4 Symmetrische Verschlüsselung

In unserem Alice-Bob-Mallory-Modell wollen wir uns nun die Frage stellen, welche **Verschlüsselungsverfahren** Alice und Bob einsetzen können, um ihre Nachrichten vor Bösewicht Mallory zu verbergen. Wie Sie im Verlauf dieses Kapitels erfahren werden, ist es sinnvoll, wenn die beiden ein Verschlüsselungsverfahren einsetzen, in das eine Geheiminformation (der sogenannte **Schlüssel**) mit eingeht. Je nach Verfahren ist der Schlüssel ein Passwort, eine Geheimnummer oder einfach nur eine Folge von Bits. Bei einem guten Verschlüsselungsverfahren ist es für Alice und Bob bei Kenntnis des Schlüssels einfach, die verschlüsselte Nachricht zu entschlüsseln. Für Mallory ist eine Entschlüsselung dagegen ohne Kenntnis des Schlüssels schwer bis unmöglich, selbst wenn er das Verfahren genau kennt.

4.1 Symmetrische Verschlüsselung

Da bei einem geeigneten Verschlüsselungsverfahren die Sicherheit nur vom Schlüssel abhängt, wird ein solches (man spricht auch von einem **Verschlüsselungsalgorithmus** oder einer **Chiffre**) selbst in der Regel auch nicht geheim gehalten – dies gilt zumindest für das nichtmilitärische Umfeld. Stattdessen gilt es als sinnvoller, gerade den entgegengesetzten Weg zu gehen und die verwendeten Methoden so bekannt wie möglich zu machen. Erst wenn genügend Experten sich mit einem Verfahren beschäftigt haben, wenn es auf alle denkbaren Schwächen abgeklopft wurde und wenn dennoch keine Schwachstellen ans Licht gekommen sind, dann kann man davon ausgehen, dass auch Mallory keine Chance hat (da wir Mallory als besonders schlau annehmen, stellen wir ihn uns als einen hervorragenden Codeknacker vor).

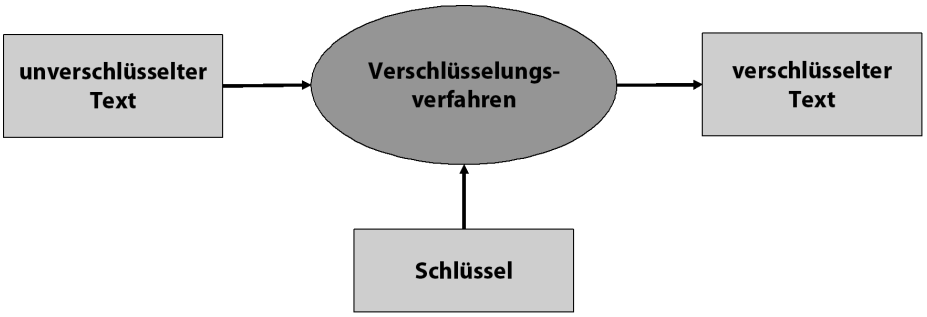

Abb. 4–1 *Bei einem guten Verschlüsselungsverfahren geht ein Schlüssel (eine Art Passwort) in die Verschlüsselung ein.*

Davon abgesehen ist es in der Praxis oft eine vergebliche Mühe, ein Verschlüsselungsverfahren geheim zu halten. Vor allem dann, wenn ein Verfahren in einer verbreiteten Software implementiert ist, wird sich früher oder später jemand die Mühe machen, den Quellcode zu analysieren und das Verfahren anschließend bekannt zu machen. Sie werden in diesem Buch mehrere Verfahren kennenlernen (z. B. A5, Crypto1, RC2 und RC4), die ursprünglich geheim waren, irgendwann jedoch öffentlich bekannt wurden. Ähnliche Überlegungen wie bei Verschlüsselungsverfahren gelten übrigens auch für andere Teilbereiche der Computersicherheit: Die Sicherheit eines Systems sollte – falls möglich – nicht von der Geheimhaltung der Funktionsweise (**Security by Obscurity**) abhängen.

4.1.1 Kryptografische Fachbegriffe

An dieser Stelle will ich noch einige Fachbegriffe einführen: Verschlüsselungsverfahren, die gemäß der beschriebenen Weise mit Schlüsseln arbeiten, nennt man auch **symmetrische Verfahren** oder **Secret-Key-Verfahren.** Später werden Sie auch Verschlüsselungsverfahren kennenlernen, bei denen ein Schlüssel nicht in allen Fällen geheim ist und die daher als asymmetrische Verfahren oder Public-Key-Verfahren bezeichnet werden. Man spricht in diesem Zusammenhang auch von **symmetrischer Kryptografie** und **asymmetrischer Kryptografie** oder von **Public-Key-Kryptografie** und **Secret-Key-Kryptografie**. Verbreitet sind auch Ausdrücke wie symmetrische Verschlüsselung, asymmetrische Verschlüsselung, Secret-Key-Verschlüsselung oder Public-Key-Verschlüsselung.

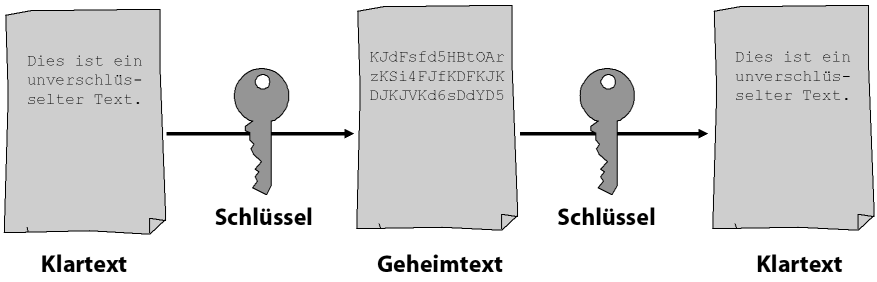

Abb. 4–2 *Eine Nachricht, die verschlüsselt wird, heißt Klartext. Das Resultat der Verschlüsselung wird als Geheimtext bezeichnet. Verschlüsselungsverfahren werden auch Chiffren genannt.*

Eine Nachricht, die verschlüsselt wird, heißt **Klartext**, der verschlüsselte Text **Geheimtext** (auch wenn es sich nicht um einen Text im eigentlichen Sinne handeln muss). In der Sprache der Mathematik sind Verschlüsselung und Entschlüsselung Funktionen, für die wir die Buchstaben *e* (encrypt) bzw. *d* (decrypt) verwenden. Ist *k* der Schlüssel, *m* der Klartext und *c* der Geheimtext, dann gelten folgende zwei Formeln:

$$e(m,k)=c$$
$$d(c,k)=m$$

4.1.2 Angriffe auf Verschlüsselungsverfahren

Versucht Mallory, einen Geheimtext zu entschlüsseln, den Alice an Bob schickt, oder den Schlüssel herauszufinden, so nennt man dies einen **Angriff** oder eine **Attacke**. Die Kryptoanalyse ist somit die Wissenschaft der Angriffe auf Verschlüsselungsverfahren. Man sagt auch, Mallory versucht das Verfahren zu **brechen** oder (etwas weniger wissenschaftlich) zu **knacken**. Gelingt es Mallory, mit nicht-

kryptoanalytischen Methoden an einen Schlüssel zu kommen (durch Stehlen, Bestechen oder wie auch immer), so hat er einen Schlüssel **kompromittiert**.

Angriffe auf Verschlüsselungsverfahren kann man in verschiedene Gruppen einteilen:

- Kennt Mallory den Klartext nicht, dann spricht man von einer **Ciphertext-Only-Attacke**.
- Kennt Mallory den Klartext und versucht, für das Abhören weiterer Nachrichten den Schlüssel zu erfahren, so nennt man dies eine **Known-Plaintext-Attacke**.
- Will Mallory den Schlüssel herausfinden und hat dabei die Möglichkeit, den Klartext selber zu wählen, so spricht man von einer **Chosen-Plaintext-Attacke**.

Keine Frage, die Ciphertext-Only-Attacke ist bei weitem die schwierigste. Gleichzeitig ist sie jedoch auch diejenige, die in der Praxis am häufigsten vorkommt, denn im Normalfall weiß Mallory ja nicht, was in der abgefangenen Nachricht steht. Wenn doch, dann ist er am Schlüssel vielleicht gar nicht mehr interessiert. Trotzdem spielen auch die beiden anderen Angriffe eine wichtige Rolle.

Eine Known-Plaintext-Attacke ist häufig dann möglich, wenn sich Nachrichten oder Teile davon wiederholen. Wenn Alice für ihre E-Mails beispielsweise stets den gleichen Briefkopf verwendet oder alle ihre Mails mit den Worten »Hallo Bob« beginnt, dann kennt Mallory, sofern er dies weiß, zumindest teilweise den Klartext. Mit einer Known-Plaintext-Attacke kann er nun versuchen, den Schlüssel herauszufinden, um so auch den Rest der E-Mail zu entschlüsseln.

Die Chosen-Plaintext-Attacke ist der einfachste Angriff. Bei vielen herkömmlichen Verfahren ist dieser Angriff ein Kinderspiel – bei modernen Verfahren zum Glück nicht. Eine Chosen-Plaintext-Attacke kann Mallory beispielsweise am Entschlüsselungschip eines Pay-TV-Decoders starten. Der Schlüssel ist in diesem Fall in einer Hardware (Smartcard) gespeichert und damit nicht ohne weiteres auslesbar. Da Mallory jedoch zum eigenen Decoder unbeschränkten Zugang hat, kann er diesen mit selbst gewähltem Klartext füttern. Allerdings gilt bei dieser Chosen-Plaintext-Attacke: Die im Bezahlfernsehen verwendeten Verfahren sind gegen einen solchen Angriff nur bedingt anfällig.

Die Moral von dieser Geschichte: Ein gutes Verschlüsselungsverfahren muss auch einer Chosen-Plaintext-Attacke widerstehen, ansonsten ist es nicht wirklich sicher. Verspricht dagegen sogar ein Known-Plaintext- oder gar Ciphertext-Only-Angriff Erfolg, dann gehört das Verfahren nicht ins Internet, sondern in den Papierkorb.

4.2 Monoalphabetische Substitutionschiffren

Nach all den theoretischen Vorüberlegungen wollen wir nun zur Sache kommen und uns einige Verschlüsselungsverfahren anschauen. Wir beginnen mit einfachen Algorithmen, die Alice und Bob von Hand ausführen können. In der Praxis werden diese Verfahren seit Aufkommen des Computers kaum noch verwendet, zumal viele davon äußerst unsicher sind. Sie bilden jedoch eine wichtige Grundlage für komplexere Verfahren, um die es in späteren Kapiteln geht.

4.2.1 Cäsar-Chiffre

Da Alice und Bob sich hauptsächlich Texte per E-Mail zuschicken, bietet sich zunächst ein Verschlüsselungsverfahren an, das jeden Buchstaben durch einen anderen ersetzt. Beispielsweise kann jeder Buchstabe um eine Zahl n verschoben werden:

Ist n=1, dann gilt: aus A wird B, aus B wird C, aus C wird D, ...

Ist n=2, dann gilt: aus A wird C, aus B wird D, aus C wird E, ...

Der Klartext

DERMENSCHMACHTFEHLER,FUERKATASTROPHENISTDERCOMPUTERZUSTAENDIG.

wird bei n=5 zu folgendem Geheimtext:

IJWRJSXHMRFHMYKJMQJW,KZJWPFYFXYWTUMJSNXYIJWHTRUZYJWEZXYFJSINL.

Sie haben es sicher erraten, n ist der Schlüssel bei diesem Verfahren, das man als **Cäsar-Chiffre** bezeichnet (weil es schon Julius Cäsar bekannt war). Die Cäsar-Chiffre kennt 26 verschiedene Schlüssel (der Schlüssel 26 sollte jedoch aus naheliegenden Gründen vermieden werden). Natürlich ist das Verfahren nicht sicher, selbst eine Ciphertext-Only-Attacke ist möglich. Von Hand oder mit Computerunterstützung muss Mallory dazu die Zahlen 1 bis 25 durchprobieren und kann so den Schlüssel schnell ermitteln. Einen solchen Angriff, bei dem alle möglichen Schlüssel durchprobiert werden, nennt man **vollständige Schlüsselsuche** oder auch **Brute-Force-Attacke**. Es versteht sich von selbst, dass eine gute Chiffre auch einer vollständigen Schlüsselsuche mit Computerunterstützung widerstehen sollte.

Eine andere wirksame Attacke auf die Cäsar-Chiffre ist die sogenannte Häufigkeitsanalyse, die vor allem bei längeren Texten hervorragend funktioniert. Die Häufigkeitsanalyse beruht auf der einfachen Tatsache, dass in einem Text normalerweise nicht alle Buchstaben gleich häufig vorkommen. In der deutschen Sprache ist das E mit über 17 Prozent der häufigste Buchstabe (siehe Abbildung 4–3), gefolgt vom N (10 Prozent) und dem R (7 Prozent). Dies kann Mallory ausnutzen, indem er beim obigen Beispiel-Geheimtext das Vorkommen der einzelnen Buchstaben zählt. Es ergeben sich folgende Häufigkeiten:

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
3	1	0	0	1	4	0	3	3	9	2	4	2	0	1	1	3	3	2	2	0	6	4	5	0	0

Sie sehen, das J ist mit 9 Vorkommnissen der häufigste Buchstabe des Geheimtexts. Tatsächlich ist es das J, auf das das E abgebildet wurde, schon alleine damit wäre diese Cäsar-Chiffrierung gebrochen. Dass der zweithäufigste Buchstabe das V ist, obwohl dieses nicht für das N steht, gehört zu den Widrigkeiten im Leben eines Kryptoanalytikers. Bei längeren Texten kommt so etwas in der Regel nicht vor.

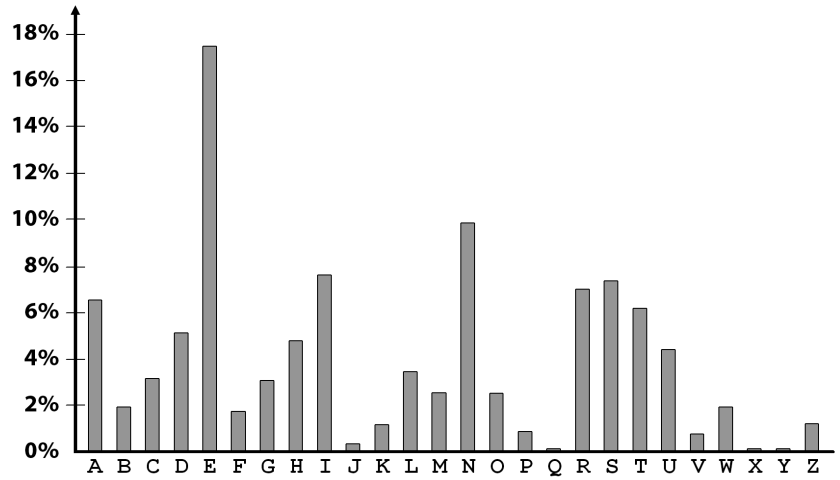

Abb. 4–3 *Die Buchstaben in der deutschen Sprache sind ungleich verteilt. Das »E« ist mit Abstand der häufigste Buchstabe. Dies kann sich Mallory beim Knacken einer Verschlüsselung zunutze machen.*

4.2.2 Weitere Substitutionschiffren

Die Cäsar-Chiffre ersetzt jeden Klartext-Buchstaben durch einen Chiffretext-Buchstaben. Ein Verfahren mit dieser Eigenschaft wird **Substitutionschiffre** genannt. Die folgende Tabelle stellt ein weiteres Beispiel für eine Substitutionschiffre dar (jeder Buchstabe in der oberen Zeile wird auf den direkt darunter stehenden abgebildet):

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

Auch hier kommt Mallory mit einer Häufigkeitsanalyse zum Ziel. Allerdings genügt es dieses Mal nicht, nur den häufigsten Buchstaben im Geheimtext zu bestimmen. Stattdessen muss Mallory für mehrere (am besten alle) die relative Häufigkeit berechnen. Hat er dies erst einmal gemacht und ist der Geheimtext lang genug, dann hat Mallory mithilfe einer Statistik wie in Abbildung 4–3 keine Probleme mehr, den Klartext zu bestimmen.

Natürlich könnten Alice und Bob Mallory die Arbeit noch etwas erschweren, indem sie nicht von 26 Buchstaben ausgehen, sondern beispielsweise von 256 ASCII-Zeichen. In diesem Fall wären Wortzwischenräume und Satzzeichen für Mallory nicht mehr als solche zu erkennen. Zudem ist es aufwendiger, eine Tabelle wie in Abbildung 4–3 für 256 Zeichen aufzustellen. Da Mallory in unserem Modell genau weiß, was für ein Verfahren verwendet wird (und somit auch, wie die einzelnen Zeichen kodiert sind), wäre dies nur unwesentlich sicherer. Darüber hinaus ist zu berücksichtigen, dass wir bisher nur über eine Ciphertext-Only-Attacke geredet haben. Eine Known-Plaintext- und erst recht eine Chosen-Plaintext-Attacke ist bei einer Substitutionschiffre trivial.

4.2.3 Homophone Chiffre

Da die unterschiedlichen Buchstabenhäufigkeiten bei einer einfachen Substitutionschiffre den entscheidenden Schwachpunkt bilden, liegt es nahe, eine Ersetzungstabelle zu verwenden, die diese Unterschiede ausgleicht. Alice und Bob können beispielsweise die Zahlen zwischen 00 und 99 so auf die 26 Buchstaben des Alphabets verteilen, dass jede Zahl etwa gleich oft vorkommt. Ein solches Verfahren nennt man **homophone Chiffre**. Es zählt ebenfalls zu den Substitutionschiffren.

Bei einer homophonen Chiffre müssen Alice und Bob jedem Buchstaben so viele Zahlen zuweisen, wie es seiner prozentualen Häufigkeit im Klartext entspricht. Im Deutschen erhält beispielsweise das E (17 Prozent Häufigkeit) 17 Zahlen, während dem N 10 und dem I 8 Zahlen zugeordnet sind. Die folgende Tabelle beschreibt ein Beispiel (unter den Buchstaben steht jeweils die Anzahl der zugeordneten Zahlen, wobei ich teilweise gerundet habe, damit es aufgeht).

A	B	C	D	E	F	G	H	I	J	K	L	M
6	*2*	*3*	*5*	*17*	*1*	*3*	*4*	*8*	*1*	*1*	*3*	*2*
34,45, 54,72, 79,86	14,71	04,28, 61	07,39, 47,87, 99	11,20, 24,32, 42,48, 49,53, 60,65, 70,78, 81,84, 91,96, 98	15	27,38, 63	21,43, 59,88	00,08, 22,31, 35,64, 76,89	66	01	44,52, 75	12,80

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	*2*	*1*	*1*	*7*	*7*	*6*	*4*	*1*	*2*	*1*	*1*	*1*
10,29, 40,41, 62,74, 83,85, 90,92	30,58	03	37	19,33, 51,67, 82,93, 97	05,16, 25,36, 46,55, 68	26,50, 56,69, 77,94	02,23, 57,73	17	06,18	95	09	13

Der Klartext EBENE lässt sich so in den Geheimtext 20 71 48 29 98 verschlüsseln. Das Zählen der Buchstaben hilft Mallory selbst bei einem längeren Geheimtext nicht weiter, da die Häufigkeiten keine Rückschlüsse auf den jeweiligen Buchstaben erlauben.

Eine homophone Chiffre ist nicht leicht zu knacken. Wirklich sicher ist sie dennoch nicht. Wenn Mallory ein paar Wörter oder Buchstaben des Texts erraten kann, dann reicht dies möglicherweise aus, um weitere Buchstaben zu ergänzen und so schließlich den gesamten Text zu rekonstruieren. Wie so etwas funktionieren kann, zeigt das Beispiel des sogenannten Zodiac-Killers. Dabei handelt es sich um einen Serienmörder, der Ende der sechziger Jahre in Kalifornien sein Unwesen trieb. Der bis heute nicht identifizierte Täter schrieb insgesamt vier verschlüsselte Nachrichten an verschiedene Zeitungen, von denen bisher nur eine geknackt wurde. Die erfolgreiche Kryptoanalyse gelang einem rätselbegeisterten Ehepaar, das die Nachricht aus der Presse kannte. Die beiden vermuteten, dass der Verfasser eine homophone Chiffre verwendet hattte, und sie nahmen an, dass das erste Wort im Text »I« (ich) lautete. Dieser Ansatz erwies sich als Volltreffer und reichte, um den gesamten Klartext zu ermitteln.

Leider enthielt der entschlüsselte Text keine Informationen, die zum Täter führten. Die drei weiteren verschlüsselten Nachrichten des Zodiac-Killers sind nach wie vor ungelöst. Es ist nicht bekannt, ob der Täter auch hier eine homophone Chiffre verwendete.

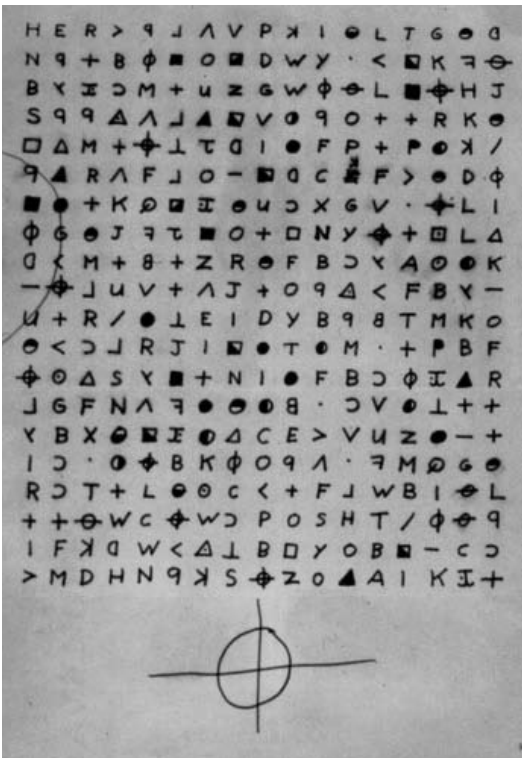

Abb. 4–4 *Der Zodiac-Killer schickte vier verschlüsselte Nachrichten an verschiedene Zeitungen yon denen nur eine gelöst wurde. Die Abbildung zeigt eine der ungelösten Nachrichten.*

Kann Mallory eine Known-Plaintext-Attacke anwenden, dann ist das Knacken einer homophonen Verschlüsselung trivial. Wenn Alice und Bob befürchten, dass Mallory in den Besitz eines Klartexts kommt, dann sollten sie daher für jede Datenübertragung einen neuen Schlüssel (also eine neue Tabelle) vereinbaren. Dies macht das ohnehin unhandliche Verfahren noch unhandlicher. Die homophone Chiffre wurde daher bereits in der Vor-Computerära selten verwendet und ist seit Aufkommen des Computers nur noch historisch interessant.

4.3 Polyalphabetische Substitutionschiffren

Die bisher betrachteten Verfahren haben alle die Eigenschaft, dass beim Entschlüsseln ein bestimmter Geheimtextbuchstabe (bzw. eine Geheimtextzahl) immer auf denselben Klartextbuchstaben abgebildet wird. Wenn Mallory im Geheimtext mehrfach den Buchstaben G findet, dann weiß er, dass sich jedes Mal der gleiche Buchstabe dahinter verbirgt. Dies gilt auch für die homophone Chiffre, bei der im oben genannten Beispiel die Zahl 14 immer für das C steht.

Eine Chiffre mit dieser Eigenschaft nennt man **monoalphabetisch.** Versuchen wir unser Glück also mit einem Verfahren, das nicht monoalphabetisch und daher **polyalphabetisch** ist.

4.3.1 Vigenère-Chiffre

Das bekannteste polyalphabetische Verschlüsselungsverfahren ist die **Vigenère-Chiffre**. Diese ist nach dem französischen Kryptografen Blaise de Vigenère (1523–1596) benannt. Um deren Funktionsweise zu verstehen, nehmen wir an, dass Alice folgenden Klartext verschlüsseln will:

ALLES IST EINE FOLGE VON BITS.

Der Schlüssel ist in diesem Fall ein Wort, zum Beispiel ALICE. Zur Verschlüsselung schreibt Alice Klartext und Schlüssel folgendermaßen untereinander:

ALLES IST EINE FOLGE VON BITS.
ALICE ALI CEAL ICEAL ICE ALIC.

Anschließend addiert Alice die Buchstaben spaltenweise (A=0, B=1, C=2, ...; nach Z fängt sie wieder bei A an):

ALLES IST EINE FOLGE VON BITS.
ALICE ALI CEAL ICEAL ICE ALIC.

AWTGW IDB GMNP NQPGP DQR BTBU.

Der Geheimtext lautet also AWTGW ... Wie Sie sehen, kann derselbe Geheimtext-Buchstabe hier für verschiedene Klartext-Buchstaben stehen, wie zum Beispiel das erste W für ein L und das zweite W für ein S. Die Vigenère-Chiffre ist daher polyalphabetisch. Dank dieser Eigenschaft ist die Vigenère-Chiffre wesentlich sicherer als die Cäsar-Chiffre, zumal eine vollständige Schlüsselsuche hier schon sehr aufwendig ist. Trotzdem kann auch die Vigenère-Chiffre schon mit einer Ciphertext-Only-Attacke leicht gebrochen werden. Der entscheidende Punkt bei diesem Angriff ist die Länge des Schlüssels. Ist Mallory diese bekannt, dann besteht sein Problem nur noch darin, mehrere Cäsar-Chiffren zu brechen, und das ist wie beschrieben nicht besonders schwierig. Um die Schlüssellänge zu ermitteln, genügt es oft schon, den Geheimtext auf Buchstabenfolgen abzusuchen, die sich wiederholen. Kommt beispielsweise im Geheimtext die Buchstabenkombination BJHG zweimal vor und beträgt der Abstand 56, so ist dies ein Indiz dafür, dass 56 durch die Schlüssellänge teilbar ist. Findet Mallory ein weiteres Muster, das doppelt vorkommt, mit dem Abstand 105, so ist der Fall schon klar: Die Teiler von 56 sind 2, 4, 7, 8, 14 und 28, die Teiler von 105 sind 3, 5 und 7. Da 7 als einzige Zahl sowohl 105 als auch 56 teilt, ist dies mit großer Wahrscheinlichkeit die Schlüssellänge.

Es gibt noch andere Methoden, mit denen Mallory die Schlüssellänge ermitteln kann, doch diese wollen wir hier überspringen, da das Vigenère-Verfahren in der Praxis ohnehin keine Rolle spielt. Klar ist jedenfalls Folgendes: Eine Ciphertext-Only-Attacke mit Computerunterstützung ist auch in diesem Fall kein Problem, und Mallory hat bei bekanntem oder gar frei wählbarem Klartext erst recht keine Mühe.

4.3.2 Vernam-Chiffre

Obwohl die Vigenère-Chiffre genauso alt wie unsicher ist, ist sie keineswegs nutzlos. Sie kann sogar zu einer sehr sicheren Chiffre ausgebaut werden, wenn Alice und Bob den richtigen Schlüssel verwenden. Damit es Mallory so schwer wie möglich gemacht wird, sollten Alice und Bob den Schlüssel möglichst lang wählen. Je länger der Schlüssel nämlich ist, desto mehr Cäsar-Chiffren muss Mallory brechen und desto weniger Text steht diesem für jede Cäsar-Chiffre zur Verfügung. Idealerweise wählen Alice und Bob den Schlüssel einer Vigenère-Chiffre sogar so lang, dass er die gleiche Länge wie der Klartext hat. Diesen Spezialfall nennt man dann **Vernam-Chiffre** (benannt nach ihrem Erfinder Gilbert Vernam). Die Vernam-Chiffre ist mit einer einfachen Häufigkeitsanalyse oder mit einer vollständigen Schlüsselsuche nicht zu brechen. Wirklich sicher ist sie aber trotzdem nicht. Falls der Geheimtext – und damit auch der Schlüssel – lang genug sind und beide aus einer natürlichen Sprache (zum Beispiel Deutsch) stammen, kann sich Mallory zunutze machen, dass Buchstaben im Klartext und Schlüssel nicht mit der gleichen Häufigkeit auftreten und dass damit auch im Geheimtext eine ungleiche Verteilung vorliegt. Mallory kann also wiederum eine Häufigkeitsanalyse einsetzen. Natürlich ist diese wesentlich komplizierter als bei einer einfachen Substitutionschiffre, für geübte Kryptoanalytiker mit Computerunterstützung vom Schlage eines Mallory ist so etwas jedoch nur eine Fleißaufgabe.

4.3.3 One-Time-Pad

Wenn Mallory die Vernam-Chiffre auf die beschriebene Weise brechen will, dann müssen Schlüssel und Klartext jeweils ungleichmäßige Buchstabenverteilungen besitzen. Wählen Alice und Bob dagegen als Schlüssel eine rein zufällige Buchstabenfolge, dann hat eine Häufigkeitsanalyse keinen Erfolg mehr. Eine Vernam-Chiffre, bei der der Schlüssel eine solche Zufallsfolge ist, nennt man **One-Time-Pad**. Wie der Name sagt, wird beim One-Time-Pad der Schlüssel (der wiederum die gleiche Länge hat wie der Klartext) nur einmal verwendet, ansonsten wäre die Buchstabenfolge ja nicht mehr zufällig, und es würde für den Angreifer wieder darauf hinauslaufen, eine Vigenère-Chiffre zu brechen.

Sicherheit des One-Time-Pad

Gibt es nun überhaupt eine Methode der Kryptoanalyse, die gegen den One-Time-Pad Erfolg verspricht? Interessanterweise nicht, zumindest dann, wenn der Schlüssel wirklich zufällig ist (was unter zufällig zu verstehen ist, lesen Sie in Kapitel 14). Dann kann sogar bewiesen werden, dass der Geheimtext ebenfalls vollkommen zufällig ist und damit nicht gebrochen werden kann. Oder mit anderen Worten: Jeder mögliche Klartext kann in jeden möglichen Geheimtext verschlüsselt werden, und das mit jeweils gleicher Wahrscheinlichkeit – da hat Mallory ausgespielt. Der One-Time-Pad in seinen verschiedenen Formen ist übrigens das einzige Verschlüsselungsverfahren, für das diese Eigenschaft gilt. Es ist absolut sicher.

Der One-Time-Pad funktioniert nicht nur mit den 26 Buchstaben des Alphabets. Genauso gut können auch die 256 ASCII-Zeichen oder eine andere Menge von Zeichen verwendet werden. In der modernen Kryptografie werden nur die zwei Zahlen 0 und 1 verwendet. Der Klartext ist in diesem Fall eine Bit-Folge, der Schlüssel ebenfalls. Die Addition von einem Klartext-Bit mit einem Schlüssel-Bit entspricht dabei einer sogenannten **Exklusiv-oder-Verknüpfung**. Eine Exklusiv-oder-Verknüpfung liefert genau dann den Wert 1, wenn ein Eingabewert 0 und der andere 1 ist. Ansonsten ist das Ergebnis 0. Notiert wird diese Operation mit dem Zeichen »⊕«. Es ergeben sich daher folgende Gleichungen:

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

Die Exklusiv-oder-Verknüpfung spielt in der Kryptografie eine sehr wichtige Rolle und wird Ihnen in diesem Buch noch des Öfteren begegnen.

Nachteile des One-Time-Pad

Nun, da wir schon am Anfang dieses Buches ein absolut sicheres und obendrein einfaches Verschlüsselungsverfahren entdeckt haben, wozu müssen wir uns überhaupt weiterhin mit diesem Thema beschäftigen? Ganz einfach, weil der One-Time-Pad leider auch seine Nachteile hat. Im Wesentlichen sind es drei:

- Der Umgang mit einem Schlüssel, der genauso lang ist wie die Nachricht, ist nicht besonders handlich. Wollen Alice und Bob dieses Verfahren im Internet anwenden, dann muss zu jedem verschickten Bit ein Schlüssel-Bit existieren, das nur Alice und Bob bekannt ist. Verwendeten beispielsweise alle Internetanwender den One-Time-Pad, dann würde sich das Datenaufkommen im Internet verdoppeln.

- Wenn ein Schlüssel übers Computernetz übertragen wird, dann kann er abgehört werden. Mehr dazu im Kapitel über das Schlüsselaustausch-Problem (Kapitel 10).
- Es ist wesentlich schwieriger, als man denkt, große Mengen an Zufallszahlen herzustellen, die wirklich zufällig sind. Mehr dazu im Kapitel über Zufallszahlen (Kapitel 14).

Die genannten Nachteile sind so gravierend, dass der One-Time-Pad in der Praxis nicht eingesetzt wird. Es gibt jedoch sehr viele Verfahren, die die dahinter stehende Idee ausnutzen, indem sie aus einem kurzen Schlüssel einen langen generieren, der dann wie im One-Time-Pad eingesetzt wird. Eine gewisse Bedeutung hat der One-Time-Pad zudem im Geheimdienst- und im Militärbereich. Ist beispielsweise Bob als Spion im Auftrag des Geheimdiensts von Kryptoland unterwegs, dann trägt er stets einen versiegelten Umschlag mit sich, der eine längere Folge von zufälligen Buchstaben enthält. Diese Buchstabenfolge kann Bob in Notfällen als One-Time-Pad-Schlüssel verwenden, um eine Nachricht an die Einsatzzentrale zu schicken. Ein solches Verschlüsselungsverfahren ist sehr sicher und obendrein einfach zu handhaben. Selbst ein Laie kann damit eine Nachricht zuverlässig verschlüsseln und braucht dazu nur Stift und Papier.

4.4 Permutationschiffren

Neben den Substitutionschiffren gibt es eine weitere einfache Klasse von Verschlüsselungsverfahren: die **Permutationschiffren**. Bei einer Permutationschiffre werden die Buchstaben des Klartexts nicht durch andere ersetzt, sondern in ihrer Reihenfolge vertauscht. Betrachtet man beispielsweise jeweils fünf Klartextbuchstaben auf einmal, dann ist durch folgende Vorschrift eine Permutationschiffre gegeben:

> Buchstabe 4 kommt auf Position 1, 1 auf 2, 2 auf 3, 5 auf 4 und 3 auf 5. Der Schlüssel ist hierbei (in Kurzform): (4, 1, 2, 5, 3).

Der Klartext

ESGIBTZWEIARTENVONLEUTEN:SOLCHE,DIEZUENDEBRINGEN,WASSIEANFANGEN.

wird durch diese Chiffrierung zum Geheimtext:

IESBGETZIWEARNTLVOENNUTS:EHOLEC,ZDIUEEENBDGRIENS,NWSANIEFAEANNG.

Eine solche Verschlüsselung können Alice und Bob auch mit einem Passwort als Schlüssel durchführen, das leichter zu merken ist als eine Folge von Zahlen. Die Vertauschungsvorschrift erhalten sie, indem sie die Buchstaben dieses Worts alphabetisch sortieren. Beispielsweise ergibt sich aus dem Passwort ALICE die alphabetisch sortierte Folge ACEIL, was (1, 4, 5, 3, 2) entspricht. Am einfachsten

können Alice und Bob dieses Verfahren nutzen, wenn Absenderin Alice den Klartext unter dem Schlüsselwort zeilenweise aufschreibt und dann die Spalten umsortiert:

```
ALICE      ACEIL
_____      _____
ESGIB      EIBGS
TZWEI      TEIWZ
ARTEN      AENTR
VONLE      VLENO
UTENS      UNSET
OLCHE  =>  OHECL
DIEZU      DZUEI
ENDEB      EEBDN
RINGE      RGENI
NWASS      NSSAW
IEANF      INFAE
ANGEN      AENGN
```

Der Geheimtext lautet also EIBGSTEIWZA... Eine in dieser Form verwendete Permutationschiffre wird auch als **Würfel** bezeichnet. Führt Alice den Würfel zweimal hintereinander mit unterschiedlichen Passwörtern aus, dann spricht man von einem **Doppelwürfel**.

Die Kryptoanalyse einer Permutationschiffre ist oft einfacher, als man zunächst vermutet. Mallory stehen für diesen Zweck Verfahren zur Verfügung, die Häufigkeiten von Buchstabenpaaren (Bigrammen) und Buchstabendreiergruppen (Trigrammen) ausnutzen. Im Deutschen kommen beispielsweise die Bigramme EN, ER und CH sowie die Trigramme ICH, EIN und UND am häufigsten vor. Mallorys Kryptoanalyse läuft daher darauf hinaus, die Buchstaben des Texts auf unterschiedliche Weise umzugruppieren, um danach jeweils die Anzahl der Bigramme und Trigramme zu untersuchen. Bei einer Schlüssellänge von fünf (wie in den beiden Beispielen) ist dies durchaus zu schaffen. Mit zunehmender Schlüssellänge wird die Aufgabe für Mallory jedoch immer schwieriger.

Besonders schwer zu knacken ist ein Doppelwürfel. Wenn Alice und Bob dieses Verfahren richtig verwenden (mit zwei langen Wörtern, deren Länge keine gemeinsamen Teiler haben), dann ist die Kryptoanalyse selbst mit Computerunterstützung schwierig bis unslösbar. Der Doppelwürfel zählt daher zu den besten Verfahren, die sich ohne Computerunterstützung praktikabel nutzen lassen. Im Kalten Krieg war der Doppelwürfel deshalb ein beliebtes Verfahren für Spione, die verschlüsselte Nachrichten an ihre Agentenführer verschickten. Da ein Spion im Feindesland nicht mit einer One-Time-Pad-Liste oder gar einer Ver-

schlüsselungsmaschine erwischt werden wollte, bevorzugten viele Geheimdienste den Doppelwürfel, für den ein Agent nur ein Blatt Papier und zwei Passwörter benötigte.

Leider gibt es bisher nur wenig öffentliche Literatur über den Doppelwürfel. Es ist daher nicht genau bekannt, wie schwierig die Kryptoanalyse wirklich ist. Auf Anregung des ehemaligen BSI-Präsidenten Otto Leiberich veröffentlichte ich daher 2007 einen mit dem Doppelwürfel verschlüsselten Geheimtext mit der Aufforderung, diesen zu knacken [Schm07/1]. Der Geheimtext ist in Kapitel 38.1.4 abgedruckt. Der Klartext und die beiden Schlüsselwörter stammen aus der englischen Sprache. Bis heute hat mir niemand eine Lösung des Texts zugeschickt.

Trotz einer potenziell hohen Sicherheit haben Permutationschiffren auch einige Nachteile. So ist eine Known-Plaintext-Attacke für Mallory in jedem Fall trivial. Alice und Bob können dies wiederum ausgleichen, indem sie für jede Nachricht einen neuen Schlüssel verwenden. Ein weiterer Nachteil besteht darin, dass sich am Geheimtext auch ohne Entschlüsselung einiges erkennen lässt. Insbesondere kann Mallory über die Buchstabenhäufigkeit auf die verwendete Sprache schließen. Bei kürzeren Nachrichten (etwa solchen, die nur aus einem Wort bestehen) ist die Sicherheit einer Permutationschiffre nicht besonders hoch.

Permutationschiffren sind daher nur bedingt und unter geeigneten Umständen empfehlenswert. Ich habe diese Art von Verfahren an dieser Stelle vor allem deshalb eingeführt, weil sich später zeigen wird, dass Alice und Bob mit einer Mischung aus Permutationschiffre und Substitutionschiffre (z. B. One-Time-Pad) hervorragende Verschlüsselungsverfahren zusammenbasteln können.

4.5 Ungelöste Verschlüsselungen

Die meisten Verschlüsselungsverfahren, die ich auf den vorhergehenden Seiten beschrieben habe, sind schon recht alt und lassen sich mit der heute verfügbaren Computertechnik einfach lösen. Ausnahmen, wie der One-Time-Pad oder der Doppelwürfel, sind erst in den letzten 100 Jahren entstanden. Man kann daher sagen: Verschlüsselungsverfahren, die aus der Zeit vor dem 20. Jahrhundert stammen, stellen Kryptografen heute vor keine größeren Probleme mehr. Interessanterweise gibt es dennoch einige wenige verschlüsselte Texte, die bereits über ein Jahrhundert alt sind und dennoch bis heute allen Kryptoanalyse-Versuchen getrotzt haben. Die drei wichtigsten Beispiele schauen wir uns im Folgenden an. Ausführlichere Betrachtungen dazu können Sie in [Schm07/1] nachlesen.

4.5.1 Das Voynich-Manuskript

Das Voynich-Manuskript ist das wohl bedeutendste ungelöste Rätsel der Kryptografie-Geschichte. Es handelt sich dabei um ein handgeschriebenes Buch, in dem zahlreiche Abbildungen enthalten sind. Das Alter des Manuskripts ist nicht

bekannt, wird jedoch meistens auf etwa 500 Jahre geschätzt. Der Text ist in unbekannten Buchstaben verfasst. Insgesamt enthält das Voynich-Manuskript etwa 170.000 Schriftzeichen. Dies ist eigentlich eine gute Voraussetzung, um eine erfolgreiche Kryptoanalyse durchzuführen, auch wenn das verwendete Verfahren nicht bekannt ist. Bisher sind jedoch alle Versuche, das Voynich-Manuskript zu entschlüsseln, erfolglos geblieben.

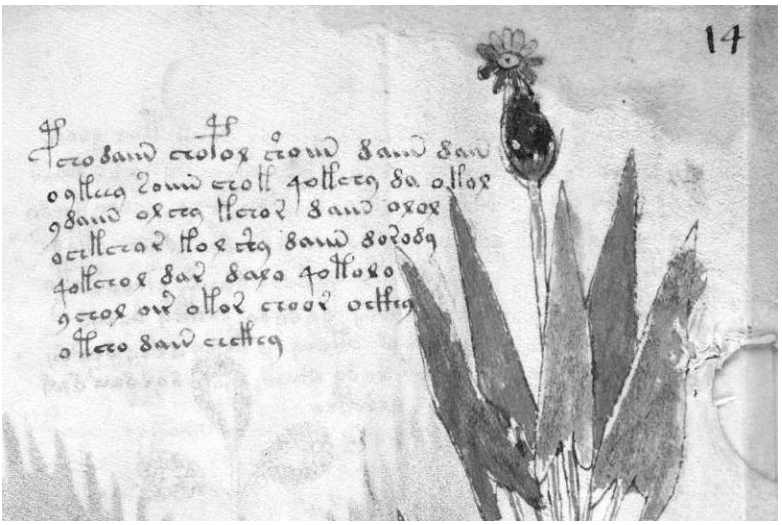

Abb. 4–5 *Das Voynich-Manuskript ist das bekannteste Rätsel der Kryptografie-Geschichte. Bis heute ist nicht bekannt, was sich hinter den seltsamen Buchstaben verbirgt.*

Einigermaßen sicher ist inzwischen immerhin, dass der Text nicht in einer natürlichen Sprache in unverändertem Zustand verfasst ist. Diesen Schluss lassen zahlreiche statistische Untersuchungen zu, deren Ergebnisse kaum mit einer bekannten Sprache in Einklang zu bringen sind. Möglich ist dagegen eine natürliche Sprache in veränderter Form, eine Kunstsprache oder eine Verschlüsselung. Ebenfalls denkbar (und nach Meinung einiger Experten nicht gerade unwahrscheinlich) ist die Hypothese, dass der gesamte Voynich-Text nur bedeutungslosen Unfug enthält.

Allerdings tappt die Voynich-Forschung bezüglich dieser Fragen noch reichlich im Dunkeln. Die Befürworter der Verschlüsselungstheorie konnten bisher noch nicht erklären, welches Verfahren der Verfasser verwendete. Eine erfolgreiche Kryptoanalyse gelang ohnehin nicht. Auch nach einer passenden Kunstsprache oder Sprachveränderung suchen Voynichologen bisher vergebens. Selbst die Unfug-Theorie leidet darunter, dass bisher niemand herausgefunden hat, mit welcher Methode der Urheber einen sinnlosen Buchstabensalat mit den entsprechenden statistischen Eigenschaften produziert hat.

Wenn Sie mehr über das Voynich-Manuskript und die zahlreichen, teilweise widersprüchlichen Theorien zu diesem Thema wissen wollen, dann empfehle ich

Ihnen meinen online verfügbaren Artikel [Schm09/1]. Dort habe ich auch einige Ideen für zukünftige Untersuchungen aufgeführt, die etwas mehr Klarheit bringen könnten.

4.5.2 Rohonczi-Kodex

Angesichts der vergleichsweise großen Popularität des Voynich-Manuskripts wird oft übersehen, dass es noch ein weiteres Buch gibt, dessen Inhalt ungelöst ist: den Rohonczi-Kodex. Dabei handelt es sich um ein aus Ungarn stammendes Buch, das im Mittelalter entstanden ist. Der Rohonczi-Kodex hat etwa doppelt so viele Seiten wie das Voynich-Manuskript, dafür sind die (unbekannten) Buchstaben deutlich größer.

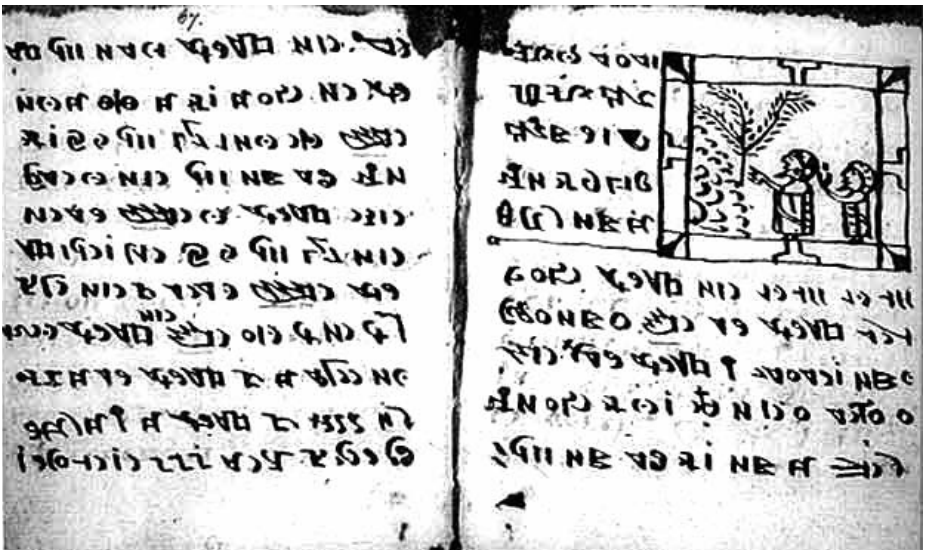

Abb. 4–6 *Der Rohonczi-Kodex ist ein weiteres ungelöstes Rätsel aus der Geschichte der Kryptografie. Bisher haben sich nur wenige damit beschäftigt.*

Leider haben Krypto-Historiker dem Rohonczi-Kodex bisher nicht die Aufmerksamkeit zukommen lassen, die er verdient hätte. Die Fachzeitschrift Cryptologia hat bis heute keinen einzigen Artikel zu diesem Thema veröffentlicht. Es gibt nur wenige Untersuchungen des rätselhaften Texts, und praktisch die gesamte Fachliteratur ist auf Ungarisch verfasst. Wenn Sie also eine spannende Aufgabe suchen (und vielleicht sogar Ungarisch können), dann sollten Sie eine Beschäftigung mit dem Rohonczi-Kodex in Erwägung ziehen. Da sich bisher nur wenige mit diesem Thema auseinandergesetzt haben, stehen die Chancen, den Text zu entschlüsseln, nicht einmal schlecht. Ich würde mich in jedem Fall freuen, wenn es in den nächsten Jahren neue Veröffentlichungen zum Rohonczi-Kodex gäbe.

4.5.3 Dorabella-Chiffre

Im Vergleich zum Voynich-Manuskript und zum Rohonczi-Kodex wirkt ein weiteres ungelöstes Rätsel der Krypto-Geschichte eher unscheinbar: die Dorabella-Chiffre. Unter diesem Namen ist ein gerade einmal 87 Buchstaben langer Geheimtext bekannt, den der britische Komponist Edward Elgar (1857–1934) im Jahr 1897 an eine Bekannte schickte. Der Text ist in Phantasiebuchstaben verfasst, die jeweils aus einem oder mehreren Bögen bestehen. Die Dorabella-Chiffre blieb der Nachwelt erhalten, bisher hat jedoch niemand die Lösung gefunden.

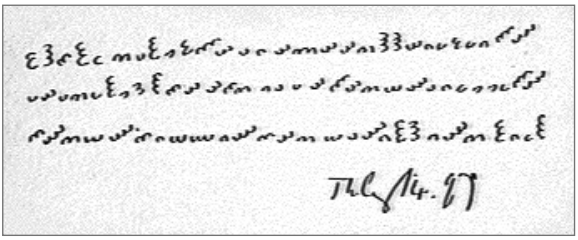

Abb. 4–7 *Die Dorabella-Chiffre aus dem Jahr 1897 ist bisher ungelöst.*

5 Die Enigma und andere Verschlüsselungsmaschinen

Um das Jahr 1920 begann in der Kryptografie eine neue Ära und damit eines der spannendsten Kapitel der Technikgeschichte. Noch im Ersten Weltkrieg hatten die beteiligten Armeen ihre Funksprüche mit Verfahren verschlüsselt, die meist der Vigenère-Chiffre ähnelten und sich mit Papier und Bleistift durchführen ließen. Die Folgen waren oft verheerend, denn praktisch alle damals eingesetzten Chiffren wurden früher oder später vom jeweiligen Kriegsgegner geknackt. Der Bedarf an verbesserten Verschlüsselungsverfahren war daher offensichtlich und rief nach Kriegsende verschiedene Tüftler auf den Plan, die erstmals spezielle Maschinen für die Verschlüsselung entwickelten. Bereits in den zwanziger Jahren kamen mehrere Geräte dieser Art auf den Markt. Bis zum Aufkommen des Computers gehörten derartige Verschlüsselungsmaschinen zur Standardausstattung von Behörden und Militär.

Zur gleichen Zeit rüsteten jedoch auch die Codeknacker kräftig auf. Sie betrieben ihr Handwerk teilweise in industriellen Dimensionen und schafften es immer wieder, scheinbar sichere Verschlüsselungsmaschinen zu knacken. Vor allem

der Zweite Weltkrieg war von einem unglaublichen Wettlauf zwischen Kryptografen und Dechiffrierern geprägt, dessen Einzelheiten erst Jahrzehnte später öffentlich bekannt wurden. Dabei spielte nicht zuletzt die legendäre deutsche Verschlüsselungsmaschine Enigma eine wichtige Rolle. Auch sie galt als sicher und wurde doch geknackt.

Die ausgesprochen faszinierende Geschichte der mechanischen Verschlüsselungsmaschinen, die bis etwa 1970 dauerte, wird ausführlich in meinem Buch *Codeknacker gegen Codemacher* beschrieben [Schm07/1]. An dieser Stelle will ich mich mit einer kurzen Zusammenfassung begnügen, in der neben historischen Aspekten auch die verwendeten Verfahren betrachtet werden.

5.1 Rotorchiffren

Zu den wichtigsten Pionieren der maschinellen Verschlüsselungstechnik gehörte der US-Amerikaner Edward Hebern. Dieser kam 1918 auf die Idee, ein elektromechanisches Gerät zu bauen, das Texte verschlüsselte, die über eine Schreibmaschinentastatur eingegeben wurden.

5.1.1 Heberns Rotormaschine

Das Design von Heberns Maschine sah eine oder mehrere kreisrunde Scheiben (Rotoren) vor, die auf beiden Seiten mit jeweils 26 Metallkontakten versehen waren. Im Folgenden gehen wir von drei derartigen Rotoren aus. Jeder Kontakt auf der einen Seite eines Rotors war mit einem Kontakt auf der anderen Seite verdrahtet. Die drei Rotoren waren wie bei einem Tachometerzähler aneinandergekoppelt. Wurde ein Kontakt auf der linken Seite des linken Rotors durch Drücken einer von 26 Tasten mit einer Stromquelle verbunden, dann floss Strom durch alle drei Rotoren hindurch und brachte nach dem dritten Rotor eine von 26 angeschlossenen Lampen zum Aufleuchten. Jede Taste war mit einem Buchstaben beschriftet, jede Lampe ebenfalls.

Durch diese Anordnung ließ sich jeder Buchstabe auf einen durch die Rotorverdrahtung festgelegten anderen abbilden – dadurch entstand ein Verschlüsselungsverfahren (siehe Abbildung 5–1). Dieses wurde dadurch noch komplizierter, dass nach jedem Tastendruck der linke Rotor um eine Einheit gedreht wurde. Nach einer vollen Umdrehung drehte sich auch der mittlere Rotor um eine Einheit, entsprechend nach einer vollen Umdrehung des mittleren der rechte (wie beim Tachometerzähler).

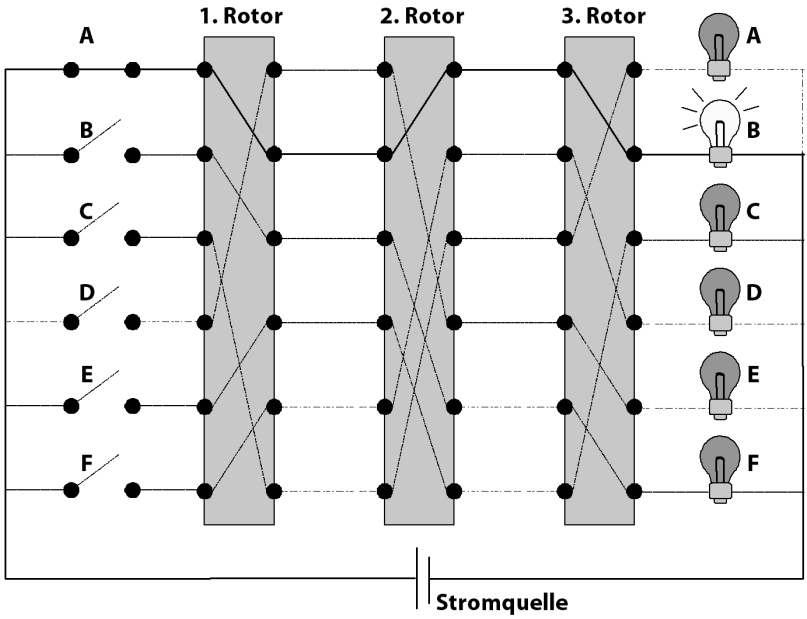

Abb. 5–1 *Eine Rotorchiffre mit drei Rotoren (statt 26 sind nur sechs Buchstaben vorhanden): Wird die »A«-Tastege drückt, dann leuchtet durch die Verdrahtung die »B«-Lampe auf. Da sich die Rotoren drehen, ändert sich der Weg des Stroms ständig.*

Eine Chiffre dieses Typs wird **Rotorchiffre** genannt. Fast zeitgleich mit Edward Hebern kamen drei weitere Erfinder auf die Idee, eine Maschine dieser Art zu bauen. Der bekannteste davon war Arthur Scherbius, von dem noch die Rede sein wird (seine Maschine war die Enigma). Aus Kryptografen-Sicht ist eine Rotorchiffre eine polyalphabetische Substitutionschiffre. Die Tabelle, nach der aus dem Klartext der Geheimtext gebildet wird, ändert sich nach jedem Buchstaben, da sich nach jeder Eingabe mindestens ein Rotor dreht. Erst wenn sich der rechte Rotor einmal komplett gedreht hat, wiederholt sich die Substitutionsvorschrift. Dies ist erst nach 26^3 (also 17.576) Buchstaben der Fall.

Wie jedes gute Verschlüsselungsverfahren, so arbeiten auch Rotorchiffren mit einem Schlüssel. Geht man davon aus, dass die Verdrahtung der Rotoren über längere Zeit konstant bleibt und Mallory bekannt ist, dann ist die Anfangsstellung der Rotoren der Schlüssel. Die Anzahl der Schlüssel ist dann so groß wie die der Rotorstellungen und beträgt damit 17.576. Diese Zahl lässt sich noch deutlich erhöhen, wenn man die Rotoren austauschen kann. Hat man beispielsweise fünf unterschiedlich verdrahtete Rotoren zur Verfügung und kann davon jeweils drei in beliebiger Reihenfolge einsetzen, dann versechzigfacht sich die Anzahl der Schlüssel auf etwa eine Million. Die meisten Anwender von Rotorchiffren gingen zudem davon aus, dass der Angreifer die Verdrahtung der Rotoren nicht kannte.

Die Erfindung einer Rotor-Chiffriermaschine brachte Edward Hebern übrigens kein Glück. Zwar erhielt er 1924 ein Patent für sein Gerät. Abgesehen von einigen Testexemplaren blieb seine eigens gegründete Firma jedoch auf den Maschinen sitzen und musste 1926 Konkurs anmelden. Nachdem sich das Militär in den USA Jahre später dann doch für den Einsatz von Rotorchiffren entschloss, versuchte Hebern 1947 eine Entschädigung von 50 Millionen US-Dollar einzuklagen. Der Erfolg war jedoch wieder bescheiden: 1958, vier Jahre nach seinem Tod, erhielten seine Erben 30.000 US-Dollar zugesprochen.

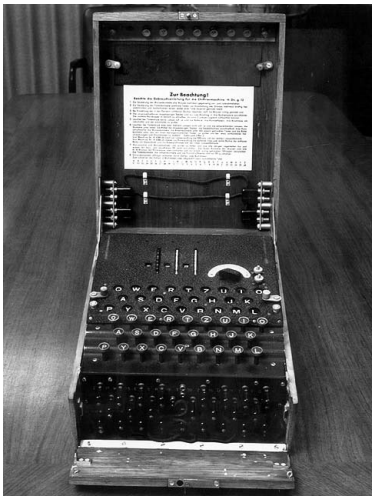

Abb. 5–2 *Die Enigma wurde im Zweiten Weltkrieg von den Deutschen eingesetzt. Sie gilt als die berühmteste Verschlüsselungsmaschine der Welt.*

5.1.2 Die Enigma

Ebenfalls um das Jahr 1918 baute der Deutsche Arthur Scherbius unabhängig von Hebern eine Verschlüsselungsmaschine, die eine Rotorchiffre realisierte. Seiner Maschine, die 1926 patentiert wurde, gab er den bezeichnenden Namen **Enigma** (griechisch für »Rätsel«) – sie wurde später zur bekanntesten Verschlüsselungsmaschine überhaupt. Die Enigma hatte in ihrer gängigsten Variante drei Rotoren. Es gab jedoch ein zusätzliches Bauteil: Hinter dem dritten Rotor war ein weiterer, unbeweglicher Rotor (ein sogenannter Reflektor) angebracht, der nur auf einer Seite Kontakte hatte. Diese waren miteinander paarweise verdrahtet (siehe Abbildung 5–3). Wurde eine der 26 Tasten gedrückt, dann floss der Strom durch die drei Rotoren in den Reflektor und von dort wieder zurück, wiederum durch die drei Rotoren hindurch, um danach eine Lampe zum Leuchten zu bringen. Der Reflektor, so dachte man damals, würde die Maschine deutlich sicherer machen – ein fataler Irrtum, wie wir heute wissen.

Auch Scherbius konnte sich nicht lange über seine Erfindung freuen. 1926 starb er nach einem Unfall, und 1934 ging seine Firma in Konkurs. Bereits Ende der zwanziger Jahre setzte jedoch die Deutsche Wehrmacht die Enigma für militärische Zwecke ein und bescherte der Nachfolgegesellschaft von Scherbius' Unternehmen Ende der 30er Jahre dann doch noch ein einträgliches Geschäft.

Kryptoanalyse der Enigma

Wie die Enigma von polnischen und britischen Kryptografen zwischen 1928 und 1945 trotz ständiger Verbesserungen immer wieder geknackt wurde, ist vermutlich die spannendste Geschichte, welche die Kryptografie überhaupt zu bieten hat.

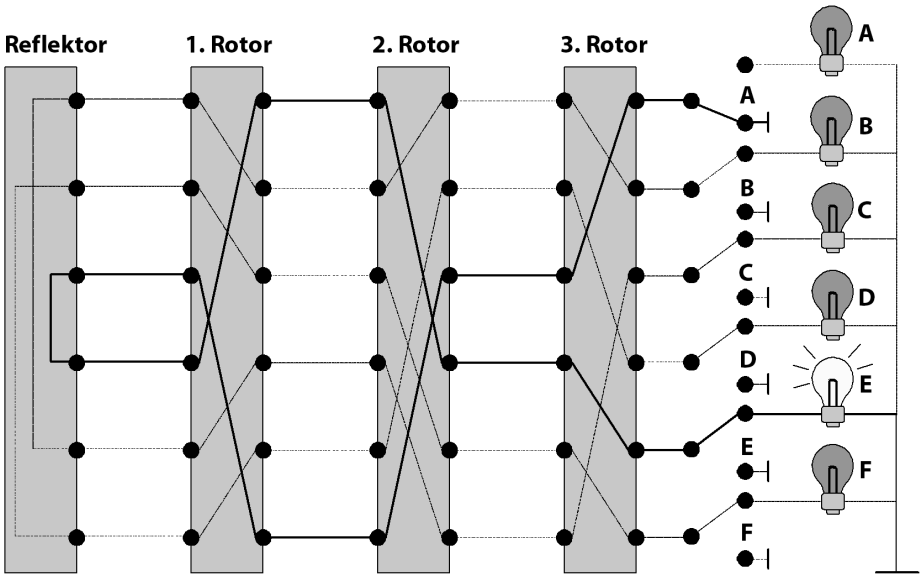

Abb. 5–3 *Die Enigma realisiert eine Rotorchiffre, bei der jeder Rotor zweimal durchlaufen wird . Diese Eigenschaft wird durch den Reflektor gewährleistet, der nur auf einer Seite Kontakte hat.*

Den Anfang dieser Geschichte markierte das Jahr 1927, als sich der polnische Geheimdienst eine der damals noch käuflich erwerbbaren Enigma-Maschinen besorgte und dadurch die Funktionsweise der Maschine kannte (dies bestätigt, dass man immer davon ausgehen sollte, dass der Abhörer das Verfahren kennt). Die drei polnischen Mathematiker Marian Rejewski, Henryk Zygalski und Jerzy Rozycki machten sich in der Folgezeit an die Arbeit und konnten schon bald erste Erfolge verzeichnen. Nicht zuletzt auch dank der Unterstützung durch einen Spion gelang es ihnen 1932, die Verdrahtung von Wehrmacht-Enigmas zu rekonstruieren. Bereits im folgenden Jahr waren sie so weit, dass sie die jeweilige Rotor-Anfangsstellung (also den Schlüssel) bestimmen konnten, wodurch sie die Enigma geknackt

hatten. 1938 schafften es Rejewski und seine Kollegen sogar, eine Maschine zu konstruieren, die das Entschlüsseln von Enigma-Nachrichten deutlich erleichterte und als Vorläufer heutiger Computer betrachtet werden kann. Die Erfinder nannten die Maschine »Bomba« nach dem polnischen Wort für Eisbombe.

Probleme machte den Polen allerdings die Tatsache, dass die Deutschen unterschiedliche Enigma-Versionen verwendeten (insgesamt mindestens 50 bis Ende des Kriegs) und für besonders sicherheitskritische Bereiche einen vierten Rotor und weitere Verbesserungen einführten. Diese Übermacht veranlasste die polnischen Mathematiker 1938 dazu, den britischen Geheimdienst einzuweihen. Die Briten wussten die Informationen zu nutzen. Unter Mitwirkung des bedeutenden Mathematikers Alan Turing entwickelten sie die Bomba zu einer leistungsfähigen Maschine weiter, die sie »Bombe« nannten (auch dies bedeutet »Eisbombe« und ist nicht mit dem Wort »bomb« zu verwechseln). Im Deutschen ist der Begriff **Bombe** bzw. **Turing-Bombe** verbreitet. In ihrem Dechiffrier-Zentrum in Bletchley Park bei London betrieben die Briten bis zum Ende des Zweiten Weltkriegs die Enigma-Kryptoanalyse mithilfe von Turing-Bomben in industriellen Ausmaßen. Bis zu 7.000 Mitarbeiter – darunter viele Frauen – waren dort unter strengster Geheimhaltung mit dem Dechiffrieren beschäftigt. Die meisten Angestellten kannten nur ihr unmittelbares Arbeitsumfeld und wussten daher nicht, was für eine entscheidende Bedeutung ihre Arbeit hatte.

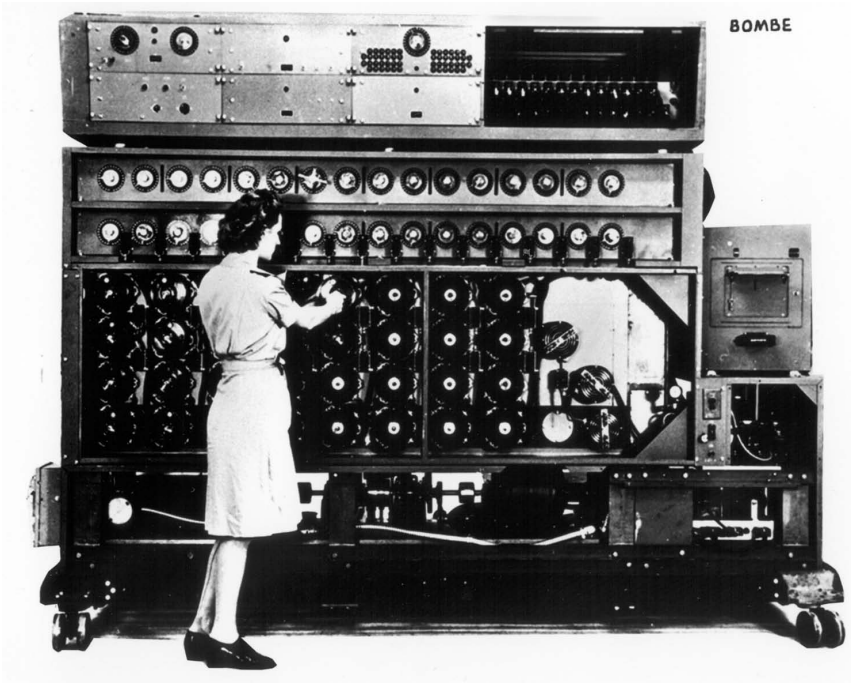

Abb. 5–4 *Mit der Turing-Bombe knackten die Briten die Enigma.*

Mithilfe der Dechiffrier-Fabrik in Bletchley Park gelang es den Briten zwar, einen Großteil der abgefangenen deutschen Funksprüche zu entschlüsseln. Die zahlreichen Enigma-Varianten und die diversen Verbesserungen machten jedoch auch ihnen zu schaffen, und so gab es durchaus auch Nachrichten, welche die Briten nicht lösen konnten. Dennoch ist heute klar: Die erfolgreiche Kryptoanalyse der Enigma hatte einen enormen Einfluss auf den Verlauf des Zweiten Weltkriegs. Vor allem der U-Boot-Krieg im Nordatlantik wäre ohne die geknackte Enigma anders verlaufen, denn durch abgefangene und entschlüsselte Funksprüche waren die Alliierten oftmals bestens über die Position der deutschen U-Boote informiert. Möglicherweise hätte Deutschland im Zweiten Weltkrieg sogar eine Atombombe abbekommen, wenn die Enigma nicht geknackt worden wäre. Denn dies hätte den Krieg zweifellos verlängert, und bekanntlich warfen die Amerikaner bereits drei Monate nach der Kapitulation Deutschlands die erste Atombombe auf Hiroshima.

Von der dramatischen Geschichte der Enigma erfuhr die Öffentlichkeit nach dem Zweiten Weltkrieg erst einmal nichts. Der britische Premierminister Winston Churchill ließ die Maschinen in Bletchley Park vernichten, die Resultate der Codeknacker blieben Staatsgeheimnis. Erst 1974 wurde die Sache öffentlich. Die ganze Wahrheit über die Enigma ist damit sicherlich noch nicht auf dem Tisch. Man kann beispielsweise nur darüber spekulieren, was die Sowjetunion über die Enigma wusste. Es ist kaum anzunehmen, dass sich von den zahlreichen hervorragenden sowjetischen Mathematikern keiner damit beschäftigte.

Wie die Enigma-Kryptoanalyse funktionierte

Die Kryptoanalyse der Enigma ist deutlich komplexer als die der Vigenère- oder gar der Cäsar-Chiffre. Ich kann auf dieses Thema daher nur überblicksweise eingehen. Zunächst einmal ist es wichtig zu wissen, dass eine Ciphertext-Only-Attacke auf die Enigma bei unbekannter Verdrahtung sehr schwierig ist. Es gibt jedoch wirksame Known-Plaintext-Attacken. Mit diesen gelang es den Polen und den Briten, die Verdrahtung einiger Maschinen zu bestimmen.

Zur Bestimmung des Schlüssels bei bekannter Verdrahtung (also der Rotor-Anfangsstellung) gibt es eine Ciphertext-Only-Attacke, bei der eine Eigenschaft der Enigma hilft, die auf den Reflektor zurückzuführen ist – obwohl gerade dieser die Maschine sicherer machen sollte. Wie Sie sich leicht überzeugen können, sorgt der Reflektor dafür, dass kein Buchstabe bei der Verschlüsselung auf sich selbst abgebildet werden kann. Kennt man ein längeres Wort, das irgendwo im Klartext vorkommen könnte (der Wortschatz im Krieg war ja begrenzt), dann schiebt man dieses so lange über den Geheimtext, bis kein Buchstabe des Worts mit dem Geheimtext übereinstimmt. Nun hat man mit einer gewissen Wahrscheinlichkeit ein Klartext-Geheimtext-Paar. Auf dieser Basis konnte der Schlüssel oft bestimmt werden.

Trotz all dieser Kryptoanalyse-Ansätze hätten die Polen und die Briten nicht allzu viel erreicht, wenn ihnen nicht einige günstige Umstände geholfen hätten.

Dazu gehörten etwa der bereits erwähnte Spion und die Tatsache, dass den Briten 1941 ein deutsches U-Boot samt Schlüsselbuch in die Hände fiel. Vor allem gehörte dazu aber auch die sträfliche Sorglosigkeit der Deutschen. Diese begingen so ziemlich jeden Fehler, den man bei der Nutzung eines Verschlüsselungssystems machen kann. Immer wieder verwendeten sie einfach zu erratende Anfangsstellungen (etwa AAA oder ABC). Ein täglicher Schlüsselwechsel bereitete den Dechiffrierern häufig keine großen Probleme, da Routinemeldungen oftmals mit gleichem Wortlaut und täglich zur gleichen Uhrzeit abgeschickt wurden – dies ermöglichte eine Known-Plaintext-Attacke. Solche und ähnliche Fehler erleichterten den Polen und Briten ihre Arbeit ungemein.

Bleibt noch die Frage, ob die Enigma ohne den Reflektor (also bei gleicher Bauweise wie die Hebern-Maschine) wesentlich sicherer gewesen wäre. Vermutlich nicht, denn auch die Hebern-Maschine ist zu knacken, wenn auch auf andere Weise. Der US-Kryptologe William Friedman (siehe Kapitel 39.1.3) demonstrierte dies im Jahr 1926. Erst spätere Generationen der Rotor-Chiffriermaschinen boten eine ausreichend hohe Sicherheit.

5.1.3 Weitere Rotor-Chiffriermaschinen

Schon in den dreißiger Jahren war einigen Experten bewusst, dass weder die Enigma noch die Hebern-Maschine ausreichende Sicherheit bot. Die Hinzunahme weiterer Rotoren konnte dieses Problem alleine nicht lösen, da sich nur bei sehr langen Funksprüchen mehr als drei Rotoren bewegen. Sowohl die Deutschen als auch die Briten und Amerikaner erkannten, dass stattdessen eine Änderung der Fortschaltung der Rotoren Abhilfe schaffen konnte. Diese sollten sich nicht mehr tachometerartig, sondern nach einem möglichst unregelmäßigen Mechanismus bewegen.

Auch die deutschen Krypto-Experten beschäftigten sich mit einer Änderung der Fortschaltung bei der Enigma. Sie kamen jedoch zu dem Schluss, dass ein solcher Schritt die Periode verkürzen würde, und verzichteten darauf. Die US-Amerikaner konstruierten dagegen eine neue Maschine, die sie SIGABA nannten. Es handelte sich dabei um eine Rotor-Chiffriermaschine mit 15 Rotoren, von denen jedoch nur fünf verdrahtet waren. Die restlichen zehn Rotoren steuerten die Fortschaltung der fünf verdrahteten. Die SIGABA-Rotoren drehten sich also nicht nach dem Tachometer-Prinzip, sondern nach einer komplexen Mechanik, die alle 15 Rotoren einbezog. Einen Reflektor gab es bei der SIGABA nicht. Für einen Außenstehenden war praktisch nicht nachvollziehbar, wie die Bewegung ablief.

Die komplexe Fortschaltung und die große Anzahl an Rotoren machten die SIGABA so sicher, dass sie nach heutigem Kenntnisstand nie geknackt wurde. Von Nachteil war lediglich, dass die SIGABA groß und unhandlich war. Sie war deshalb für den Einsatz im Gefecht nur bedingt geeignet. An der Front mussten

Abb. 5–5 *Die SIGABA wurde von den US-Amerikanern im Zweiten Weltkrieg eingesetzt. Sie bot eine größere Sicherheit als die Enigma.*

die US-Soldaten deshalb mit der deutlich weniger sicheren M-209 vorliebnehmen, von der noch die Rede sein wird.

Während die US-Amerikaner mit der SIGABA arbeiteten, hatten die Briten ein ähnliches Gerät namens **Typex**. Dieses arbeitete mit fünf unregelmäßig fortgeschalteten Rotoren und wurde ebenfalls – nach heutigem Kenntnisstand – nie geknackt. Allerdings war auch die Typex kein Gerät für den Einsatz an der Front, sondern wurde nur von hochrangigen Militärs verwendet.

Auch nach dem Zweiten Weltkrieg kamen noch zahlreiche Rotor-Chiffriermaschinen zum Einsatz. So entstand in der Schweiz die **NEMA** und in der Sowjetunion die **Fialka**. Auch die Schweizer Crypto AG brachte eine solche Maschine namens **HX-63** auf den Markt. Innerhalb der NATO wurde ein Gerät namens **KL-7** eingesetzt. Alle diese Maschinen wurden allem Anschein nach nie geknackt, da sie ausreichend viele Rotoren und eine komplexe Fortschaltmechanik hatten.

5.2 Andere Verschlüsselungsmaschinen

Nicht alle Verschlüsselungsmaschinen arbeiteten nach dem Rotorprinzip. Vor allem in den dreißiger Jahren, als die Nachfrage nach sicheren Verfahren deutlich zunahm, ließen sich die Konstrukteure einiges einfallen, um den Codeknackern ihr Handwerk zu erschweren. Im Zweiten Weltkrieg kamen mehrere unterschiedliche Typen von Verschlüsselungsmaschinen zur Anwendung, von denen noch die meisten geknackt wurden. Erst in den fünfziger Jahren gewannen die Chiffren-Designer gegenüber den Kryptoanalytikern die Oberhand, was einen entscheidenden Einschnitt in der langen Geschichte der Kryptografie darstellt.

5.2.1 Die Kryha-Maschine

Zu den Kuriositäten in der Kryptografie-Geschichte zählt zweifellos die Verschlüsselungsmaschine des ukrainischen Ingenieurs und Geschäftsmanns Alexander von Kryha. Diese wird als **Kryha-Maschine** bezeichnet. Von Kryha kam Anfang der zwanziger Jahre nach Deutschland, wo er sich als Unternehmer betätigte. Nachdem er zuvor beim ukrainischen Militär mit Verschlüsselung zu tun gehabt hatte, entwickelte er ein Verschlüsselungsgerät, das er um 1925 auf den Markt brachte. Es gab drei (kryptografisch gleichwertige) Varianten der Kryha-Maschine: die *Kryha Standard*, die *Kryha Liliput* und die *Kryha Elektrik*. Uns soll nur die Kryha Standard interessieren.

Die Kryha Standard enthielt einen Federantrieb und musste daher wie eine Uhr aufgezogen werden. Die Verschlüsselung wurde durch zwei konzentrische Buchstabenscheiben angezeigt, von denen sich die innere drehte. Im Innern der Maschine steckte ein unregelmäßig gezahntes Rad, das in 17 Einheiten aufgeteilt war. Pro Knopfdruck drehte es sich – bewegt vom Federantrieb – mit der inneren Buchstabenscheibe um eine Einheit. Eine Einheit entsprach zwischen einem und sechs Buchstaben auf der Scheibe. Geht man davon aus, dass sich die Zahnung des Rads und die Position der Buchstaben auf der Scheibe nicht änderten, dann konnte die Maschine 442 Zustände annehmen (dies ergibt sich aus 17 Zahnradstellungen und 26 Möglichkeiten, die Buchstabenscheibe dagegen zu verdrehen). Dies entsprach der Zahl der möglichen Schlüssel. Es versteht sich von selbst, dass eine Verschlüsselungsmethode mit einer so geringen Schlüsselzahl nicht besonders sicher ist.

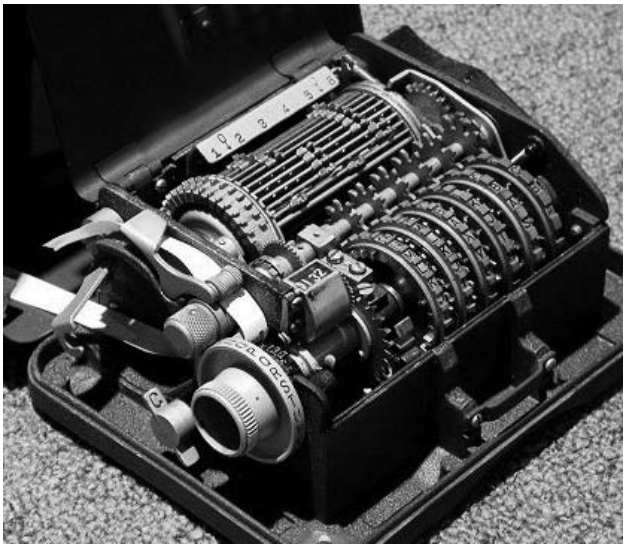

Abb. 5–6 *Die Kryha-Maschine bot keine hohe Sicherheit.*

Der wenig anspruchsvolle Aufbau der Kryha-Maschine zeigt: Im Gegensatz zu anderen Erfindern von Verschlüsselungsmaschinen war Alexander von Kryha kein überragender Techniker. Dafür war er ein begnadeter Selbstdarsteller und Vermarktungsexperte. Er verpasste seiner Maschine ein modernes Aussehen und verkaufte sie in einer samtgefütterten Ledertasche. Die Werbematerialien, die von Kryha drucken ließ, waren anspruchsvoll gestaltet und wirken heute noch erstaunlich aktuell. Zusätzlich startete der umtriebige Unternehmer mehrere PR-Aktionen und erreichte eine ausführliche Berichterstattung in den Medien.

Angesichts der aggressiven Vermarktung versäumte es von Kryha jedoch, sich um die kryptografischen Eigenschaften seiner Maschine zu kümmern. Dabei wäre dies dringend notwendig gewesen, denn die Kryha-Maschine zählte zu den unsichersten Verschlüsselungsmaschinen, die je gebaut wurden. Der bereits erwähnte US-Kryptologe William Friedman knackte das Gerät 1933 in weniger als drei Stunden. Das US-Militär setzte die Kryha-Maschine deshalb nie ein. Auch ansonsten glückten dem charismatischen Ukrainer nur wenige Verkaufserfolge. Militärische Kunden entschieden sich meist für andere Maschinen, und in der Wirtschaft war die Nachfrage zu gering. Die Kryha-Maschine erwies sich daher als kommerzieller Flop.

5.2.2 Hagelin-Maschinen

Auch wenn sich die Kryha-Maschine ordentlich verkaufte, konnte es Alexander von Kryha sicherlich nicht mit dem wirtschaftlichen Erfolg aufnehmen, den der Schwede Boris Hagelin mit seinen Verschlüsselungsgeräten erzielte. Hagelin, der sowohl als Geschäftsmann als auch als Ingenieur hohes Ansehen erwarb, gründete in den zwanziger Jahren zusammen mit dem schwedischen Tüftler Arvid Damm ein Unternehmen für Verschlüsselungstechnik. Damm hatte um 1920 etwa zeitgleich mit Arthur Scherbius und Edward Hebern eine Rotor-Verschlüsselungsmaschine entwickelt und versuchte nun, diese zu vermarkten. Als Damm 1927 starb, musste Hagelin alleine weitermachen.

Nach einer längeren Durststrecke, die Hagelin nur durch die Unterstützung seines wohlhabenden Vaters überstand, kam für sein Unternehmen 1934 der Durchbruch. Als ersten großen Auftraggeber konnte Hagelin die französische Regierung gewinnen, die seine leicht abgewandelte Rotor-Verschlüsselungsmaschine **B-21** übernahm. Das nach leichten Modifikationen als **B-211** bezeichnete Gerät war kompakt und einfach zu bedienen, erwies sich jedoch später als unsicher. Doch immerhin, ein Anfang war gemacht.

Zum Markenzeichen Hagelins wurde ein Typ von Verschlüsselungsmaschinen, den er in den Jahren darauf im Auftrag der Franzosen erfand. 1935 kam die erste davon unter dem Namen **C-35** auf den Markt. Das Design dieser als **C-Maschinen** bezeichneten Geräte basierte auf einer Geldwechselmaschine, die Hagelin einige Jahre zuvor entwickelt, aber nie gebaut hatte. Das Herzstück der

C-Maschinen bildete ein Rad (Stangenrad), das sich bei der Eingabe eines Buchstabens um 360 Grad drehte und dabei eine Buchstabenscheibe antrieb. Dieser Antrieb war zusätzlich von mehreren unregelmäßig gezahnten Rädern abhängig, deren Zahnung sich ändern ließ.

Abb. 5–7 *Die B-211 von Hagelin war etwa zur gleichen Zeit wie die Enigma im Einsatz. Sie erwies sich als unsicher, was sich jedoch bei den Nachfolgemodellen ändern sollte.*

Zu Hagelins größtem Verkaufserfolg wurde eine C-Maschine, die er an die US-Armee verkaufen konnte. Unter dem Namen **M-209** produzierten die USA in Lizenz insgesamt 140.000 Geräte dieses Typs. Diese kamen im Zweiten Weltkrieg in der US-Armee zum Einsatz. Im Gegensatz zur schweren und sperrigen SIGABA, die nur auf höherer militärischer Ebene verwendet wurde, ließ sich die M-209 bequem im Marschgepäck eines Soldaten unterbringen. Sie wurde dementsprechend vor allem für taktische Funksprüche eingesetzt.

Inzwischen weiß man, dass die M-209 unsicher war. Den Deutschen gelang es, die Maschine zu knacken, wie beispielsweise der ehemalige BSI-Präsident Dr. Otto Leiberich berichtet [Leiber]. 2004 hatte ich zudem die Gelegenheit, mich mit dem damals 84-jährigen Frankfurter Reinold Weber zu unterhalten, der seinerzeit am Knacken der M-209 beteiligt gewesen war und der nach über 60 Jahren erstmals öffentlich über seine Arbeit sprach. Die ausgesprochen spannende Geschichte Webers ist kostenlos im Internet nachzulesen [Schm04].

5.2.3 Die Purple

Im Jahr 1937 entwickelte die japanische Marine eine Verschlüsselungsmaschine, die »97-shiki O-bun In-ji-ki« hieß. Dieses Gerät, das in der Literatur meist als **Purple** bezeichnet wird, hatte einen ungewöhnlichen Aufbau, für den es anderswo keine Parallele gibt. Es spielte im Pazifikkrieg zwischen Japan und den USA eine wichtige Rolle. Bekannt wurde die Purple vor allem dadurch, dass es die Amerikaner in einer geradezu genialen Kryptoanalyse schafften, sie zu knacken.

Die japanischen Entwickler der Purple kannten die Enigma und ließen sich von deren Funktionsweise inspirieren. Anstatt auf Rotoren zu setzen, wählten sie jedoch Telefon-Vermittlungsschalter als wichtigstes Bauelement. Wie bei der Enigma drückte der Bediener eine Buchstabentaste auf einer Schreibmaschinentastatur, wodurch sich ein Stromkreis schloss, der den zugehörigen Geheimtextbuchstaben anzeigte.

Eine vereinfachte Purple-Variante ist in Abbildung 5–8 zu sehen. Der dort verwendete Telefonschalter hat drei Eingänge und pro Eingang drei Ausgänge. Über ein Verbindungsstück (*Zeiger*) ist jeder Eingang mit einem der drei zugehörigen Ausgänge verbunden. Mit der Eingabe eines Buchstaben bewegen sich alle drei Zeiger um eine Einheit nach unten (ist der unterste Ausgang erreicht, dann geht es mit dem obersten weiter). Die Verdrahtung zwischen den Ausgängen und den Lampen muss natürlich so gestaltet sein, dass nie zwei Zeiger bei derselben Lampe landen.

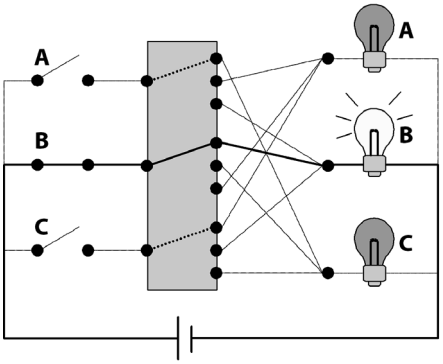

Abb. 5–8 *Die Purple (hier eine vereinfachte Version mit drei Buchstaben) arbeitete mit Telefon-Vermittlungsschaltern, in denen sich mehrere Zeiger synchron bewegten.*

Die echte Purple arbeitete mit 13 Vermittlungsschaltern. Jeder davon hatte sechs Ein- und 150 Ausgänge. Die Verdrahtung ist in Abbildung 5–9 zu sehen. Die mit x gekennzeichneten Elemente führen eine festverdrahtete Permutation durch, die uns an dieser Stelle nicht interessieren soll. Die jeweils 150 Ausgänge an einem Vermittlungsschalter sind nicht einzeln abgebildet. Wie man sieht, bleibt bei den

meisten Vermittlungsschaltern ein Eingang unbelegt. Die Anfangsstellung der Zeiger diente als Schlüssel. Die Ausgabe erfolgte nicht über Lampen, sondern wie bei einer elektrischen Schreibmaschine.

Die Purple war zwar komplexer aufgebaut als die Enigma, doch dafür war es einfacher, bei bekanntem Aufbau den Schlüssel zu ermitteln. Es gibt Hinweise darauf, dass deutsche Dechiffrier-Spezialisten im Dritten Reich die Purple knacken konnten. Sie taten dies, obwohl die Japaner mit dem Deutschen Reich verbündet waren. Es ist jedoch anzunehmen, dass die Deutschen Informationen über die Funktionsweise der Purple hatten.

Wesentlich mehr Raum in der Literatur nimmt das Knacken der Purple durch die US-Amerikaner während des Pazifikkriegs ein. William Friedman, der vielleicht beste Codeknacker der Krypto-Geschichte, war der Leiter des Kryptoanalyse-Projekts, in dem ein US-Team ab 1939 versuchte, die Purple zu dechiffrieren. Friedmans Truppe stand praktisch nichts zur Verfügung außer abgefangenen Purple-Geheimtexten, von denen sie in Einzelfällen auch den zugehörigen Klartext kannten. Informationen über den Aufbau der Maschine lagen nicht vor.

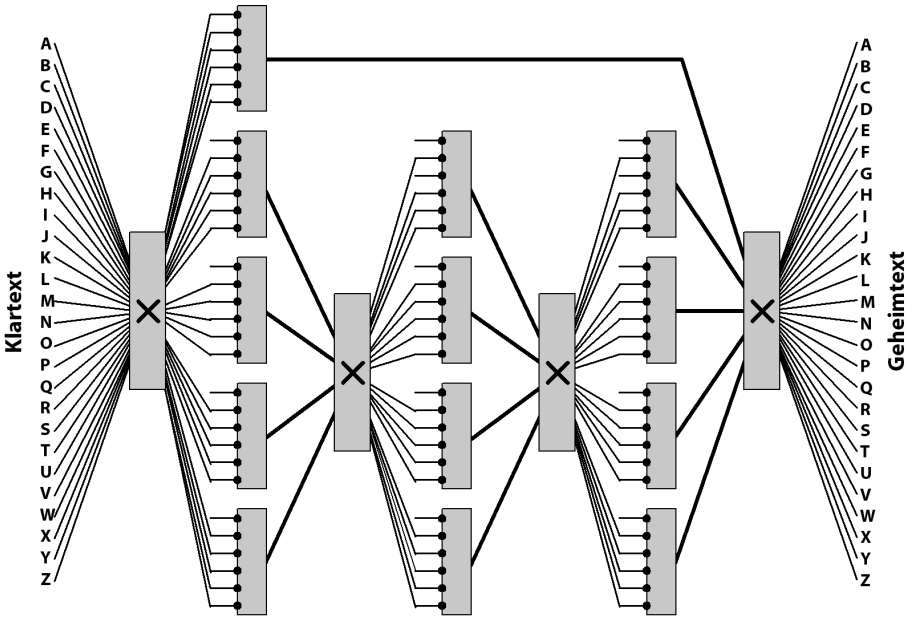

Abb. 5–9 *DiePurple arbeitete mit 13 Telefon-Vermittlungsschaltern, die je sechs Eingänge hatten (teilweise blieb einer davon ungenutzt). In jedem Schalter verbanden sechs Zeiger die Eingänge mit 150 Ausgängen. Zeiger und Ausgänge sind hier nicht abgebildet.*

Allerdings kannten die Amerikaner einige ältere japanische Verschlüsselungsmaschinen, wodurch sie ahnten, dass Telefon-Vermittlungsschalter zu den Bauelementen gehörten. In langwieriger Arbeit kamen Friedman und seine Leute dem Design der Purple auf die Spur. 1940 gelang es ihnen, das Gerät nachzubauen, auch eine Methode zur Berechnung des Schlüssels wurde gefunden. Ab 1941 konnten die Amerikaner den Funkverkehr der Japaner routinemäßig innerhalb weniger Stunden entschlüsseln. Eine der größten Leistungen in der Geschichte der Kryptoanalyse war perfekt.

5.2.4 Der Geheimschreiber

Die Enigma war nicht die einzige Verschlüsselungsmaschine, die die Deutschen im Zweiten Weltkrieg einsetzten. Das bekannteste unter den mindestens fünf anderen Geräten trug den Namen **T-52** und wird heute meist als **Geheimschreiber** bezeichnet. Es wurde von der Firma Siemens & Halske hergestellt. Im Vergleich zur Enigma handelte es sich dabei um ein größeres Gerät, das nur stationär einsetzbar war. Es wurde auf höherer militärischer Ebene eingesetzt und insgesamt in einigen hundert Exemplaren gebaut.

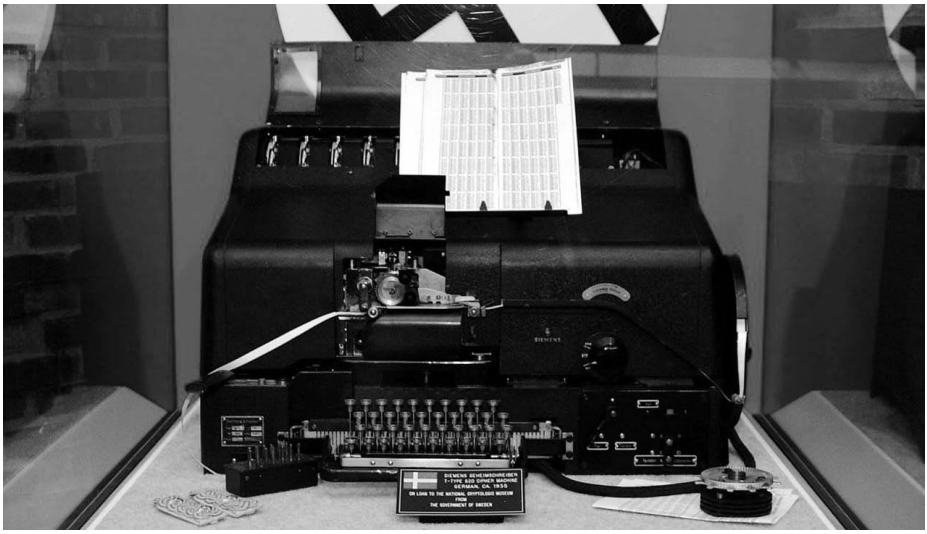

Abb. 5–10 *Der Geheimschreiber war nach der Enigma das bedeutendste deutsche Verschlüsselungsgerät des Zweiten Weltkriegs.*

Das Funktionsprinzip des Geheimschreibers unterschied sich deutlich von dem der Enigma. Zweck des Geräts war die Ver- und Entschlüsselung von Fernschreiben, die damals in einem fünfstelligen Binärcode (*Baudot-Code*) verschickt wurden. Aufgabe des Geheimschreibers war es also, einen Fünf-Bit-Wert auf einen

anderen abzubilden. Dies geschah online: Tippte der Bediener einen Buchstaben ein, dann wurde dieser nach der Verschlüsselung direkt per Fernschreiber verschickt. Umgekehrt druckte das Gerät eingehende Buchstaben nach der Entschlüsselung automatisch aus.

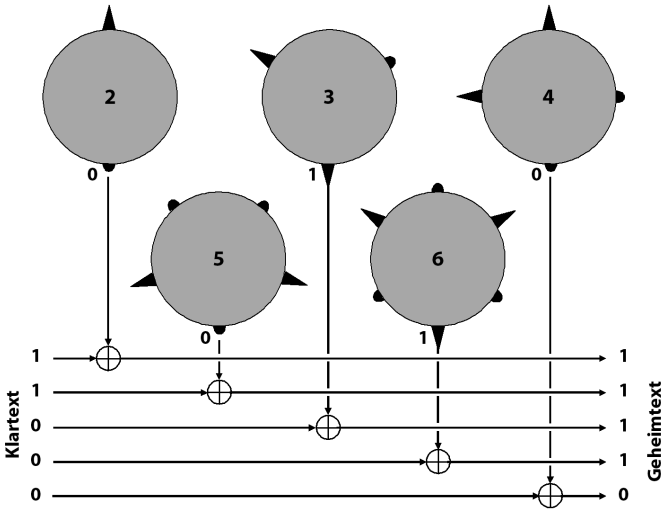

Abb. 5–11 *Vereinfachte Variante eines Geheimschreibers: Fünf gezahnte Räder bilden ein Muster von Nullen und Einsen, die mit dem Klartext exklusiv-oder-verknüpft werden.*

Eine vereinfachte Darstellung der Funktionsweise des Geheimschreibers ist in Abbildung 5–11 zu sehen. Das wichtigste Bauelement waren gezahnte Räder, deren Zähne teilweise gekürzt (nicht aktiv) waren. In der Abbildung sind fünf solcher Räder zu sehen. Die Anzahl der Zähne variiert von Rad zu Rad. Jeweils ein Zahn pro Rad nimmt eine Position ein, in der er »gelesen« wird (Leseposition). Befindet sich ein aktiver Zahn in der Leseposition, dann entspricht dies einer Null, ansonsten einer Eins. Zur Verschlüsselung werden die fünf Bit des Klartextbuchstabens mit den fünf Bit der Lesepositionen exklusiv-oder-verknüpft. Im Beispiel entsteht so aus der Zahl 11000 die Zahl 11110. Nach der Eingabe eines Buchstabens drehen sich alle fünf Zahnräder um jeweils einen Zahn weiter.

Die vollständige Funktionsweise des Geheimschreibers ist in Abbildung 5–12 ersichtlich. Dabei kommen zehn Räder zum Einsatz. Fünf davon liefern die zum Verschlüsseln verwendeten Bits. Die anderen fünf sorgen für deren Transposition. Die Anzahl der Zähne auf den Rädern beträgt zwischen 47 und 73 und ist so gewählt, dass der kleinste gemeinsame Teiler 1 ist. Dadurch wird eine möglichst lange Periode erreicht. Die Anfangsstellung der Räder entspricht dem Schlüssel.

Wer nun denkt, der Geheimschreiber hätte mehr Sicherheit geboten als die Enigma, der täuscht sich. Der schwedische Mathematiker Arne Beurling, der im

neutralen Schweden verschlüsselte Nachrichten aus dem besetzten Norwegen vorliegen hatte, schaffte es, eine frühe Version der Maschine in nur zwei Wochen zu knacken. Er brauchte dazu keine fremde Hilfe und keine Maschinen. Dies gilt neben dem Knacken der Purple als eine der größten Leistungen in der Geschichte der Kryptoanalyse.

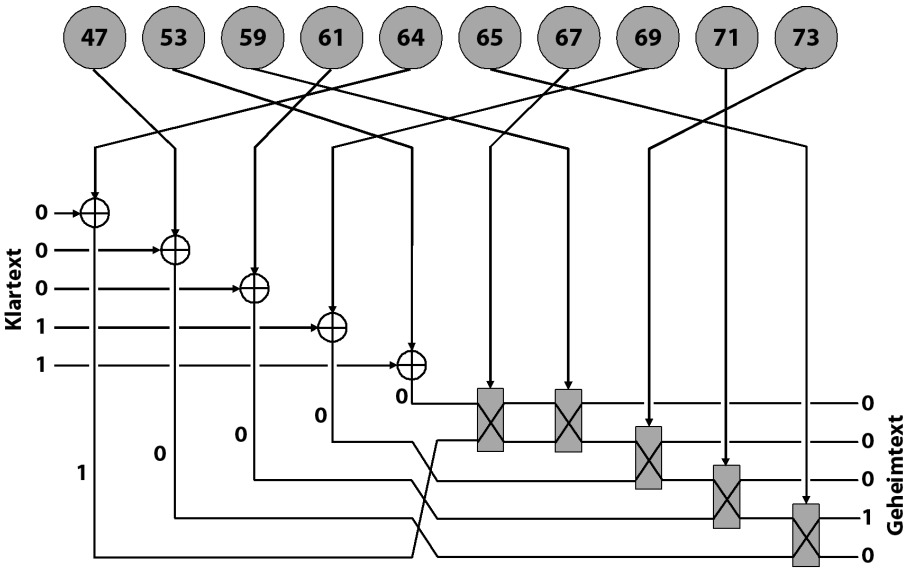

Abb. 5–12 *Der Geheimschreiber arbeitete mit zehn gezahnten Rädern. Fünf davon beeinflussten den Klartext direkt, die anderen fünf sorgten für eine zusätzliche Durchmischung.*

5.2.5 Lorenz-Maschine

Für die Verschlüsselung auf höchster staatlicher Ebene setzten die Deutschen im Zweiten Weltkrieg weder die Enigma noch den Geheimschreiber ein. Vielmehr gab es für diesen besonders wichtigen Bereich eine dritte Verschlüsselungsmaschine: die **Lorenz-Maschine**. Diese diente wie der Geheimschreiber der Verschlüsselung von Fernschreiben und verwendete den bereits erwähnten Baudot-Code. Im Gegensatz zum Geheimschreiber hatte die Lorenz-Maschine keine Tastatur, sondern wurde an einen Fernschreiber angeschlossen.

Die Funktionsweise der Lorenz-Maschine ähnelte dem des Geheimschreibers. Der Aufbau sah gezahnte Räder mit aktiven und passiven Zähnen vor. Insgesamt gab es 12 Räder, wobei die Zahl der Zähne zwischen 23 und 61 lag (die Räder werden im Folgenden mit der Anzahl ihrer Zähne bezeichnet). Nur die Räder mit 41, 31, 29, 26 und 23 Zähnen drehten sich mit jedem Buchstaben. Rad 37 drehte sich nur dann, wenn die Leseposition von Rad 61 auf 1 stand. Stand die Leseposition

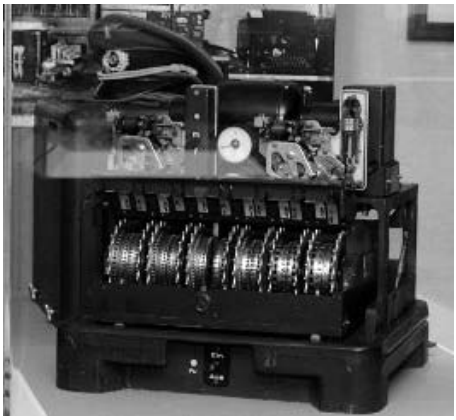

Abb. 5–13 *Die Lorenz-Maschine kam auf höchster militärischer Ebene zum Einsatz. Die Briten konnten sie knacken.*

von Rad 37 auf 1, dann drehten sich auch die Räder 59, 53, 51, 47 und 43, die den Klartext direkt beeinflussten.

Wie die Enigma und der Geheimschreiber wurde auch die Lorenz-Maschine geknackt. Die Geschichte dieser Kryptoanalyse ist mindestens so spannend wie die der Enigma und wurde ebenfalls von britischen Spezialisten in der Dechiffrier-Fabrik in Bletchley Park durchgeführt. Um das Dechiffrieren zu bewerkstelligen, entwickelten die dortigen Kryptoanalytiker eine spezielle Maschine, die bereits einige Merkmale eines Computers hatte (sie arbeitete mit binären Daten, war jedoch nicht frei programmierbar). Der Name dieser kleiderschrankgroßen Maschine war **Colossus**. Ein Nachbau dieses technischen Wunderwerks ist heute im Museum von Bletchley Park zu bewundern.

5.2.6 Schlüsselgerät 41 (Hitler-Mühle)

Zu den weniger bekannten deutschen Verschlüsselungsmaschinen aus dem Zweiten Weltkrieg gehört das **Schlüsselgerät 41**, das auch als **Hitler-Mühle** bezeichnet wird. Das Interesse an diesem durchaus bemerkenswerten Gerät ist leider erst in den letzten Jahren erwacht. Eine von dem Stuttgarter Verschlüsselungsmaschinen-Experten Klaus Kopacz angestellte Suche nach Zeitzeugen, die in die Entwicklung oder Produktion des Schlüsselgeräts 41 involviert waren, blieb bisher erfolglos.

Das Schlüsselgerät 41 entstand vermutlich 1941, also während des Zweiten Weltkriegs. Ziel der Konstrukteure war es, mit dieser Maschine die damals in der deutschen Armee zu Zehntausenden eingesetzte Enigma zu ersetzen. Zwar wussten die Deutschen nicht, dass die Briten die Enigma zu diesem Zeitpunkt längst geknackt hatten, doch die mangelnde Sicherheit ihrer wichtigsten Verschlüsse-

lungsmaschine war einigen deutschen Kryptologen durchaus bewusst. Außerdem war das Schlüsselgerät 41 im Vergleich zur Enigma handlicher und leichter zu bedienen. Gegen Kriegsende lagen den Wanderer-Werken in Chemnitz, wo das Gerät gebaut wurde, 13.000 Bestellungen vor, allerdings wurden nur 500 davon ausgeliefert. Vermutlich kam das Gerät vereinzelt zum Praxiseinsatz, doch auch diesbezüglich sind keine Zeitzeugenberichte verfügbar.

Technisch gesehen war das Schlüsselgerät 41 eng mit den C-Maschinen von Boris Hagelin verwandt. Man kann sogar von einem Ideenklau sprechen. Allerdings bauten die deutschen Entwickler einen zusätzlichen Mechanismus ein, der die Verschlüsselung vermutlich noch sicherer machte. Leider hat sich meines Wissens bisher niemand mit den mathematischen Details dieses Geräts beschäftigt. Zweifellos wäre der Zweite Weltkrieg anders verlaufen, wenn die Deutschen früher von der unsicheren Enigma auf diese Maschine umgestellt hätten.