrag je unterschrieben zu haben.

Anonymität Die *Anonymität* fordert, dass die Identität einer teilhabenden Person gegenüber den anderen geheim gehalten wird und nicht herausgefunden werden kann.

Es gibt Situationen, wie zum Beispiel beim Online-Handel, elektronischen Wahlen oder elektronischem Geld, bei denen die teilnehmenden Parteien trotz der Anonymität eindeutig identifizierbar sein müssen.

Unter Anonymität stellt man sich meistens eine unbekannte Person vor. Anonymität tritt aber auch in vielen anderen Formen auf. Zum Beispiel ist der klassische Geldverkehr, also das Bezahlen mit Münzen und Noten, anonym: Man sieht einer Münze nicht an, wer alles schon im Besitz dieser Münze war. Ebenso wenig muss der Kunde den Verkäufer kennen, um etwas kaufen zu können.

Viele dieser Anforderungen treten erst in moderneren Anwendungen der Kryptographie auf. Dafür kommen sie heutzutage um so mehr zum Einsatz.

2.1.2 Grundschema eines Verschlüsselungsverfahrens

Ein *Verschlüsselungsverfahren* verschlüsselt beliebige Daten. Der Einfachheit halber ist hier nur von der Verschlüsselung von Textnachrichten die Rede.

In der Kryptologie wird ein unverschlüsselter Text als *Klartext* bezeichnet. Ein verschlüsselter Text wird als *Chiffretext* bezeichnet.

Ein Verschlüsselungsverfahren ist im Grunde genommen nichts anderes, als eine Abbildung $E : P \to C$, welche die Menge der Klartexte P (plaintext) auf die Menge der Chiffretexte C (ciphertext) abbildet.

Die Abbildung E hängt vom Verschlüsselungsschlüssel k_e (encryption key) ab. Zudem hängt das Bild der Abbildung vom Klartext p, der verschlüsselt werden soll, ab.

$$E_{k_e}(p) = c$$

Es ist wichtig, dass für zwei unterschiedliche Klartexte, welche mit gleichem Schlüssel verschlüsselt werden, auch deren Chiffretexte unterschiedlich sind. Wenn dies nicht der Fall wäre, dann könnte man den Chiffretext nicht mehr eindeutig entschlüsseln. Es muss also gelten:

$$p_1 \neq p_2 \quad \Rightarrow \quad E_{k_e}(p_1) \neq E_{k_e}(p_2)$$

Das bedeutet, dass die Abbildung E_{k_e} injektiv ist.

Der Chiffretext c wird mit einem zum Verschlüsselungsverfahren gehörenden Entschlüsselungsverfahren entschlüsselt. Dieses Entschlüsselungsverfahren ist eine Abbildung $D : C \rightarrow P$, welches die Menge der Chiffretexte C auf die Menge der Klartexte P abbildet.

Sofern der zum Verschlüsselungsschlüssel k_e passende Entschlüsselungsschlüssel k_d (decryption key) gewählt wird, liefert die Abbildung wieder den ursprünglichen Klartext.

$$D_{k_d}(c) = p$$

Die Abbildung D_{k_d} ist also die Umkehrabbildung der Abbildung E_{k_e}.

$$D_{k_d} = {E_{k_e}}^{-1}$$

Ist k_d gleich k_e oder ist k_d leicht aus k_e zu berechnen, so spricht man von einem *symmetrischem Verschlüsselungsverfahren*.

Liefert k_e keine Kenntnisse von k_d, so spricht man von einem *asymmetrischen Verschlüsselungsverfahren*. In diesem Fall kann k_e öffentlich gemacht werden. Man spricht auch von einem *Public-Key-Verfahren*.

2.1.3 Kerckhoffsches Prinzip

Ein wichtiger Grundsatz der modernen Kryptographie ist das nach Auguste Kerckhoffs benannte *Kerckhoffsche Prinzip*:

> „Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels."

Mit anderen Worten: Selbst wenn ein Verschlüsslungsverfahren bekannt ist, darf eine Nachricht nur durch Kenntnis des Schlüssels dechiffriert werden können. Damit eine Nachricht nicht durch Ausprobieren der möglichen Schlüssel zu entziffern ist, ist zudem auch eine Vielzahl möglicher Schlüssel für die Gewährleistung der Sicherheit nötig.

Kapitel 3

Klassische Verschlüsselungen

3.1 Monoalphabetische Substitution

Eines der einfachsten Verschlüsselungsverfahren, das man sich vorstellen kann, ist die *monoalphabetische Substitution*. Bei diesem Verfahren wird jeder Buchstabe des Alphabets durch einen anderen Buchstaben ersetzt.

Wenn eine mit der monoalphabetischen Substitution verschlüsselte Nachricht übermittelt werden soll, so müssen sich Absender und Empfänger zuerst auf einen gemeinsamen Schlüssel, ein Geheimtextalphabet, einigen. Das heisst, sie müssen festlegen, welcher Buchstabe durch welchen ersetzt wird. Ein Beispiel für einen solchen Schlüssel ist in Abbildung 3.1 dargestellt.

Wenn nun der Absender die Nachricht verschlüsseln will, so muss er alle Buchstaben des Klartexts durch den entsprechenden Buchstaben des Geheimtextalphabets ersetzten. Würde der Absender die Nachricht `ALLES IN ORDNUNG` unter der Verwendung des in Abbildung 3.1 dargestellten Schlüssels verschlüsseln, so würde der Chiffretext `HNNOR XM DITMQMW` lauten.

Der Empfänger kann, wenn er die Nachricht empfangen hat und den korrekten Schlüssel besitzt, ohne grosse Schwierigkeiten herausfinden, wie der Klartext lauten muss. Er beginnt mit dem ersten Buchstaben und geht die Nachricht Buchstabe für Buchstabe durch. Er wird feststellen, dass das `H` für ein `A` steht, das `N` für ein `L` usw. Nachdem er alle Buchstaben der Nachricht entschlüsselt hat, kann er den gesamten Klartext lesen.

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

Abbildung 3.1: Der Schlüssel enthält in der oberen Zeile die Klartextbuchstaben, unter denen die entsprechenden Geheimtextbuchstaben stehen.

3.1.1 Verschlüsselung als Permutation

Wie bereits erklärt, bildet ein Verschlüsselungsverfahren einen Klartext auf einen Chiffretext ab (siehe Kapitel 2.1.2).

Der Klartext p einer Nachricht der Länge r besteht aus r Buchstaben eines Alphabets A.

$$p = p_1 \ \ldots \ p_r \qquad p_i \in A$$

Sind Klartextalphabet und Chiffretextalphabet identisch, so besteht der Chiffretext c auch aus r Buchstaben des Alphabets A.

$$c = c_1 \ \ldots \ c_r \qquad c_i \in A$$

Der Schlüssel φ ist eine der möglichen Permutationen von A (Permutation; siehe Anhang B.4). Die Anzahl der möglichen Schlüssel hängt von der Länge n des Klartextalphabets A ab und beträgt $n!$ (n-Fakultät; siehe Anhang A.1).

Verschlüsselt wird, indem auf jeden einzelnen Buchstaben p_i des Klartextes p die Permutation φ angewendet wird. Durch die Anwendung der Permutation entsteht der entsprechende Buchstabe c_i des Chiffretextes, die dann alle zusammen den Chiffretext c bilden.

$$E_\varphi(p) = \varphi(p_1) \ \ldots \ \varphi(p_r) = c_1 \ \ldots \ c_r = c$$

Die Menge der Permutation φ von der Menge A ist eine nichtkommutative Gruppe, welche *symmetrische Gruppe* (siehe Anhang B.10) genannt wird. Dies ist von Bedeutung, denn dadurch ist garantiert, dass zu jeder Permutation φ eine inverse Permutation φ^{-1} existiert, welche zur Entschlüsselung notwendig ist.

Nebst den inversen Permutationen gibt es noch die neutrale Permutation φ_n, die den Klartext nicht verändert. Diese Permutation ist zudem ihre eigene inverse Permutation.

Der Chiffretext c wird entschlüsselt, indem die inverse Permutation φ^{-1} auf die einzelnen Buchstaben angewendet wird. Dadurch entsteht wieder die ursprüngliche Buchstabenfolge und somit auch der Klartext.

$$D_{\varphi^{-1}}(c) = \varphi^{-1}(c_1) \ \ldots \ \varphi^{-1}(c_r) = p_1 \ \ldots \ p_r = p$$

Da sich der Entschlüsselungsschlüssel k_d direkt aus dem Verschlüsselungsschlüssel k_e berechnen lässt ($k_d = {k_e}^{-1}$), ist die monoalphabetische Substitution ein symmetrisches Verschlüsselungsverfahren.

3.1.2 Verschiebechiffre

Die *Verschiebechiffre* ist ein besonders einfacher Fall der monoalphabetischen Substitution. Bei ihr wird jeder einzelne Buchstabe durch den Buchstaben ersetzt, der eine bestimmte Anzahl Positionen weiter hinten im Alphabet steht.

Man kann sagen, jeder Buchstabe wird um eine bestimmte Anzahl Positionen verschoben. Der Schlüssel bestimmt die Anzahl der Positionen, um die die Buchstaben verschoben werden.

Ist die Anzahl der Positionen, um die die Buchstaben verschoben werden 3, so spricht man von der *Caesarchiffre*. Dies kommt daher, dass schon der römische Feldherr Gaius Julius Caesar die Verschiebechiffre für seine militärische Korrespondenz verwendet hat. Dabei hat er oft den in Abbildung 3.2 dargestellten Schlüssel verwendet, der einer Verschiebung des Alphabets um drei Buchstaben entspricht.

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

Abbildung 3.2: Das Alphabet in der unteren Zeile des Schlüssels ist um drei Stellen nach links verschoben. Die links fehlenden Buchstaben wurden rechts wieder hinzugefügt.

3.1.3 Sicherheit monoalphabetischer Substitutionen

Die monoalphabetische Substitution ist ein recht unsicheres Verschlüsselungsverfahren und die Verschiebechiffre eine besonders unsichere Variante davon.

Sofern man von einem Alphabet mit 26 Buchstaben ausgeht, gibt es bei der Verschiebechiffre lediglich 26 verschiedene Schlüssel. Davon sind jedoch nur 25 sinnvoll, da eine Verschiebung um 26 Buchstaben einer Verschiebung um 0 Buchstaben entspricht. Man kann eine mit diesem Verschlüsselungsverfahren verschlüsselte Nachricht sehr leicht durch Ausprobieren entziffern; spätestens nach 25 Versuchen hat man den Klartext vor sich liegen.

Bei der monoalphabetischen Substitution allgemein ist die Schlüsselmenge schon wesentlich grösser. Es gibt $26! \approx 4 * 10^{26}$ verschiedene Schlüssel. Die verschlüsselte Nachricht lässt sich also nicht mehr so einfach durch Ausprobieren entziffern.

Es gibt jedoch verschiedene Methoden, um auf den Klartext zu kommen, ohne dass alle Schlüssel durchprobiert werden müssen. Die monoalphabetische Substitution lässt sich mit relativ geringem zeitlichen Aufwand durch die Häufigkeitsanalyse und eine Mustersuche entziffern.

3.1.4 Häufigkeitsanalyse und Mustersuche

Bei der monoalphabetischen Substitution wird jeder Buchstaben durch einen anderen Buchstaben ersetzt. Da eine Verschlüsselung eindeutig umkehrbar sein muss, werden dabei nie zwei verschiedene Buchstaben durch denselben Buchstaben ersetzt. Das hat zur Folge, dass die Häufigkeit eines Buchstabens der Nachricht beim Verschlüsseln erhalten bleibt. Wenn also der Buchstabe `A` 10-mal im Klartext vorkommt und im Chiffretext durch den Buchstaben `B` ersetzt

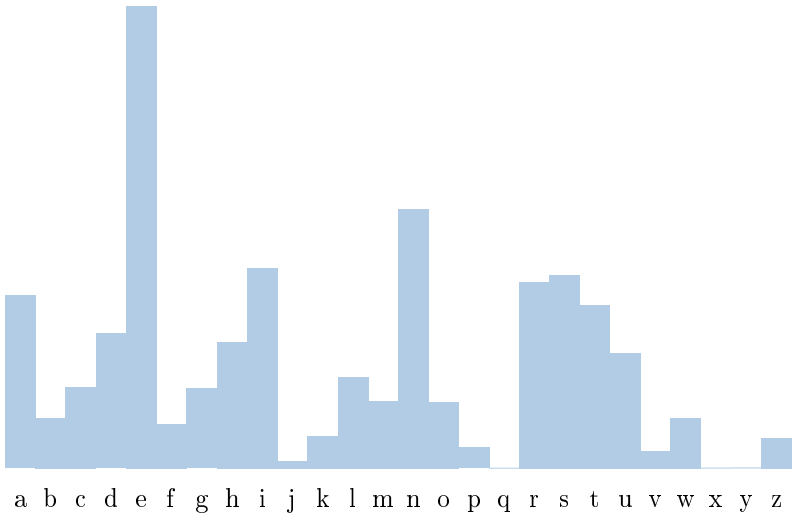

Abbildung 3.3: Die Häufigkeitsverteilung der Buchstaben der deutschen Sprache.

wird, folgt daraus, dass der Buchstabe `B` im Chiffretext auch 10-mal vorkommen muss.

In jeder Sprache treten die einzelnen Buchstaben in unterschiedlicher Häufigkeit auf. Wie in Abbildung 3.3 zu erkennen ist, kommt in der deutschen Sprache der Buchstabe `E` auffallend oft vor; Buchstaben wie `Q`, `X` oder `Y` hingegen äusserst selten.

Man kann also davon ausgehen, dass der im Chiffretext am meisten vorkommende Buchstabe dem Klartextbuchstaben `E` entspricht. Genauso lässt sich der dem zweithäufigsten Klartextbuchstaben `N` entsprechende Buchstabe mit relativ hoher Wahrscheinlichkeit bestimmen.

Die nächst häufigen Buchstaben `I`, `S`, `R` etc. lassen sich nur bei genügend grosser Chiffretextmenge bestimmen.

Ebenso wie einzelne Buchstaben lassen sich auch häufige Buchstabenpaare wie `EN`, `ER` oder `DE` sowie Buchstabentripel wie `SCH` oder `DER` im Chiffretext leicht erkennen.

Diese Methoden sind besonders bei längeren Chiffretexten sehr effektiv. Oft können mit diesen Methoden nicht alle Buchstaben bestimmt werden; die restlichen müssen dann aus dem Kontext erraten werden.

Es besteht jedoch die Möglichkeit, dass Buchstaben mit diesen Methoden falsch bestimmt werden. Besonders bei kürzeren Chiffretexten kommt dieses Problem zum Tragen.

3.2 Polyalphabetische Substitution

Der grösste Schwachpunkt der monoalphabetischen Substitution ist, dass jeder Buchstabe des Textes gleich verschlüsselt wird und somit häufige Buchstaben und Buchstabenmuster leicht erkannt werden können. Die polyalphabetische Verschlüsselung versucht, den Angriff durch Häufigkeitsanalyse und Mustersuche zu erschweren, indem nicht alle Buchstaben gleich verschlüsselt werden. Anstatt einem einzigen Geheimtextalphabet werden mehrere verschiedene Geheimtextalphabete verwendet.

Ähnlich wie bei der monoalphabetischen Verschlüsselung lässt sich das Übersetzen des Klartexts in den Chiffretext mit Hilfe mehrerer Geheimtextalphabete als Anwenden von Permutationen betrachten. Der Schlüssel besteht also aus einer bestimmten Anzahl l verschiedener Permutationen $\varphi_1, \ \dots \ , \varphi_l$.

Bevor der Klartext chiffriert werden kann, muss er in Buchstabenfolgen der Länge l eingeteilt werden. Wenn die Anzahl der Buchstaben des Klartexts nicht durch l teilbar ist, können folglich nicht alle Buchstabenfolgen die Länge l haben. In diesem Fall bildet man so viele Buchstabenfolgen der Länge l wie möglich und bildet mit den restlichen Buchstaben dann eine letzte, kürzere Buchstabenfolge.

Wenn man beispielsweise eine 100 Buchstaben lange Nachricht verschlüsseln will und als Schlüssel 6 verschiedene Permutationen gewählt hat, so teilt man diese in 16 Buchstabenfolgen mit jeweils 6 Buchstaben und erhält eine 17. Buchstabenfolge mit den restlichen 4 Buchstaben ($100 \div 6 = 16$ Rest 4).

Nachdem der Text in Buchstabenfolgen zerlegt und der Schlüssel gewählt worden ist, kann das eigentliche Verschlüsseln der Nachricht beginnen. Alle Buchstabenfolgen werden mit dem gleichen Verfahren verschlüsselt; jeder Buchstabe einer Buchstabenfolge jedoch mit einer anderen Permutation. Auf den ersten Buchstaben p_1 wird die erste Permutation φ_1 angewandt, auf den zweiten Buchstaben p_2 die zweite Permutation φ_2 usw.

$$E_{\varphi_1 \ \dots \ \varphi_l}(p) = \Big(\varphi_1(p_1) \ \dots \ \varphi_l(p_l)\Big) = c_1 \ \dots \ c_l = c$$

Daraus entstehen neue Buchstabenfolgen, die ebenfalls die Länge l haben. Diese Buchstabenfolgen aneinandergereiht bilden den Chiffretext.

Der Entschlüsslungsprozess erfolgt im Prinzip gleich, wie das Verschlüsseln. Der einzige Unterschied dabei ist, dass jeweils die inversen Permutationen $\varphi_1^{-1}, \ \dots \ , \varphi_l^{-1}$ der Permutationen $\varphi_1, \ \dots \ \varphi_l$ angewandt werden.

$$D_{\varphi_1^{-1} \ \dots \ \varphi_l^{-1}}(c) = \Big(\varphi_1^{-1}(c_1) \ \dots \ \varphi_l^{-1}(c_l)\Big) = p_1 \ \dots \ p_l = p$$

3.2.1 Sicherheit polyalphabetischer Substitutionen

Die Anzahl der möglichen Schlüssel m hängt von der Länge des Alphabets n und der Anzahl der verwendeten Permutationen l ab:

$$m = (n!)^l$$

Bei einem Alphabet mit 26 Buchstaben und 6 verwendeten Permutationen würde die Anzahl der möglichen Schlüssel also bei $(26!)^6 \approx 4.3{*}10^{159}$ liegen. Die Zahl der möglichen Permutationen hat in diesem Fall unglaubliche 159 Stellen. Um sich der Grösse solcher Zahlen bewusst zu werden, vergleicht man diese gerne mit dem Alter des Universums. Im Vergleich mit dieser Zahl scheint das Universum mit einem Alter von 13.7 Milliarden Jahren $\approx 4.3 * 10^{17}$ Sekunden noch relativ jung zu sein.

Die Sicherheit des Verfahrens verhält sich proportional zur Anzahl l der verwendeten Permutationen: Je mehr Permutationen verwendet werden, desto sicherer wird das Verschlüsselungsverfahren. Umgekehrt verliert das Verschlüsselungsverfahren an Sicherheit, wenn weniger Permutationen verwendet werden. Dies hat damit zu tun, dass es bei einer grösseren Anzahl Permutationen länger dauert, bis sich das Verschlüsselungsmuster wiederholt, als wenn nur wenige Permutationen verwendet werden. Die Periodenlänge, nach der sich das Verschlüsselungsmuster wiederholt, entspricht der Anzahl l der Permutationen. Falls l gleich 1 ist, oder alle Permutationen $\varphi_1, \ldots, \varphi_l$ identisch sind, entspricht die Verschlüsselung einer monoalphabetischen Substitution.

Teilt man den Chiffretext in Stücke der Länge l, so erhält man Buchstabenfolgen, die alle eine Gemeinsamkeit haben: Der erste Buchstabe jeder Buchstabenfolge wurde mit der Permutation φ_1 verschlüsselt. Genauso wurden alle Buchstaben an zweiter Stelle mit φ_2, diejenigen an dritter Stelle mit φ_3 usw. verschlüsselt. Das bedeutet, dass alle Buchstaben an der Position $n * l + a$ im Chiffretext mit der selben Permutation φ_a – also mit einer monoalphabetischen Substitution – verschlüsselt wurden.

Die polyalphabetische Substitution lässt sich also auch mit der Häufigkeitsanalyse entziffern. Im Unterschied zur monoalphabetischen Substitution kann der Chiffretext jedoch nicht als Ganzes analysiert werden, sondern lediglich die Buchstaben, die jeweils mit der gleichen Permutation verschlüsselt wurden. Es müssen daher l Häufigkeitsanalysen durchgeführt werden, bis der Chiffretext vollständig entschlüsselt ist. Die Schwierigkeit liegt darin, die Periodenlänge l zu bestimmen.

Kapitel 4

Die Enigma

Die Enigma ist eine elektromechanische Chiffriermaschine, die vor allem durch das deutsche Militär nach dem Ersten Weltkrieg und während des Zweiten Weltkrieges Verwendung fand.

4.1 Funktionsweise der Enigma

Die Enigma besteht im Wesentlichen aus einer Tastatur, einer Verschlüsselungseinheit und einem Lampenfeld. Alle 26 Tasten der Tastatur sind mit einer der 26 Lampen des Lampenfelds verdrahtet, so dass bei jedem Tastendruck eine Lampe aufleuchtet.

Die Verdrahtungen von Tastatur und Lampenfeld führen durch die Verschlüsselungseinheit, welche sich aus mehreren Walzen, einer Umkehrwalze und einem Steckerbrett zusammensetzt. Durch die Verdrahtung werden die Buchstaben des Alphabets miteinander vertauscht. Dieses Vertauschen ist das Verschlüsseln der Enigma.

Das Besondere an der Enigma ist, dass sich die Verdrahtung der Verschlüsselungseinheit bei jedem Tastendruck verändert. So leuchtet bei mehrmaligem Drücken auf die gleiche Taste immer ein anderes Lämpchen auf.

Um die Funktionsweise der Enigma verstehen zu können, muss man die Elemente der Enigma, insbesondere diejenige der Verschlüsselungseinheit, und deren Funktionen sowie die Zusammenhänge zwischen den einzelnen Elementen kennen.

4.1.1 Die Walzen

Die *Walzen* sind das Herzstück der Enigma. Eine Enigma verfügt über einen Walzensatz von drei drehbar angeordneten Walzen. Es gab aber auch Enigma-

Abbildung 4.1: Eine Enigma ohne Abdeckung. Hinter der Tastatur befindet sich das Lampenfeld. Hinter dem Lampenfeld sieht man die drei Walzen; links davon die Umkehrwalze. An der Vorderseite der Enigma befindet sich das Steckerbrett.

Abbildung 4.2: Zwei Walzen der Enigma. Man erkennt gut die 26 elektrischen Kontakte, sowie den beschrifteten Ring und das Zahnrad für die Fortschaltung der Walze.

Varianten, die über mehr als drei Walzen verfügten. Die in den deutschen U-Booten eingesetzte Enigma hatte zum Beispiel 4 Walzen.

Jede dieser Walzen weist auf beiden Seiten für jeden der 26 Buchstaben des lateinischen Alphabets einen elektrischen Kontakt auf. Diese Kontakte sind nach einem festen, unregelmässigen Muster miteinander verdrahtet, so dass jeder Kontakt auf der einen Seite mit einem Kontakt auf der anderen Seite verbunden ist. Diese Verdrahtung ist von Walze zu Walze verschieden.

Fliesst bei einem Verschlüsselungsvorgang elektrischer Strom durch eine Walze, so tritt dieser durch einen bestimmten Kontakt in die Walze ein, durchläuft die Verdrahtung und verlässt die Walze auf der anderen Seite durch einen anderen Kontakt.

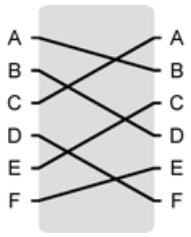

Abbildung 4.3: Vereinfachte schematische Darstellung der Verdrahtung einer Walze mit nur 6 Buchstaben. Der Buchstabe `A` ist mit `B` verdrahtet. Ebenso ist `B` mit `D`, `C` mit `A`, `D` mit `F`, `E` mit `C` und `F` mit `E` verdrahtet.

Für die Verschlüsselung bedeutet dies ein Vertauschen der Buchstaben des Alphabets. Die Verdrahtung einer einzelnen Walze entspricht einer monoalphabetischen Substitution.

Bei einem Verschlüsselungsvorgang fliesst der elektrische Strom jedoch nicht nur durch eine Walze, sondern der Reihe nach durch alle Walzen des Walzensatzes. Da jede einzelne Walze die Buchstaben des Alphabets miteinander vertauscht, vertauscht auch der ganze Walzensatz die Buchstaben des Alphabets. Dieses Vertauschen setzt sich aus den Substitutionen der einzelnen Walzen zusammen.

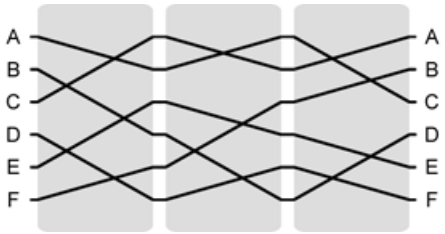

Abbildung 4.4: Schematische Darstellung der Verdrahtung drei hintereinander liegender Walzen.

Wie bereits angedeutet können sich die Walzen der Enigma drehen. Dabei werden die Walzen in Schritten von $\frac{1}{26}$ einer ganzen Umdrehung weitergedreht,

da dies genau der Drehung um einen Buchstaben entspricht. Auf einem äusseren Ring der Walzen sind die Zahlen von 1 bis 26 abgebildet, so dass durch ein kleines Fensterchen an der Enigma die aktuellen Walzenstellungen abgelesen werden können.

Die Drehung einer oder mehrerer Walzen bewirkt eine Veränderung der Verschlüsselung. Da sich die Walzen nach jedem Tastendruck ähnlich wie ein mechanischer Kilometerzähler weiter drehen, wird jeder Buchstabe einer Nachricht mit einer anderen Verschlüsselung verschlüsselt.

Die Anfangstellungen der Walzen, sind Teil des Schlüssels. Sie bestimmen, mit welchen Walzenstellungen der erste Buchstabe einer Nachricht verschlüsselt wird. Zudem zählt die Walzenlage – das heisst die Reihenfolge, in der die Walzen angeordnet sind – auch als Teil des Schlüssels.

Die Verschlüsselung der Enigma ist im Prinzip nichts anderes als eine polyalphabetische Substitution. Da es sehr lange geht, bis alle Walzen wieder ihre Anfangsstellungen einnehmen, ist die Periodenlänge der Verschlüsselung sehr gross, so dass im Normalfall kein sich wiederholendes Verschlüsslungsmuster zu erkennen ist.

4.1.2 Die Ringstellungen

Der äussere Ring einer Walze verfügt über eine Übertragungskerbe. Diese Kerbe bewirkt, dass durch einen ausgeklügelten Mechanismus beim Drehen der Walze immer an einer bestimmten Stelle die nächste Walze mitgedreht wird. Dadurch entsteht die kilometerzählerartige Fortschaltung der Walzen.

Diese Ringe sind verstellbar. Wird der Ring einer Walze verstellt, wird dadurch die innere Verdrahtung gegenüber der Übertragungskerbe und der Buchstabenanzeige auf dem Ring gedreht. Die Fortschaltung der Walzen wird also durch das Verändern einer Ringstellung geändert.

Die *Ringstellungen* der einzelnen Walzen sind ebenfalls Teil des Schlüssels.

4.1.3 Die Umkehrwalze

Nebst den Walzen ist auch eine *Umkehrwalze* ein wichtiger Bestandteil der Enigma.

Der bedeutende Unterschied zwischen der Umkehrwalze und einer normalen Walze ist, dass die Umkehrwalze nur auf einer Seite 26 Kontakte aufweist. Diese Kontakte sind jeweils paarweise miteinander verdrahtet. Zudem kann sich die Umkehrwalze nicht drehen.

Der Strom tritt, nachdem er die drei Walzen passiert hat, in die Umkehrwalze ein. Da alle Kontakte auf der gleichen Seite liegen, verlässt er die Umkehrwalze wieder auf der gleichen Seite. Danach fliesst er ein zweites Mal – in umgekehrter

Richtung – durch alle drei Walzen des Walzensatzes. Daher hat die Umkehrwalze auch ihren Namen.

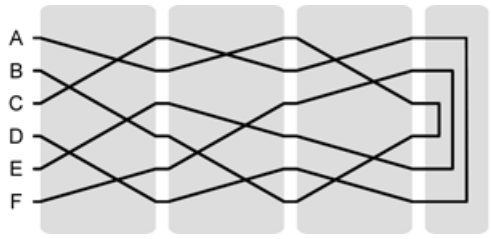

Abbildung 4.5: Schematische Darstellung der Verdrahtung der drei Walzen mit der Umkehrwalze (rechts). Durch die Umkehrwalze werden die Buchstaben jeweils paarweise miteinander verdrahtet.

Wie man aus der Abbildung 4.5 herauslesen kann, wird durch die Umkehrwalze die Verschlüsselung entscheidend verändert: Wird mit einer bestimmten Walzenstellung ein Buchstabe `A` in ein `B` verschlüsselt, so wird mit der gleichen Walzenstellung auch der Buchstabe `B` in ein `A` verschlüsselt. Auf die damit zusammenhängenden Konsequenzen werde ich später noch eingehen.

4.1.4 Das Steckerbrett

Das *Steckerbrett* liegt zwischen der Tastatur und den Walzen und erlaubt es dem Benutzer, durch das Setzen einzelner *Stecker* Buchstaben paarweise miteinander zu vertauschen.

Ein Grund, warum das Steckerbrett in die Enigma eingebaut wurde war, dass dies die Anzahl möglicher Schlüssel enorm vergrösserte wurde (siehe Kapitel 4.5.1).

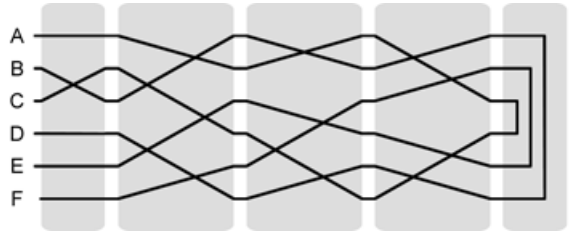

Abbildung 4.6: Schematische Darstellung der Verdrahtung der Walzen, der Umkehrwalze und des Steckerbretts (links). Es ist ein Stecker gesetzt, der die Buchstaben `B` und `C` miteinander vertauschen.

4.2 Historischer Hintergrund der Enigma

Zu Beginn des 20. Jahrhunderts kamen drei Erfinder aus verschiedenen Ländern unabhängig voneinander und fast gleichzeitig auf die Idee, eine Chiffriermaschine mit rotierenden Walzen zu bauen. Einer von ihnen war der deutsche Erfinder und Unternehmer Arthur Scherbius (1878-1929). Dieser reichte am 23. Februar 1918 sein Patent für eine Verschlüsselungsmaschine nach dem Walzenprinzip ein. Diese Verschlüsselungsmaschine nannte er *Enigma*. Das Wort Enigma kommt aus dem Griechischen und bedeutet Rätsel.

Scherbius war von der Sicherheit der Enigma überzeugt. Er erhoffte sich durch die kryptologische Stärke eine grosse Nachfrage. Doch der hohe Preis schreckte die Käufer ab. Auch das deutsche Militär hatte anfangs keine Interesse an der Enigma.

4.2.1 Die Enigma kommt zum Einsatz

Winston Churchill veröffentlichte im Jahre 1923 sein Buch *The World Crisis* und beschrieb darin, wie die Briten während des Ersten Weltkriegs an kryptographisches Material der Deutschen gelangten und auch in der Lage waren, einige Funksprüche der deutschen Flotte zu entschlüsseln. Im selben Jahr veröffentlichte die Royal Navy ein Dokument, aus dem hervorging, dass die Alliierten sich dank dem Entschlüsseln von Nachrichten einen klaren strategischen Vorteil verschaffen konnten.

Um ein weiteres kryptographisches Desaster zu vermeiden, entschloss sich das deutsche Militär, die Enigma einzusetzen. Scherbius begann mit der Serienanfertigung der Maschine, so dass sie 1926 für militärische Zwecke eingesetzt werden konnte. Im Verlaufe der folgenden 20 Jahren kaufte das Militär über 30 000 Exemplare der Enigma. Doch gerade als der Vertrieb der Enigma einen Aufschwung verzeichnete, verunglückte Scherbius bei einem Kutschenunfall. Er konnte all die Erfolge und Misserfolge seiner Chiffriermaschine nicht mehr miterleben.

Auch in der Zeit nach dem Ersten Weltkrieg wurde der deutsche Funkverkehr von den Briten überwacht. Doch nachdem 1926 immer mehr Enigmas eingesetzt wurden, konnten zunehmend weniger Funksprüche entschlüsselt werden. Auch nachdem es den Alliierten gelang, ein Duplikat der Enigma zu bauen, blieben die Erfolge aus.

4.2.2 Erste Erfolge polnischer Kryptoanalytiker

Auch polnische Kryptoanalytiker bissen sich an den Funksprüchen der Deutschen die Zähne aus. Obwohl man lange Zeit glaubte, Sprachwissenschaftler wären die besten Kryptoanalytiker, stellte der polnische Geheimdienst drei Mathe-

matiker für das Entschlüsseln von Nachrichten ein. Einer dieser Mathematiker, Marian Rejewski, konzentrierte sich ausschliesslich auf die Enigma.

Angetrieben von der Angst einer Invasion, mit dem Scharfsinn der Mathematiker und den Ergebnissen der Spionage, versuchten sie verbissen, die deutschen Funksprüche zu entschlüsseln.

Der polnische Geheimdienst wusste, dass die Deutschen nebst einem täglich ändernden *Tagesschlüssel* auch einen sogenannten *Spruchschlüssel* benutzten. Dieser Spruchschlüssel, bestehend aus drei Buchstaben, gab die Walzenstellungen für die Chiffrierung der eigentlichen Nachricht an. Der Spruchschlüssel wurde beim Verschlüsseln zweimal hintereinander in die auf den Tagesschlüssel eingestellte Enigma eingetippt. Danach wurden die Walzen auf den Spruchschlüssel eingestellt und dann die Nachricht eingetippt. Der Nachricht gingen also zwei identische, mit dem Tagesschlüssel verschlüsselte Buchstabentripel voraus.

Schon bald erzielte Rejewski erste Erfolge. Er erkannte in den ersten 6 Buchstaben eine gewisse Systematik, die er später für das Bestimmen des verwendeten Schlüssels benutzen konnte. Des Weiteren entwickelte er eine Methode, mit der sich der Einfluss des Steckerbretts beim Ausprobieren der möglichen Schlüssel vernachlässigen liess.

Diese Erkenntnisse erlaubten ihm und seinen Mitarbeitern, die Tagesschlüssel auszuwerten und in einem Katalog aufzulisten. Nach einem Jahr mühseliger Arbeit war der polnische Geheimdienst in der Lage, den deutschen Funkverkehr zu lesen.

Als die Deutschen ihr Verfahren der Nachrichtenübermittlung leicht modifizierten, wurde sein Katalog nutzlos. Anstatt diesen umzuschreiben, entwarf er eine mechanische Maschine – die *Bombe* – die diesen Katalog ersetzen sollte. Diese Maschine ähnelte der Funktionsweise der Enigma und konnte in relativ kurzer Zeit alle Walzenstellungen prüfen. War die richtige Walzenstellung bestimmt, mussten nur noch die Steckerverbindungen herausgefunden werden, was keine grossen Schwierigkeiten mit sich brachte. Da mit 3 Walzen 6 verschiedene Walzenlagen möglich waren, wurden auch 6 verschiedene Maschinen gebaut. Mit diesen Bomben konnte der Tagesschlüssel in etwa zwei Stunden gefunden werden.

Wieso diese Maschine Bombe genannt wurde, ist unklar, doch man vermutet, dass dies auf das bombenartige Ticken der laufenden Maschine zurückzuführen ist.

Was Rejewski nicht wusste war, dass der Chef seines Dienstes, Major Gwido Langer, die ganze Zeit über die aktuellen Tagesschlüssel gehabt hatte. Die Vorenthaltung dieser Information hatte jedoch ihre Berechtigung; er wollte sich auf den Fall vorbereiten, dass die Tagesschlüssel nicht mehr durch Spionage zu eruieren gewesen wären.

Als die Deutschen Ende 1938 zwei weitere Walzen einführten und die Anzahl der verwendeten Stecker von 6 auf 10 erhöhten, waren die Kryptoanalytiker nicht mehr in der Lage, den Tagesschlüssel zu bestimmen.

1939 gab der polnische Geheimdienst das von ihm erlangte Wissen aus weiser Vorhersicht an die Alliierten weiter. Diese waren verblüfft als sie erfuhren, dass Polen ihnen etwa 10 Jahre voraus war. Besonders der französische Geheimdienst staunte nicht schlecht, denn dieser versorgte den polnischen Geheimdienst über die ganze Zeit hinweg mit den Informationen – im Glauben, diese wären nichts wert.

Zwei Wochen später, am 1. September 1930, begann mit dem Überfall der Deutschen auf Polen der Zweite Weltkrieg.

4.2.3 Bletchley Park

Nachdem die Alliierten 13 Jahre lang geglaubt hatten, es wäre nicht möglich, die Enigma-Verschlüsselung zu entziffern, wurde ihnen durch den polnischen Erfolg das Gegenteil bewiesen. Die Engländer bemühten sich nun, auch Mathematiker und Naturwissenschaftler einzustellen. In *Bletchley Park*, dem Sitz der Government Code and Cypher School, sollte von nun an auf Hochtouren an der Entschlüsselung des feindlichen Funkverkehrs gearbeitet werden. Anfangs arbeiteten etwa 200 Personen in Bletchley Park, später waren es 7 000.

Schon bald hatten sich die Wissenschaftler und Mathematiker in Bletchley Park die polnischen Methoden angeeignet. Da mehr Personal und Mittel vorhanden waren, konnte man auch mit den durch die grössere Walzenzahl gegebenen Anforderungen zurechtkommen. Die Entschlüsselung der Nachrichten lief wieder auf Hochtouren und im Laufe einiger Wochen sammelte sich eine gewaltige Bibliothek entschlüsselter Funksprüche an.

Britische Experten vermuteten, dass es nicht mehr lange dauern würde, bis die Deutschen bemerken würden, dass die Wiederholung des Spruchschlüssels am Anfang der Nachricht die Sicherheit der Enigma gefährdete und als entsprechende Massnahme diese nicht mehr wiederholen würden – was dann auch wirklich der Fall war.

Um sich auf diese Massnahme seitens der Deutschen vorzubereiten, wurde nach einer alternativen Angriffsmöglichkeit gesucht.

Alan Turing, ein britischer Logiker, Mathematiker und Kryptoanalytiker, bemerkte, dass in vielen entschlüsselten Nachrichten eine Systematik enthalten war, durch die es möglich war, Teile des Inhalt unentschlüsselter Meldungen vorauszusagen. Die Aufgabe war nun, durch vermutete Wörter, sogenannten *Cribs*, den Tagesschlüssel herauszufinden.

Turing konstruierte eine Maschine, die noch leistungsfähiger und ausgeklügelter als die polnische Bombe war. Mit der *Turing-Bombe* konnten die täglich

Abbildung 4.7: Hier in Bletchley Park arbeiteten während des Zweiten Weltkriegs 7 000 Personen an der Entschlüsselung von Nachrichten der Achsenmächte. Unter anderem wurden hier auch Enigma-Nachrichten entschlüsselt.

abgefangenen Funksprüche nach im deutschen Militärjargon üblichen Worten – wie zum Beispiel `OBERKOMMANDO` oder `KOMMANDEUR` – abgesucht werden.[1]

Kurz nachdem die Deutschen die Wiederholung des Spruchschlüssels aufgaben, wurde der erste Prototyp der Turing-Bombe am 10. Mai 1940 in Betrieb genommen. Die Maschine war viel langsamer als erwartet und benötigte bis zu einer Woche, um den Schlüssel zu finden. Bis am 8. August eine überarbeitete Version der Turing-Bombe ihre Dienste aufnahm, konnten nur wenige Nachrichten entschlüsselt werden. In den nächsten anderthalb Jahren wurden 15 weitere Bomben in Betrieb genommen. Unter der Voraussetzung einer richtiger Annahme, war eine Bombe in der Lage, den Schlüssel innerhalb einer Stunde zu bestimmen. Die Schwierigkeit des Entschlüsselns lag darin, die richtigen Cribs und deren Position im Chiffretext zu finden.

Die Entschlüsselung der vierwalzigen Enigma der deutschen Marine bereitete den Briten mehr Schwierigkeiten. Um beim Entschlüsseln bessere Chancen zu erhalten, wurden nicht nur geistige Anstrengungen unternommen: Beispielsweise wurden deutsche Schiffe durch Legen von Seeminen dazu veranlasst, den Briten schon bekannte Positionen zu funken, die dann als Cribs eingesetzt werden konnten. Auch wurden Schlüsselbücher bei Überfällen auf Schiffe und U-Boote erbeutet.

Um bei den Deutschen kein Misstrauen zu erwecken, mussten die durch Funksprüche erhaltenen Informationen jedoch mit Bedacht verwendet werden.

[1] Die genauere Funktionsweise der Turing-Bombe wird im Kapitel 4.6 beschrieben

4.2.4 Auswirkungen auf den Krieg

Die Deutschen waren sich einiger Schwachpunkte der Enigma bewusst, dachten aber, dass sich niemand diese enorme Mühe nehmen würde, die Funksprüche der Enigma zu entschlüsseln. Als eine Gruppe von Tank- und Versorgungsschiffen der Deutschen versenkt wurde, schöpften sie allerdings Verdacht. Eine Untersuchung wurde eingeleitet; man kam zu dem Schluss, dass die Verluste entweder reines Pech waren, oder die Schuld eines Spions. Eine erfolgreiche Entschlüsselung hielten die Deutschen für ausgeschlossen.

Man weiss, dass eine abgefangene Nachricht, aus der hervorging, dass die Deutschen eine Invasion zwischen Le Havre und Cherbourg vermuteten, die Alliierten im letzten Moment dazu veranlasste, ihre Pläne auf eine Landung in der Normandie zu ändern. Dadurch erlangten die Alliierten einen bedeutenden strategischen Vorteil. Wie weit die Auswirkungen der Enigma den Verlauf des Zweiten Weltkrieges prägten, lässt sich jedoch nur erahnen.

4.3 Die Mathematik der Enigma

Die Enigma scheint durch ihre sich ständig verändernde Verdrahtung, die sich im Wesentlichen aus mehreren sich drehenden Walzen und einer feststehenden Umkehrwalze zusammensetzt, die Buchstaben einer Nachricht willkürlich durch andere zu ersetzen. Doch hinter dem vermeintlichen Chaos verbergen sich klare Strukturen, die sich mit Kenntnissen aus der Gruppentheorie mathematisch festhalten lassen.

Genau darum wird es sich in den nächsten Abschnitten handeln: Anhand der 3-walzigen Enigma werden diese mathematischen Strukturen aufgezeigt und erklärt.

4.3.1 Walzen als Permutationen

Die innere Verdrahtung einer Walze der Enigma vertauscht die einzelnen Buchstaben des Alphabets nach einem festen Muster. Dieses Vertauschen weist die Eigenschaften einer Permutation auf. Die Verdrahtung der Walzen der Enigma können also als Permutationen $\alpha_1, \alpha_2, \alpha_3$ betrachtet werden. Jede dieser Permutationen vertauscht die 26 Buchstaben des lateinischen Alphabets.

Die Umkehrwalze ist ebenfalls eine Permutation β. Die Umkehrwalze vertauscht jeweils zwei Buchstaben miteinander. Das bedeutet, die Permutation besteht aus 13 disjunkten Zweierzyklen (Zyklus; siehe Anhang B.6) und hat folglich die Ordnung 2 (Ordnung von Gruppenelementen; siehe Anhang B.3). Das hat zur Folge, dass die Permutation zugleich ihre inverse Permutation ist und keine Fixpunkte hat (Fixpunkt; siehe Anhang B.9). Man spricht von einer fixpunktfreien involutorischen Permutation. Diese Eigenschaften der Umkehrwalze sind für die Chiffrierung der Enigma von grosser Bedeutung und zugleich auch ihr grösster Schwachpunkt (siehe Kapitel 4.3.6 und Kapitel 4.4.1).

Genau wie die Walzen und die Umkehrwalze lässt sich auch das Steckerbrett als Permutation δ betrachten. Wenn kein Stecker gesteckt ist, entspricht die Permutation der Identität. Ansonsten besteht die Permutation aus n Zweierzyklen; wobei n die Anzahl der gesteckten Stecker ist. Wie die Permutation der Umkehrwalze ist diejenige des Steckerbretts involutorisch.

4.3.2 Zusammenspiel der Walzen

Bei einem Verschlüsselungsvorgang fliesst der Strom in einer bestimmten Reihenfolge durch die Walzen, die Umkehrwalze und das Steckerbrett. Daraus lässt sich schliessen, dass die Chiffrierung der Enigma aus einer Hintereinanderausführung – einer Komposition – der Permutationen der Walzen besteht (Komposition von Permutationen; siehe Anhang B.5).

Um herauszufinden, wie die einzelnen Permutationen zusammenhängen, untersucht man am besten, was genau beim Chiffrieren eines Buchstabens in der Enigma vorgeht.

Wenn ein Buchstabe mit der Enigma verschlüsselt wird, dann geht der durch den Tastendruck ausgelöste Stromfluss zuerst durch das Steckerbrett δ und die drei Walzen $\alpha_1, \alpha_2, \alpha_3$. Danach leitet die Umkehrwalze β den Strom zurück durch die drei Walzen und das Steckerbrett; dabei fliesst der Strom in umgekehrter Richtung und Reihenfolge durch die Walzen und das Steckerbrett. Wenn der Strom in umgekehrter Richtung durch die Walzen fliesst, entspricht das der jeweiligen inversen Permutation $\alpha_3^{-1}, \alpha_2^{-1}, \alpha_1^{-1}$. Dies mag im ersten Moment vielleicht nicht nachvollziehbar sein, doch wenn man die durch die Verdrahtung einer Walze gegebene Abbildungsvorschrift untersucht, wird man feststellen, dass es zutrifft (siehe Abbildung 4.3).

Genauso entspricht das Steckerbrett seiner inversen Permutation δ^{-1}, wenn der Strom in umgekehrter Richtung durchfliesst. Dies ist jedoch nicht von Bedeutung, da die Permutation δ ihre eigene inverse Permutation δ^{-1} ist.

Wenn man von der Rotation der Walzen absieht und davon ausgeht, dass alle Walzen in ihrer ungedrehten Stellung bleiben, dann würde die Chiffrierung E der Enigma folgender Komposition entsprechen (beachte, dass die Komposition von hinten nach vorne gelesen wird! siehe dazu Anhang B.5):

$$E = \delta^{-1}\ \alpha_1^{-1}\ \alpha_2^{-1}\ \alpha_3^{-1}\ \beta\ \alpha_3\ \alpha_2\ \alpha_1\ \delta$$

Die Chiffrierung E ist demnach zur Permutation β der Umkehrwalze konjugiert (Konjugation; siehe Anhang B.8); wie später noch erklärt wird, ist dadurch die gesamte Chiffrierung E auch – wie die Umkehrwalze – involutorisch und fixpunktfrei.

4.3.3 Rotation der Walzen

Im nächsten Schritt gilt es nun herauszufinden, wie sich die Rotation der Walzen auf die einzelnen Permutationen und die resultierende Permutation auswirkt.

Wenn eine Walze um eine Stelle gedreht wird, dann verschiebt sich mit ihr auch ihre innere Verdrahtung um eine Stelle. Das hat zur Folge, dass nun jeder Buchstabe so permutiert wird, wie sein nachstehender Buchstabe im Alphabet in der ungedrehten Stellung der Walze permutiert werden würde.

Um zu erreichen, dass die Permutation einen Buchstaben wie beschrieben permutiert, wird auf diesen Buchstaben zunächst eine zyklische Permutation ρ angewandt, die jeden Buchstaben auf seinen nachstehenden Buchstaben abbildet. Wenn jetzt die Permutation α einer Walze auf ihn angewandt wird, wird dieser entsprechend – wie sein nachstehender Buchstabe – permutiert. Das daraus hervorgehende Ergebnis ist nun aber um einen Buchstaben im Alphabet

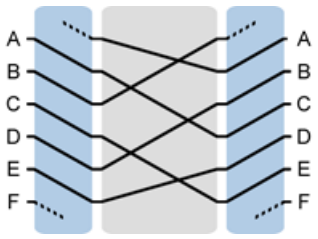

Abbildung 4.8: Durch das Verschieben der Buchstaben (blau) vor und nach der Walze wird erreicht, dass ein Buchstabe so permutiert wird, wie wenn die Walze um eine Stellung gedreht wäre.

verschoben. Um dies zu korrigieren, wird zusätzlich noch die inverse Permutation ρ^{-1} angewandt, welche das Ergebnis um einen Buchstaben zurück verschiebt.

Wenn die Walze α um n Stellen gedreht wird, dann wird jeder Buchstabe so permutiert wie der Buchstabe, der n Stellen nach ihm im Alphabet, in der ungedrehten Stellung der Walze permutiert werden würde. Der Buchstabe muss also bevor er mit der Permutation α der Walze permutiert wird, um n Stellen verschoben werden. Dies geschieht indem man die zyklische Permutation ρ anstatt einmal n-mal auf ihn anwendet (ρ^n). Genauso wird auch die inverse Permutation ρ^{-1} n-mal angewandt (ρ^{-n}), um den Buchstaben wieder um n Stellen zurück zu verschieben.

Demnach sieht die Permutation einer Walze unter Berücksichtigung ihrer Drehung um n Stellungen folgendermassen aus:

$$\rho^{-n}\alpha\rho^{n}$$

Die inverse Permutation davon sieht ähnlich aus. Im Endeffekt wird lediglich die Permutation α durch ihre inverse Permutation α^{-1} ersetzt.

$$\left(\rho^{-n}\alpha\rho^{n}\right)^{-1} = \left(\rho^{n}\right)^{-1}\alpha^{-1}\left(\rho^{-n}\right)^{-1} = \rho^{-n}\alpha^{-1}\rho^{n}$$

Die Komposition der Permutationen der drei Walzen unter Berücksichtigung ihrer Drehung sieht dann folgendermassen aus:

$$\rho^{-n_3}\alpha_3\rho^{n_3}\ \rho^{-n_2}\alpha_2\rho^{n_2}\ \rho^{-n_1}\alpha_1\rho^{n_1}$$

Da die Walzen unterschiedliche Stellungen einnehmen können, unterscheidet man die Drehungen n_1, n_2, n_3 der einzelnen Walzen voneinander.

Die Chiffrierung der Enigma verändert sich mit den Stellungen der Walzen. Die Chiffrierung E_n steht für die Chiffrierung mit bestimmten Walzenstellungen:

$$E_n = \delta^{-1}\ \rho^{-n_3}\alpha_3^{-1}\rho^{n_3}\ \rho^{-n_2}\alpha_2^{-1}\rho^{n_2}\ \rho^{-n_1}\alpha_1^{-1}\rho^{n_1}\ \beta\ \rho^{-n_3}\alpha_3\rho^{n_3}\ \rho^{-n_2}\alpha_2\rho^{n_2}\ \rho^{-n_1}\alpha_1\rho^{n_1}\ \delta$$

Auch diese Chiffrierung E_n ist zur Permutation β der Umkehrwalze konjugiert.

Zu jeder Chiffrierung E_n existiert genau eine dazugehörige Walzenstellung. Die Funktion $f(n)$ sei eine Funktion, mit der sich zu jedem n die dazugehörige Walzenstellung (n_1, n_2, n_3) ausrechnen lässt.

$$f(n) \;=\; (n_1, n_2, n_3)$$

Durch die 26-adische Darstellung von n mit den Walzenstellungen n_1, n_2 und n_3 lässt sich jeder Chiffrierung E_n eindeutig eine Walzenstellung zuweisen:

$$n \;\equiv\; n_1 + n_2 * 26 + n_3 * 26^2$$

Umgekehrt lässt sich auch aus jedem n die Stellungen der einzelnen Walzen errechnen:

$$\begin{aligned} n_1 &\equiv n \mod 26 \\ n_2 &\equiv \left\lfloor \frac{n}{26} \right\rfloor \mod 26 \\ n_2 &\equiv \left\lfloor \frac{n}{26^2} \right\rfloor \mod 26 \end{aligned}$$

Die Drehung n_1 der ersten Walze lässt sich am einfachsten ermitteln; man muss lediglich n modulo 26 rechnen (Modulo; siehe Anhang A.4).

Die Drehung n_2 der zweiten Walze lässt sich nicht ganz so einfach ausrechnen; bevor modulo 26 gerechnet wird, muss n zuerst durch 26 geteilt und abgerundet werden (in obiger Formel mittels der Gaussklammer; siehe Anhang A.3).

Die Drehung n_3 der dritten Walze wird ähnlich wie die Drehung der zweiten Walze ausgerechnet; der einzige Unterschied dabei ist, dass durch 26^2 geteilt wird.

Das Einstellen der Walzenstellungen vor dem Verschlüsseln legt fest, mit welchem E_n der erste Buchstabe der Nachricht verschlüsselt wird.

Wenn beispielsweise die Walzen in den Walzenstellungen $n_1 = 12, n_2 = 15$ und $n_3 = 6$ gebracht werden, dann wird der erste Buchstabe mit der Chiffrierung E_{4458} verschlüsselt $(12 + 15 * 26 + 6 * 26^2 = 4458)$.

4.3.4 Fortschaltung der Walzen

Wie in Kapitel 4.1.2 erklärt wurde, ist die Kerbe im Ring der Walze dafür verantwortlich, dass nach gewisser Walzendrehung die nächste Walze um eine Stelle gedreht wird.

Geht man davon aus, dass alle Ringe so eingestellt sind, dass immer am Ende einer vollen Umdrehung die nächste Walze weitergedreht wird, so folgt auf jede Chiffrierung E_n die nachfolgende Chiffrierung E_{n+1}:

$$\begin{aligned}
f(0) &= (0,0,0) &: E_0\\
f(1) &= (1,0,0) &: E_1\\
&\vdots\\
f(24) &= (24,0,0) &: E_{24}\\
f(25) &= (25,0,0) &: E_{25}\\
f(26) &= (0,1,0) &: E_{26}\\
f(27) &= (1,1,0) &: E_{27}\\
&\vdots
\end{aligned}$$

Der Buchstabe an Stelle p der Nachricht wird also mit der Chiffrierung E_{n+p} verschlüsselt. Man kann sagen, dass die Enigma unter diesen Umständen während des Verschlüsselns einer Nachricht die unterschiedlichen Chiffrierungen E_i in „richtiger“ Reihenfolge durchläuft.

Um die Walzenstellungen der Chiffrierung des Buchstabens an Stelle p der Nachricht auszurechnen, muss man also $p+n$ in die Funktion f einsetzen:

$$f(n+p) = (n_1, n_2, n_3)$$

Dabei steht n für die Anfangsstellung der Walzen.

4.3.5 Einfluss der Ringstellungen

Wenn eine Ringstellung einer Walze verändert wird, dann dreht im Prinzip die innere Verdrahtung dieser Walze. Man kann also sagen, dass die Permutation einer Walze mit Ringstellung r_0 der Permutation der um r_0 Stellen gedrehten Walze entspricht.

Addiert man zu den mit der Funktion f erlangten Walzenstellungen die Ringstellungen $r = (r_1, r_2, r_3)$, erhält man die Walzenstellungen unter Berücksichtigung der Ringstellungen. Die Funktion f_r der Walzenstellungen unter Berücksichtigung der Ringstellungen sieht demnach folgendermassen aus:

$$f_r(n+p) = f(n+p) + r$$

Wie sich dadurch die Verschlüsselung der Chiffrierung E_{n+p} ändert, lässt sich am einfachsten an einem konkreten Beispiel untersuchen. Verwendet man die Ringstellungen $r = (25, 0, 0)$, erhält man folgende Ergebnisse:

$$\begin{aligned}
f(0) = (0,0,0) &\rightarrow f_r(0) = (25,0,0) &: E_{25} \\
f(1) = (1,0,0) &\rightarrow f_r(1) = (0,0,0) &: E_0 \\
&\vdots \\
f(25) = (25,0,0) &\rightarrow f_r(25) = (24,0,0) &: E_{24} \\
f(26) = (0,1,0) &\rightarrow f_r(26) = (25,1,0) &: E_{51} \\
f(27) = (1,1,0) &\rightarrow f_r(27) = (0,1,0) &: E_{26} \\
f(28) = (2,1,0) &\rightarrow f_r(28) = (1,1,0) &: E_{27} \\
&\vdots
\end{aligned}$$

Durch den Einfluss der Ringstellungen ändert sich also die Durchlaufreihenfolge der verschiedenen Chiffrierungen E_i bei der Verschlüsselung einer Nachricht. Die Reihenfolge ändert sich jedoch nicht komplett; es werden lediglich Stücke der Reihenfolge miteinander vertauscht. Die Länge dieser Stücke variiert je nach Ringstellungen.

4.3.6 Involutorische Chiffre

In diesem Abschnitt geht es darum, zu zeigen, dass sich mit der Enigma Nachrichten bei gleichen Grundeinstellungen sowohl verschlüsseln, als auch wieder entschlüsseln lassen. Das bedeutet, dass die zweifache Anwendung des Verschlüsselungverfahrens der Identität entspricht.

Die zweifache Anwendung einer Abbildung ist genau dann die Identität, wenn die Abbildung ihrer inversen Abbildung entspricht, also eine involutorische Abbildung ist:

$$E_n = E_n^{-1} \quad \Leftrightarrow \quad E_n^2 = \mathrm{id}$$

Satz:
Die Enigma ist eine involutorische Chiffre.

Beweis:
Um folgende Überlegungen zu vereinfachen, fasst man am besten die Chiffrierung E_n der Enigma zusammen, indem man die Permutationen der Walzen und des Steckerbretts (nicht aber die der Umkehrwalze) durch die Permutation σ ersetzt:

$$\sigma_n \;:=\; \rho^{-n_3}\alpha_3\rho^{n_3}\;\rho^{-n_2}\alpha_2\rho^{n_2}\;\rho^{-n_1}\alpha_1\rho^{n_1}\;\delta$$

Die Chiffrierung E_n hat dann folgende Form:

$$E_n = \sigma_n^{-1}\beta\sigma_n$$

Diese Chiffrierung E_n ist wie früher schon erwähnt wurde zur Permutation β der Umkehrwalze konjugiert.

Wenn nun die Chiffrierung E_n involutorisch sein soll, so muss die zweifache Anwendung E_n^2 die Identität id ergeben:

$$\begin{aligned} E_n^2 = \left(\sigma_n^{-1}\beta\sigma_n\right)^2 &= \sigma_n^{-1}\beta\sigma_n\sigma_n^{-1}\beta\sigma_n \\ &= \sigma_n^{-1}\beta\beta\sigma_n \\ &= \sigma_n^{-1}\sigma_n \\ &= \mathrm{id} \end{aligned}$$

Da $\beta^2 = \mathrm{id}$, heben sich die verschiedenen Permutation gegenseitig auf, so dass am Schluss nur die Identität übrig bleibt. Damit ist bewiesen, dass die zweifache Anwendung der Chiffrierung E_n der Enigma der Identität entspricht und die Chiffrierung dadurch auch involutorisch ist. □

Wie obiger Beweis zeigt, ist die Chiffrierung E_n involutorisch, weil sie zur involutorischen Permutation β der Umkehrwalze konjugiert ist.

4.4 Kryptologische Schwachpunkte der Enigma

Durch das mathematische Analysieren eines Verschlüsselungsverfahren lassen sich Schwachpunkte und auch Stärken der dadurch gegebenen Strukturen festhalten; die theoretische Sicherheit des Verfahrens lässt sich bestimmen.

Genauso haben die Kryptoanalytiker während des Zweiten Weltkriegs die Sicherheit der Enigma untersucht und Schwachpunkte aufgedeckt. Wie schon angedeutet, ist die Umkehrwalze der grösste Schwachpunkt der Enigma und auch der Grund, warum die Alliierten während des Zweiten Weltkriegs in der Lage waren, den Nachrichtenverkehr des deutschen Militärs zu lesen.

4.4.1 Nachteile der Umkehrwalze

Die Enigma verschlüsselt Nachrichten, indem sie auf jeden Buchstaben der Nachricht eine Permutation der 26 Buchstaben des lateinischen Alphabets anwendet. Daher könnte man annehmen, dass die Anzahl m der von der Enigma zum Verschlüsseln verwendeten Permutationen $26! \approx 4.03 * 10^{26}$ (mehr als 400 Quadrillionen) beträgt.

Diese Annahme ist jedoch falsch: die Anzahl m der möglichen Permutationen ist deutlich geringer: Durch die Umkehrwalze sind alle mit der Enigma möglichen Permutationen involutorisch. Alle nicht involutorische Permutationen werden dadurch ausgeschlossen. Zudem entspricht ein chiffrierter Buchstabe niemals seinem Klartextbuchstaben. Das bedeutet, dass die Chiffrierung der Enig-

ma keine Fixpunkte aufweist, was wiederum eine Verringerung der möglichen Permutation bedeutet.

Satz:
Die Chiffrierung der Enigma weist keine Fixpunkte auf.

Beweis:
Nimmt man an, dass die Chiffrierung E_n der Enigma einen Fixpunkt a besitzt, so müsste die Chiffrierung E_n diesen auf sich selbst abbilden:

$$\begin{aligned} E_n(a) &= a \quad \Rightarrow \\ \left(\sigma_n^{-1}\beta\sigma_n\right)(a) &= a \quad \Rightarrow \\ \sigma_n^{-1}\Big(\beta\big(\sigma_n(a)\big)\Big) &= a \quad \Rightarrow \\ \beta\Big(\sigma_n(a)\Big) &= \sigma_n(a) \end{aligned}$$

Wenn das wahr wäre, so hätte die Permutation β der Umkehrwalze den Fixpunkt $\sigma(a)$. Da die Umkehrwalze aber wie schon erwähnt immer jeweils 2 Buchstaben miteinander vertauscht und dadurch fixpunktfrei ist, ist das ein Widerspruch und die Annahme daher falsch. Die Chiffrierung E_n besitzt also keine Fixpunkte. □

Eine Konsequenz der Tatsache, dass die Chiffrierung E_n keine Fixpunkte aufweist ist, dass ein Buchstabe nie in sich selbst verschlüsselt wird. Steht an einer Stelle im Chiffretext der Buchstabe `A`, so kann man mit Sicherheit sagen, dass der entsprechende Klartextbuchstaben kein `A` ist. Diese Erkenntnis mag unbedeutend erscheinen, war aber für das Entschlüsseln der Enigma von grosser Bedeutung.

Wenn man von allen möglichen Permutationen der 26 Buchstaben diejenigen weglässt, die entweder nicht involutorisch sind, oder einen Fixpunkt aufweisen, erhält man die Menge der Permutationen, die theoretisch von den Walzen der Enigma erzeugt werden könnten.

Satz:
Die Anzahl m dieser Permutationen ist:

$$m = \frac{(2n)!}{n!\ 2^n} = \frac{26!}{13!\ 2^{13}} \approx 7.91 * 10^{12}$$

Beweis:
Diese Formel ist ein Spezialfall einer allgemeinen Formel für die Anzahl Elemente

in einer Konjugationsklasse[2]. In vorliegendem Spezialfall kann man sie direkt verifizieren.

Eine Möglichkeit, die Formel zu verifizieren wäre, die Formel als kombinatorisches Problem zu betrachten: Die Chiffrierung der Enigma besteht aus dem Produkt 13 disjunkter Zweierzyklen. Es gibt 26! verschiedene Möglichkeiten, wie sich diese mit den 26 Buchstaben des Alphabets darstellen lassen: Man schreibt alle 26! möglichen Permutationen der 26 Buchstaben auf und setzt jeweils um ein Buchstabenpaar eine Klammer.

$$(AB)\,(CD)\,(EF)\,(GH)\,(IJ)\,(KL)\,(MN)\,(OP)\,(QR)\,(ST)\,(UV)\,(WX)\,(YZ)$$

Dabei entstehen aber auch viele Permutationen, die identisch sind. Es macht zum Beispiel keinen Unterschied, wenn zwei Buchstaben in einer Klammer miteinander vertauscht werden, da es ja keine Rolle spielt, ob A mit B oder B mit A vertauscht wird:

$$(AB) = (BA)$$

Demnach sind jeweils 2^{13} Permutationen identisch.

Zudem spielt es auch keine Rolle, in welcher Reihenfolge die Buchstabenpaare notiert werden:

$$(AB)\,(CD) = (CD)\,(AB)$$

Da es 13! Möglichkeiten gibt, die 13 Buchstabenpaare hintereinander zu schreiben, sind jeweils weitere 13! Permutationen identisch.

Jede dieser Permutation kommt also $13! \times n^{13}$-mal vor. Wenn man nun die 26! durch diese Zahl teilt, kommt man auf die Zahl der tatsächlich unterschiedlichen Permutationen, die sich aus 13 disjunkten Zweierzyklen bilden lassen. □

4.5 Kryptologische Stärken der Enigma

Die kryptologischen Stärken der Enigma sind im Wesentlichen auf den rotierenden Walzensatz im Zusammenhang mit dem Steckerbrett und den grossen Schlüsselraum (die Menge der möglichen Schlüssel) zurückzuführen.

Wie bereits erklärt sind die rotierenden Walzen des Walzensatzes für den polyalphabetischen Charakter der Verschlüsselung ausschlaggebend. Die Periodenlänge ist dabei aber so gross, dass erfolgreiche Angriffe durch Methoden wie die Häufigkeitsanalyse oder die Mustersuche in der Praxis unmöglich sind. Das Steckerbrett verhindert, dass man direkt durch Ausprobieren der Walzenstellungen den Schlüssel einer Nachricht bestimmen kann. Wie später in Kapitel 4.6.1 beschrieben wird, kann das Steckerbrett jedoch umgangen werden.

[2]Die Formel für die Anzahl der Elemente in der Konjugationsklasse einer Permutation findet man zum Beispiel im Buch: *W. Fulton, J. Harris: Representation Theory. Graduate Texts in Math. vol. 129, Springer-Verlag, 1991*

Der grosse Schlüsselraum verhindert, dass der Chiffretext durch systematisches Ausprobieren aller möglichen Schlüssel entschlüsselt werden kann.

4.5.1 Schlüsselraum der Enigma

Der Schlüssel der Enigma ist aus verschiedenen Einstellungen zusammengesetzt. Daher lässt sich die Grösse des Schlüsselraums nicht direkt berechnen; zuerst müssen die Anzahl der Möglichkeiten der einzelnen Einstellungen ausgerechnet und anschliessend miteinander multipliziert werden:

Walzenstellungen Jede Walze der Enigma kann in eine der 26 möglichen Stellungen gebracht werden. Daher existieren bei einer 3-walzigen Enigma $26 \times 26 \times 26$ Walzenstellungen:

$$26^3 = 17\,576$$

Ringstellung Jede Walze kann in eine der 26 möglichen Ringstellung gebracht werden. Die Zahl der möglichen Ringstellungen entspricht also den möglichen Walzenstellungen:

$$26^3 = 17\,576$$

Walzenlage Die drei Walzen lassen sich in 3! verschiedenen Reihenfolgen in die Enigma einsetzen:

$$3! = 6$$

Steckerbrett Die Zahl der Möglichkeiten, die sechs Stecker auf dem Steckerbrett zu stecken, ist relativ hoch. Beim Setzen des ersten Steckers hat man 325 Möglichkeiten zur Verfügung. Dies ist die Anzahl der Möglichkeiten, zwei Buchstaben aus den 26 Buchstaben des Alphabets auszuwählen. Ausgerechnet wird dies mittels des Binomialkoeffizienten (siehe Anhang A.2). Für jeden weiteren Stecker verringert sich die Zahl der Möglichkeiten: Für den zweiten Stecker stehen noch 24 Buchstaben zur Auswahl. Für den letzten der sechs Stecker stehen dann noch lediglich 16 Buchstaben zur Auswahl.

Da es keine Rolle spielt, welcher Stecker für welche der 6 Steckverbindungen genutzt wird, muss die Zahl, die man beim Multiplizieren der Steckmöglichkeiten jedes einzelnen Steckers erhält, durch 6! geteilt werden:

$$\frac{\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}}{6!} = 100\,391\,791\,500$$

Wenn man nun diese Zahlen miteinander multipliziert, erhält man die Grösse des Schlüsselraums.

$$17\,576 \times 17\,576 \times 6 \times 100\,391\,791\,500 = 186\,075\,649\,051\,516\,224\,000$$

Dabei ist zu beachten, dass sich, wenn man die Möglichkeit, die drei Walzen und die Umkehrwalze aus mehreren auszuwählen, berücksichtigt, der Schlüsselraum weiter vergrössert. Zudem ist unklar, ob einige dieser Schlüssel die gleiche Chiffrierung bewirken.

4.6 Die Turing-Bombe

Entscheidend für die Entschlüsselung der Enigma-Verschlüsselung ist die Tatsache, dass ein Buchstabe unabhängig von den bereits verschlüsselten Buchstaben verschlüsselt wird. Alle zur Entschlüsselung notwendigen Überlegungen basieren auf der Erkenntnis, dass die Verschlüsselung eines Buchstabens nur von den Anfangseinstellungen und der Position im Text abhängt.

So konnte Alan Turing beim Entwurf seiner Bombe alle durch die Enigma gegebenen Schwachpunkte ausnützen. In den folgenden Abschnitten soll das vereinfachte Prinzip und die grobe Funktionsweise erklärt werden.

4.6.1 Prinzip der Turing-Bombe

Um spätere Überlegungen in diesem Abschnitt zu vereinfachen, wird die Chiffrierung E_n aus Kapitel 4.3.3 zusammengefasst, indem die Permutationen der drei Walzen und diejenige der Umkehrwalze durch die Permutation φ_n ersetzt werden:

$$\varphi_n := \rho^{-n_3}\alpha_3^{-1}\rho^{n_3}\ \rho^{-n_2}\alpha_2^{-1}\rho^{n_2}\ \rho^{-n_1}\alpha_1^{-1}\rho^{n_1}\ \beta\ \rho^{-n_3}\alpha_3\rho^{n_3}\ \rho^{-n_2}\alpha_2\rho^{n_2}\ \rho^{-n_1}\alpha_1\rho^{n_1}$$

Die Chiffrierung E_n nimmt dadurch folgende Form an:

$$E_n = \delta^{-1}\varphi_n\delta$$

Das Prinzip der Turing-Bombe beruht auf der Kenntnis eines Cribs; das heisst, dass man mehrere Buchstaben an einer bestimmten Position der Nachricht kennt, oder vermutet. Die Turing-Bombe sucht dann nach allen Schlüsseln, die für diesen Crib in Frage kommen.

Am besten lässt sich das Prinzip anhand eines Beispiels erklären: Man vermutet zu drei aufeinander folgenden Buchstaben c_0, c_1, c_2 des Chiffretextes die dazugehörigen Klartextbuchstaben p_0, p_1, p_2. Der erste dieser Buchstaben steht an einer unbekannten, aber festen Position n des Textes. Die anderen Buchstaben stehen folglich an den Positionen $n+1$ und $n+2$.

Da die Ringstellungen die Durchlaufreihenfolge der verschiedenen Chiffrierungen E_i bei der Verschlüsselung einer Nachricht nur stückweise vertauscht (siehe Kapitel 4.3.5), kann man darauf spekulieren, dass – wenn der Buchstabe p_0 mit der Chiffrierung E_m verschlüsselt wird – die anderen beiden Buchstaben

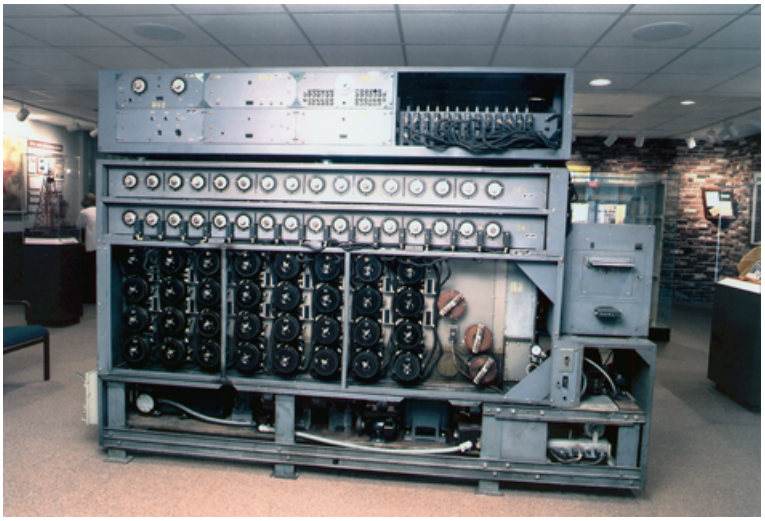

Abbildung 4.9: Die Hochgeschwindigkeitsvariante der Turing-Bombe, die speziell gegen die vierwalzigen Enigmas der deutschen U-Booten eingesetzt wurde.

p_1 und p_2 mit den darauf folgenden Chiffrierungen E_{m+1} und E_{m+2} verschlüsselt werden:

$$\begin{aligned} E_m\left(p_0\right) &= c_0 \\ E_{m+1}\left(p_1\right) &= c_1 \\ E_{m+2}\left(p_2\right) &= c_2 \end{aligned}$$

Befinden sich die Buchstaben an einer Stelle im Text, wo die Reihenfolge der Chiffrierung wegen der Ringstellungen unterbrochen wird, ist dies nicht der Fall und ein anderer Crib muss als Angriffspunkt gefunden werden.

Turing hat seine Bombe so konstruiert, dass die Permutation des Steckerbretts nicht berücksichtigt werden muss. Dazu muss der Crib jedoch spezielle Voraussetzungen erfüllen: Jeder Buchstabe des Cribs muss in seinen nachstehenden Buchstaben verschlüsselt werden. Der letzte Buchstabe muss dann in den ersten Buchstaben verschlüsselt werden:

$$\begin{aligned} E_m\left(p_0\right) &= p_1 \\ E_{m+1}\left(p_1\right) &= p_2 \\ E_{m+2}\left(p_2\right) &= p_0 \end{aligned}$$

Dadurch bildet der Crib so etwas wie eine Schleife. Das Ganze lässt sich dann auch folgendermassen notieren und umformen:

$$\begin{aligned} E_{m+2}\left(E_{m+1}\left(E_m\left(p_0\right)\right)\right) &= p_0 \\ \delta^{-1}\varphi_{m+2}\delta\ \delta^{-1}\varphi_{m+1}\delta\ \delta^{-1}\varphi_m\delta\ \left(p_0\right) &= p_0 \\ \varphi_{m+2}\delta\ \delta^{-1}\varphi_{m+1}\delta\ \delta^{-1}\varphi_m\left(\delta\left(p_0\right)\right) &= \delta\left(p_0\right) \end{aligned}$$

Die einander folgenden Permutationen δ und δ^{-1} heben sich jeweils gegenseitig auf und können daher ohne weitere Konsequenzen weggelassen werden:

$$\varphi_{m+2}\varphi_{m+1}\varphi_m \ \ (\delta\,(p_0)) = \delta\,(p_0)$$

Die Turing-Bombe prüft nun, für welche der 17 576 Walzenstellungen die Komposition $\varphi_{m+2}\varphi_{m+1}\varphi_m$ den Buchstaben $\delta\,(p_0)$ nicht verändert. Da die Permutation des Steckerbretts δ nicht bekannt ist, ist $\delta\,(p_0)$ ein unbekannter Buchstabe. Es müssen also alle 26 Buchstaben des Alphabets geprüft werden.

Durch das Ignorieren der Ringstellungen und das Umgehen des Steckerbretts muss die Turing-Bombe lediglich alle 17 576 Walzenstellungen überprüfen. Geht man davon aus, dass pro Sekunde eine Walzenstellung geprüft werden kann, dauert das Prüfen aller Walzenstellungen knappe 5 Stunden ($\frac{17\,576}{60\times 60} \approx 4.88$).

Müssten alle 186 075 649 051 516 224 000 möglichen Schlüssel überprüft werden, wäre das selbst mit einem modernen Computer nicht zu bewältigen.

4.6.2 Funktionsweise der Turing-Bombe

Die Turing-Bombe verfügt über mehrere Enigma-Walzensätze. Bevor mit dem Überprüfen der Walzenstellungen begonnen werden kann, müssen die Walzensätze in richtige Ausgangslagen gebracht werden: Walzen werden so eingestellt, dass die Walzenstellungen jeweils der Position des vermuteten Buchstabens entsprechen. Für das Beispiel aus dem vorangehenden Kapitel müssten die Walzen auf die Chiffrierungen E_n, E_{n+1} und E_{n+2} eingestellt werden.

Durch das Verwenden von 3 Walzensätzen können die Walzenstellungen aller vermuteten Buchstaben gleichzeitig überprüft werden. Die Walzensätze sind so miteinander verdrahtet, dass immer wenn ein Buchstabe durch die Walzenstellungen nicht verändert wird, der Stromkreis des entsprechenden Buchstabens geschlossen und dadurch das Überprüfen der Walzenstellungen angehalten wird.

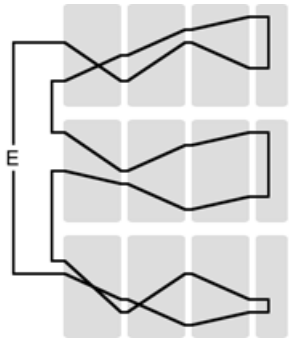

Abbildung 4.10: Stark vereinfachte schematische Darstellung der Turing-Bombe. Der Stromkreis für den Buchstaben E ist geschlossen. Somit ist eine mögliche Walzenstellung für die 3 vermuteten Buchstaben gefunden.

Die Walzenstellungen, die man bei einem erfolgreichem Durchlauf der Turing-Bombe erhält, sind die Walzenstellungen der entsprechenden Buchstaben der Nachricht. Mit der Kenntnis der Position des Cribs im Text lässt sich auf die Grundeinstellungen der Walzen, die für das Verschlüsseln der Nachricht verwendet wurde, zurückrechnen.

4.6.3 Position eines Cribs

Man weiss, dass mit der Enigma ein Buchstabe nie in sich selbst verschlüsselt wird. Daher können bestimmte Positionen des Cribs ausgeschlossen werden; und zwar genau die, an denen Kollisionen durch identische Klartext- und Chiffretextbuchstaben auftreten.

C	S	W	A	T	J	I	T	K	Y	H	M	N
P	O	S	I	**T**	I	O	N					
	P	O	S	I	T	**I**	O	N				
		P	O	S	I	T	I	O	N			
			P	O	S	**I**	**T**	I	O	N		
				P	O	S	I	T	I	O	N	
					P	O	S	I	T	I	O	**N**
C	S	W	A	T	J	I	T	K	Y	H	M	N

Abbildung 4.11: Das Wort `POSITION` kann aufgrund übereinstimmender Klartext- und Chiffretextbuchstaben (rot) an bestimmten Positionen im Chiffretext (grau) ausgeschlossen werden. So wird es bis auf 2 Positionen (blau) eingeschränkt.

Je länger die Cribs sind, desto mehr werden die möglichen Positionen dadurch eingeschränkt.

Kapitel 5

Moderne Verschlüsselungen

Da man mit dem Computer ältere Verschlüsslungsverfahren dank dessen unglaublicher Rechenfähigkeit mit Leichtigkeit entschlüsseln kann, war mit dem Einzug des Computers im 20. Jahrhundert eine neue Generation von Verschlüsselungsverfahren nötig.

Die Anforderungen an ein modernes Verschlüsslungsverfahren nehmen ganz andere Dimensionen an, als man es sich von den älteren Verfahren gewohnt ist. So gilt zum Beispiel ein Verschlüsslungsverfahren erst als sicher, wenn der Klartext und der Chiffretext bekannt sind und der Schlüssel dadurch trotzdem nicht bestimmt werden kann. Bei der Enigma wäre dies ein Kinderspiel.

Durch das Public-Key-Verfahren (asymmetrische Verschlüsselungen) sind Codebücher wie bei der Enigma heutzutage überflüssig. Ein solches Verfahren ist beispielsweise das nach seinen Erfindern Rivest, Shamir und Adleman benannte *RSA*-Verfahren.

Da Public-Key-Verfahren rechenintensiv sind, werden oft auch hybride Verschlüsselungsverfahren, die symmetrische und asymmetrische Verschlüsselungen miteinander kombinieren, eingesetzt. Dabei erfolgt die Schlüsselübertragung durch ein asymmetrisches Verfahren. Die eigentliche Nachricht wird dann zugunsten der Rechengeschwindigkeit mit einem symmetrischen Verfahren verschlüsselt. Ein bekanntes Beispiel für ein hybrides Verfahren ist *Pretty Good Privacy (PGP)*.

Die heutzutage gebräuchlichen Verschlüsslungsverfahren wurden alle durch genaue Untersuchungen auf ihre Sicherheit überprüft, doch kann bei keinem mit Sicherheit gesagt werden, dass es keine Schwachpunkte aufweise.

Werden in Zukunft noch viel leistungsfähigere Rechner – wie zum Beispiel der Quantencomputer – entwickelt, befürchtet man, dass man dadurch in der Lage wäre, erfolgreiche Brute-Force-Attacken auf heutzutage verbreitete Verschlüsslungsverfahren durchzuführen.

5.1 Data Encryption Standard (DES)

Der *Data Encryption Standard (DES)* ist ein symmetrisches Verschlüsselungsverfahren. Obwohl der DES heutzutage wegen seiner Schlüssellänge von nur 56 Bits für viele Anwendungen als zu unsicher betrachtet wird und bereits ein Nachfolger, der *Advanced Encryption Standard (AES)*, existiert, ist er ein gutes Beispiel für ein modernes Verschlüsselungsverfahren.

Der wesentliche Unterschied zu den klassischen Verfahren und der Enigma liegt darin, dass die Verschlüsselung eines Buchstabens nicht nur vom Schlüssel abhängt, sondern auch durch die bereits verschlüsselten Buchstaben beeinträchtigt wird. Die Komplexität des Verfahrens steigert sich dadurch enorm. Auch ist es dann unmöglich, durch Erraten von Textstellen einen Vorteil beim Entschlüsseln zu erlangen.

Nachwort

Rückblickend kann ich sagen, dass diese Abschlussarbeit in jeder Hinsicht ein Gewinn für mich war. Ich habe nicht nur Wissen zu den in meiner Arbeit behandelten Themen erlangt; vielmehr erlernte ich das selbständige Erarbeiten und Verfassen von Informationen wie auch den Umgang mit abstrakten Aufgabenstellungen. Zudem lernte ich während meiner Arbeit den Umgang mit LaTeX, eine Software, die sich speziell zum Erstellen wissenschaftlicher Texte mit mathematischen Formeln eignet, mit der ich meine Arbeit geschrieben habe.

Sowohl die Wahl des Mentors, sowie die eines mathematisch-kryptologischen Themas haben sich als richtig erwiesen. Dadurch habe ich, auch wenn die Arbeit hin und wieder anstrengend war und zum Teil nur stockend voranging, nie das Interesse und die Freude an meinem Thema verloren.

Im Verlaufe der Zeit hat sich die Vorstellung meiner Arbeit durch neue Erkenntnisse immer wieder verändert. Dennoch bin ich der Ansicht, dass ich – obwohl dadurch einige Teile anders ausgefallen sind als ich mir das anfänglich vorgestellt hatte – die Zielsetzung meiner Arbeit nicht verfehlt habe.

Anhang A

Elementare Zahlentheorie

A.1 Fakultät

Die *Fakultät* ist eine mathematische Funktion, die einer natürlichen Zahl $n \geq 0$ das Produkt aller natürlichen Zahlen von 1 bis n (n-Fakultät) zuordnet.

$$n! = \prod_{k=1}^{n} k = 1 * 2 * 3 * \cdots * n$$

Beispiel A.1:
$5! = 1 * 2 * 3 * 4 * 5 = 120$

Beachte:
$0! = 1$

A.2 Binomialkoeffizient

In der Kombinatorik verwendet man den *Binomialkoeffizienten* $\binom{n}{k}$, um die Anzahl der Möglichkeiten, aus einer Menge mit n Elementen k Elemente auszuwählen, zu berechnen. Die Reihenfolge der Elemente wird dabei nicht berücksichtigt.

Für $n, k \in \mathbb{N}_0^+$ mit $n \geq k$ lässt sich der Binomialkoeffizient folgendermassen definieren:

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

Beispiel A.2:

$$\binom{7}{3} = \frac{7!}{3! * (7-3)!} = 35$$

A.3 Gaussklammer

Die *Gaussklammer* $\lfloor x \rfloor$ ist eine mathematische Funktion, die einer reellen Zahl x die grösste ganze Zahl zuweist, die kleiner oder gleich x ist; die Gaussklammer rundet also auf die nächste ganze Zahl ab.

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}.$$

Beispiel A.3:
$\lfloor 3.2 \rfloor = 3$

Beispiel A.4:
$\lfloor 4 \rfloor = 4$

Beispiel A.5:
$\lfloor 6.8 \rfloor = 6$

A.4 Rechnen modulo n

Modulo ist eine mathematische Funktion, die den Rest einer Division zweier Zahlen angibt. Die Funktion lässt sich folgendermassen definieren:

$$a \bmod b \quad = \quad a - \left\lfloor \frac{a}{b} \right\rfloor * b$$

Beispiel A.6:
$18 \mod 5 = 3 \quad (18 \div 5 = 3 \text{ Rest } 3)$

Beispiel A.7:
$9 \mod 3 = 0 \quad (9 \div 3 = 3 \text{ Rest } 0)$

A.5 n-adische Darstellung

Jede natürliche Zahl a lässt sich eindeutig durch die *n-adische Darstellung* darstellen:

$$a \equiv \sum_{i=0}^{k} a_i * n^i \equiv a_0 + a_1 * n + a_2 * n^2 + a_3 * n^3 + \cdots + a_k * n^k$$

Dabei ist n eine natürliche Zahl mit $n \geq 2$. Ebenso sind alle a_i natürliche Zahlen mit $0 \leq a_i < n$.

Beispiel A.8:
Die 5-adische Darstellung von 513:

$$513 \equiv 3 + 2 * 5 + 0 * 5^2 + 4 * 5^3$$

Anhang B

Gruppentheorie

B.1 Definition einer Gruppe

Eine algebraische Struktur $(G, \circ)$ mit einer Menge G und einer binären Verknüpfung $\circ : G \times G \to G$ heisst *Gruppe*, wenn folgende Axiome erfüllt sind:

Axiom B.1 (Assoziativität):
Für alle Elemente $a, b, c \in G$ gilt:
$(a \circ b) \circ c = a \circ (b \circ c)$.

Axiom B.2 (Neutrales Element):
Es gibt ein Element $e \in G$ derart, dass für alle Elemente $a \in G$ gilt:
$a \circ e = e \circ a = a$.

Axiom B.3 (Inverse Elemente):
Zu jedem Element $a \in G$ gibt es ein inverses Element $a^{-1} \in G$, für welches gilt:
$a \circ a^{-1} = a^{-1} \circ a = e$.

Die Gruppe heisst *kommutativ* oder *abelsche Gruppe*, falls für alle Elemente $a, b \in G$ zusätzlich gilt: $a \circ b = b \circ a$

Anstelle von $a \circ b$ sind auch die Bezeichnungen $a \cdot b$, $a \times b$ oder ab üblich.

B.2 Ordnung einer Gruppe

Die Mächtigkeit der Menge G wird *Ordnung* der Gruppe genannt. Für endliche Mengen ist dies die Anzahl der Elemente.

B.3 Ordnung von Gruppenelementen

Ein Gruppenelement g hat *endliche Ordnung*, falls ein $k > 0$ mit $g^k = e$ existiert. Die kleinste Zahl $k > 0$ mit $g^k = e$ heisst Ordnung in g. Falls für ein Element keine solche Zahl k existiert, so nennt man die Ordnung dieses Elements *unendlich*. Das neutrale Element e hat stets die Ordnung 1, da e^1 gleich e ist.

Lemma B.1:
Ist g ein Element der Ordnung k und gilt $g^m = e$ für ein $m > 0$, so teilt k die Zahl m.

B.4 Permutation

Eine *Permutation* ist eine bijektive Abbildung $\alpha : A \to A$ der Menge A auf sich selbst. Mit anderen Worten heisst das, dass eine Permutation die Anordnung einer Menge durch Vertauschen ihrer Elemente verändert. Die Anzahl der möglichen Permutation auf einer Menge mit n Elementen beträgt $n!$.

Beispiel B.1:
Die Permutation α bildet die Zahlen in der oberen Zeile auf ihre unter ihnen stehenden Zahlen ab. Die 1 wird zu einer 4, die 2 zu einer 3 usw.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

B.5 Komposition von Permutationen

Unter einer *Komposition* von Permutationen versteht man die Hintereinanderausführung von Permutation. Die Komposition zweier Permutationen ist erneut eine Permutation.

Die Komposition $\alpha\beta\,(a)$ wird als $\alpha\,(\beta\,(a))$ definiert.

Beachte:
Die Permutation β wird vor der Permutation α ausgeführt.

Beispiel B.2:
Da die zweite Permutation vor der ersten Permutation ausgeführt wird, wird die Zahl 1 zuerst auf die 3 abgebildet und dann die 3 auf die 4. Entsprechend geschieht dies auch mit den anderen Zahlen.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix}$$

B.6 Zykel

Eine Permutation σ heisst *Zykel der Länge* m, wenn es m verschiedene Elemente $a_1, a_2, \ldots, a_m$ gibt, die unter σ zyklisch vertauscht werden:

$$a_1 \mapsto a_2 \mapsto a_3 \mapsto \cdots \mapsto a_m \mapsto a_1$$

Ein Zyklus wird folgendermassen notiert:

$$\sigma = (a_1\ a_2\ a_3\ \cdots\ a_m)$$

B.7 Transposition

Die *Transposition* ist eine Permutation, die genau zwei Elemente miteinander vertauscht:

$$(i\,j): \begin{array}{ll} & i \mapsto j \\ & j \mapsto i \\ & k \mapsto k \quad \text{für} \quad k \neq i, j \end{array}$$

Eine Transposition ist also ein Zykel der Länge 2.

Beispiel B.3:
Bei der folgenden Transposition werden die Elemente 3 und 5 miteinander vertauscht:

$$(3\,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}$$

B.8 Konjugation

Zwei Permutationen α, β heissen *konjugiert*, falls ein δ existiert, für das gilt:

$$\beta = \delta^{-1}\alpha\delta$$

Ebenso gilt dann:

$$\alpha = \delta\beta\delta^{-1}$$

B.9 Fixpunkt

Ein *Fixpunkt* einer Permutation ist ein Element, dessen Position sich bei der Permutation nicht ändert.

Beispiel B.4:
Bei der folgenden Permutation sind die Elemente 1 und 3 Fixpunkte:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$$

B.10 Symmetrische Gruppe

Die *symmetrische Gruppe* S_n ist eine Gruppe, die aus allen Permutationen einer Menge mit n Elementen besteht. Die Gruppenoperation ist die Komposition der Permutationen.

Eine Untergruppe der symmetrischen Gruppe nennt man dann Permutationsgruppe.

Literaturverzeichnis

[Kipp99] Rudolf Kippenhahn: *Verschlüsselte Botschaften – Geheimschrift, Enigma und Chipkarte* Rowohlt Taschenbuch Verlag, Reinbek bei Hamburg, 2. Auflage, 1999.
ISBN 3-499-60807-3

[Singh01] Simon Singh: *Geheime Botschaften – Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet* Deutscher Taschenbuch Verlag, 3. Auflage, 2001.
ISBN 3-423-33071-6

[Kozac84] Wladyslaw Kozaczuk: *Enigma – how the German machine cipher was broken, and how it was read by the Allies on World War Two*, editiert und auf Englisch übersetzt von Christopher Kasparek, University Publications of America, 1984.
ISBN 0-89093-547-5

[Form84] Dmk/Dpk: *Formeln und Tafeln – Mathematik - Physik* Orell Füssli Verlag, 3. Auflage, 1984.
ISBN 3-280-01496-4

[Meis02] Robert Meissner: *Data Encryption Standard (DES)* Seminararbeit, Fakultät für Informatik der Technischen Universität Chemnitz, 2002.
http://archiv.tu-chemnitz.de/pub/2002/0059/

[Hauck07] Peter Hauck *Vorlesung Kryptologie und Datensicherheit WiSe 2006-2007* an der Universität Tübingen auf dem Tübinger Internet Multimedia Server, Stand August 2007.
http://timms.uni-tuebingen.de/

[Wiki07] Wikipedia: Einträge aus der freien Enzyklopädie Wikipedia (Suchbegriffe: Caesarchiffre, Enigma (Maschine), Häufigkeitsanalyse, Kryptologie, Kryptographie, monoalphabetische Substitution, polyalphabetische Substitution, Turing-Bombe und Verschlüsselung), Stand Dezember 2007
http://de.wikipedia.org/

Abbildungsverzeichnis

Bemerkungen: Das Hintergrundphoto auf der Titelseite entspricht der Abbildung 4.2. Des Weiteren wurden alle hier nicht aufgeführten Abbildungen von mir selbst erstellt.

Index

Z

Ehrlichkeitserklärung

Die eingereichte Arbeit ist das Resultat meiner persönlichen, selbstständigen Beschäftigung mit dem Thema. Ich habe für sie keine anderen Quellen benutzt als die in den Verzeichnissen aufgeführten. Sämtliche wörtlich übernommenen Texte (Sätze) sind als Zitat gekennzeichnet.

Ort, Datum Unterschrift