
2.1 Beispiele für Verschlüsselungen

Früher war es vor allem ein Anliegen des Militärs, von Geheimdiensten und Politikern, über Methoden zur sicheren Übermittlung vertraulicher Nachrichten zu verfügen. Historische Verfahren zur Lösung dieser Aufgabe stellen Anfänge der Kryptologie dar, die die Teilgebiete Kryptographie und Kryptoanalyse umfasst. Beide Gebiete sind eng miteinander verbunden. Bei der Kryptographie steht die Entwicklung und Anwendung von Verschlüsselungsverfahren im Vordergrund, während es bei der Kryptoanalyse um das Erkennen von Schwächen zur Sicherheitsbeurteilung dieser Verfahren geht.

Zunächst werden wir einige Beispiele aus der Geschichte der Verschlüsselungen vorstellen und die Grenzen in der Sicherheit zeigen, die diese Verfahren bieten.

Schon die Spartaner nutzten vor fast 2500 Jahren die Skytale, um militärische Botschaften geheimzuhalten: Wird ein Stab mit festem Durchmesser spiralförmig von einem Pergamentstreifen umwickelt, kann der Absender seine Nachricht längs auf den Stab schreiben. Nach dem Abwickeln des Streifens wird sie zu einer unverständlichen Zeichenfolge, weil die Reihenfolge der Buchstaben aus der Nachricht verändert worden ist. Die Verschlüsselung mittels Skytale ist das erste Beispiel einer *Permutationschiffre*: die Zeichen der Nachricht werden permutiert.

Definition 2.1 *Man spricht von einer Permutationschiffre, wenn die Nachricht $m = m_0 m_1 \dots m_{\ell-1}$ zur Zeichenfolge $m_{\pi(0)} m_{\pi(1)} \dots m_{\pi(\ell-1)}$ verschlüsselt wird, wobei π eine Permutation auf der Menge $\{0, 1, \dots, \ell-1\}$ ist.*

Um aus dem Ergebnis der Verschlüsselung wieder einen sinnvollen Text herauslesen zu können, benötigt der Empfänger der Nachricht einen Stab mit dem gleichen Durchmesser wie der beim Notieren der Nachricht verwendete. Dieser Stab darf nicht gemeinsam mit der Nachricht transportiert werden, weil sonst jeder den Inhalt des Textes erfahren könnte.

Vor etwa 2000 Jahren wurde zum ersten Mal die sogenannte Caesar-Chiffre eingesetzt, die – wie der Name schon sagt – vom römischen Staatsmann und Feldherrn Julius Cäsar

für seine militärische Korrespondenz verwendet wurde: Jeder Buchstabe der Nachricht wird dabei durch den dritten auf ihn folgenden Buchstaben aus dem Alphabet ersetzt. So wird zum Beispiel das Wort CAESAR zur Buchstabenfolge FDHVDU verschlüsselt. Für die Einzelbuchstaben der Nachricht gilt dabei die Verschlüsselungstabelle:

Nachrichtenbuchstabe	A	B	C	D	E	...	Z
verschlüsselter Buchstabe	D	E	F	G	H	...	C

Diese Tabelle berücksichtigt nur Buchstaben; üblicherweise wurden beim Verschlüsseln von Texten Interpunktionszeichen ausgelassen. Dies ist durchaus sinnvoll, da diese Zeichen die Analyse des verschlüsselten Textes erleichtern würden.

Hier werden Einzelbuchstaben des Alphabets, über dem die Nachricht abgefasst worden ist, unabhängig voneinander ersetzt; gleiche Buchstaben der Nachricht werden stets zu gleichen Buchstaben verschlüsselt.

Definition 2.2 *Verschlüsselungen, bei denen Einzelbuchstaben des Alphabets, über dem die Nachricht abgefasst worden ist, unabhängig von ihrer Position im Text durch Zeichen ersetzt werden, die den Buchstaben durch eine Verschlüsselungstabelle eineindeutig zugeordnet sind, nennt man **monoalphabetische monographische Substitutionen (MM-Substitutionen)**.*

Monographisch bzw. monoalphabetisch heißen diese Substitutionen deshalb, weil Einzelbuchstaben ersetzt bzw. nur ein Alphabet zur Abfassung des verschlüsselten Textes verwendet wird.

Jeder, der die Verschlüsselungsmethode kennt, kann bei der Caesar-Chiffre durch Zurückzählen in der Folge der Buchstaben um $k = 3$ Schritte leicht das Original finden. Analog kann man beim Alphabet $\mathcal{A} = \{A, B, \dots, Z\}$ eine andere Zahl k von Schritten zwischen 1 und 25 wählen, um die „Verschiebung“ der Buchstaben festzulegen (bei $k = 0$ würde der Text nicht verschlüsselt). Man spricht von einer Verschiebechiffre und weiß, dass man beim *Durchprobieren aller möglichen Werte* für die Verschiebung aus dem verschlüsselten Text nach maximal 26 Versuchen wieder die Nachricht in Originalform erhalten wird. Einen sicheren Schutz der Nachricht können Verfahren dieser Art also nicht bieten.

Polybios-Chiffre

Einen Sonderfall der monographischen monoalphabetischen Substitutionen bildet die Polybios-Chiffre mit der folgenden Verschlüsselungstabelle, dem Polybios-Quadrat:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I, J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Es werden wiederum Einzelbuchstaben ersetzt, allerdings wird jedem Buchstaben ein Zeichenpaar zugeordnet. Dabei ist zu beachten, dass den Einzelbuchstaben I und J das gleiche Zeichenpaar (2, 4) – kurz: 24 – zugeordnet ist, so dass die Entschlüsselung zwar nicht eindeutig möglich ist, aber die Nachricht sich durch die sprachliche Redundanz dennoch leicht erschließen lässt. Entsprechend der Verschlüsselungstabelle wird das Wort POLYBIOS entsprechend der Stellung der Einzelbuchstaben in die Zeichenfolge 35 34 31 54 12 24 34 43 übertragen.

Die Idee der Polybios-Chiffre fand selbst bei im 20. Jahrhundert verwendeten Verschlüsselungsverfahren noch Anwendung. Ein Beispiel dafür ist die ADGFX-Chiffre. Die Verwendung dieser Chiffre durch das deutsche Militär im Ersten Weltkrieg und die Geschichte ihrer Entschlüsselung wird von Simon Singh in seinem Buch „Geheime Botschaften“ [84], aus dem man viele weitere Details zur Geschichte der Verschlüsselungen bis hin zur Gegenwart erfahren kann.

2.2 Häufigkeitsverteilung der Buchstaben

Als Meilenstein der Kryptographie des 19. Jahrhunderts gilt die Schrift *La Cryptographie militaire*, die 1883 von Auguste KERCKHOFFS von Nieuwenhof (1835–1903) verfasst wurde. In dieser Schrift formulierte er das folgende Prinzip, an dem sich auch alle heute üblichen Verschlüsselungsverfahren orientieren:

Prinzip von Kerckhoffs
Die Sicherheit eines Kryptosystems liegt allein in der Schwierigkeit, den Schlüssel zu finden – sie darf nicht auf der Geheimhaltung des Systems beruhen.

Um die Sicherheit der Verschlüsselung zu erhöhen, kann man also die Anzahl der Möglichkeiten für das Aufstellen von Verschlüsselungstabellen gegenüber der einfachen Verschiebechiffre vergrößern und zum Beispiel Tabellen wie die folgende aufstellen, die die Zuordnung der Buchstaben aus der Nachricht und zu dem Buchstaben aus der verschlüsselten Nachricht beschreibt und nicht nur eine Verschiebung der Buchstaben zulässt:

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

In der zweiten Zeile können auch (26 verschiedene) Zeichen stehen, die nicht mit den Buchstaben aus dem Originaltext übereinstimmen; die Sicherheit der Verschlüsselung verbessert das aber nicht. Auch hierbei ist die Regel zur Ersetzung von Buchstaben unabhängig von der Position im Text und es handelt sich um eine MM-Substitution. Insgesamt

gibt es 26! Möglichkeiten für Verschlüsselungstabellen bei 26 in der Nachricht verwendbaren Buchstaben, so dass ein Durchprobieren aller Möglichkeiten nicht mehr so einfach zum Ziel führt wie bei einer Verschiebechiffre. Doch trotz der erhöhten Anzahl von Möglichkeiten sind MM-Substitutionen verhältnismäßig leicht zu brechen. Ein Beispiel dafür schildert Edgar Allan Poe in seiner Erzählung „Der Goldkäfer“.

Beispiel 2.1 In der Erzählung „Der Goldkäfer“ von Edgar Allan Poe wird die Entschlüsselung des Textes

53‡‡‡305))6*;4826)4‡.)4‡);806*;48†8¶
60))85;1‡(:‡*8†83(88)5*†;46(;88*96*
‡;8)*‡(;485);5*†2:*‡(;4956*2(5*-4)8¶
8*;4069285);6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4(
‡‡?34;48)4‡;161;:188;‡‡;

Kidd

benötigt. Die folgende Tabelle gibt die Buchstabenhäufigkeiten an:

8	;	4	‡	)	*	5	6	(	†	1	0	9	2	:	3	?	¶	-	.
33	26	19	16	16	13	12	11	10	8	8	6	5	5	4	4	3	2	1	1

Man kann daraus leicht schließen, dass 8 dem Buchstaben E entspricht und dass die Zeichenfolge „; 48“, die mehrmals in dem Text vorkommt, aus dem Wort THE entstanden sein muss. Die weitere Entschlüsselung des Textes bereitet mehr Mühe, ist aber mit einer gewissen Fleißarbeit möglich, indem man bereits entschlüsselte Buchstaben ersetzt und nach Zeichenfolgen sucht, deren Bedeutung man trotz fehlender Zwischenbuchstaben erkennt.

Später werden wir sehen, dass erfahrenen Kryptoanalytikern schon etwa 25 aufeinanderfolgende Zeichen des verschlüsselten Textes genügen, um die Nachricht in Originalform zu finden – vorausgesetzt, dass es sich dabei um einen in einer natürlichen Sprache verfassten Text handelt.

Da der Aufwand für das Durchprobieren aller Möglichkeiten bei der Suche nach der benutzten Verschlüsselungstabelle zu groß ist, ist es für Nachrichtentexte aus einer natürlichen Sprache hilfreich, die typische Häufigkeitsverteilung der Buchstaben zu kennen.

► **Anmerkung** Ein weiteres Hilfsmittel, auf das wir später eingehen werden, ist das Ausnutzen der Redundanz von natürlichen Sprachen, die in Abschn. 4.4.1 eingeführt wird – man muss nicht alle Buchstaben eines Textes kennen, um den Sinn zu verstehen.

Im Falle von deutschsprachigen Texte hinreichender Länge kann man zum Beispiel auf die folgende Tabelle zurückgreifen (sie ist durch Auszählung auf Texten der Alltagssprache mit einer Länge von 4 Millionen Zeichen entstanden [9]).

Tab. 2.1 Häufigkeiten der Buchstaben in deutschsprachigen Texten

Buchstabe	Häufigkeit in %	Buchstabe	Häufigkeit in %
A	6,51	N	9,78
B	1,89	O	2,51
C	3,06	P	0,79
D	5,08	Q	0,02
E	17,40	R	7,00
F	1,66	S	7,27
G	3,01	T	6,15
H	4,76	U	4,35
I	7,55	V	0,67
J	0,27	W	1,89
K	1,21	X	0,03
L	3,44	Y	0,04
M	2,53	Z	1,13

Die häufigsten Buchstaben in deutschsprachigen Texten sind demnach E, N, I, S, R, A, T – ihr Anteil macht insgesamt mehr als 60 % des Textes aus. Die Häufigkeit des Buchstaben E ist deshalb verzerrt, weil die Umlaute als Zeichenfolgen AE, OE, UE aufgefasst worden sind.

Bei der Benutzung der Tabelle muss man aber bedenken, dass Abweichungen von dieser durchschnittlichen Verteilung auftreten können, insbesondere bei kurzen Texten. Verfeinerte Methoden berücksichtigen auch Häufigkeiten von Buchstabenfolgen. Insbesondere sind ER, EN, CH, DE, EI, ND, TE, IN, IE, GE die häufigsten Buchstabenpaare (Bigramme) und EIN, ICH, NDE, DIE, UND, DER, CHE, END, GEN, SCH die häufigsten Buchstabenfolgen der Länge drei (Trigramme) in deutschsprachigen Texten.

► **Anmerkung** Exotische Beispiele, in denen die Häufigkeitsverteilung der Buchstaben von den gewohnten Tab. 2.1 abweicht, sind sogenannte Lipogramme. Das sind Texte, in denen auf die Verwendung eines oder mehrerer Buchstaben des Alphabets verzichtet wird. Selbst ganze Romane sind ohne Verwendung des Buchstaben E geschrieben worden, zum Beispiel der 1969 erschienene Roman „La disparation“ des französischen Schriftstellers G. Perec (deutsche Übersetzung von E. Helmlé „Anton Foys Fortgang“ (1986), englische Übersetzung von G. Adair „A Void“).

Für die Kryptoanalyse von MM-Substitutionen liefert folgende Beobachtung einen wichtigen Ansatz:

Satz 2.1 *Bei allen MM-Substitutionen bleibt die Häufigkeitsverteilung der Einzelzeichen innerhalb des Textes erhalten.*

Wir haben am Beispiel der Goldkäfer-Chiffre schon gesehen, wie man diese Tatsache ausnutzen kann. Zunächst versucht man die Zeichen herauszufinden, die den häufigsten Buchstaben des Alphabets entsprechen, und ersetzt diese im Text. Anschließend versucht man die noch bestehenden Lücken in der Entschlüsselung des Textes zu schließen, indem man die Bedeutung von teilentschlüsselten Zeichenfolgen „errät“ wozu natürlich gute Kenntnisse der Sprache des verschlüsselten Textes erforderlich sind.

Es gibt ein einfaches Verfahren, für einen monoalphabetisch-monographisch chiffrierten Text festzustellen, in welcher Sprache die Nachrichten abgefasst ist, ohne sich mit Syntax und Semantik der Sprache zu beschäftigen. Dazu betrachtet man den von FRIEDMAN¹ eingeführten *Koinzidenzindex* (index of coincidence, IC) eines Textes:

Definition 2.3 Sei $x = x_1 x_2 \dots x_n$ eine Zeichenfolge über einem Alphabet. Der Koinzidenzindex $IC(x)$ von x ist die Wahrscheinlichkeit dafür, dass zwei zufällig ausgewählte Elemente x_s, x_t ($s \neq t$) von x gleich sind.

Die Häufigkeiten der Buchstaben $a_0 := A, a_1 := B, \dots, a_{25} := Z$ bezeichnen wir in dieser Reihenfolge mit $n_0, n_1, \dots, n_{25}$.

Es gibt $\binom{n}{2} = \frac{n(n-1)}{2}$ Möglichkeiten, zwei Elemente x_s, x_t ($s \neq t$) von x zufällig auszuwählen. Für jedes $i \in \{0, 1, \dots, 25\}$ gibt es $\binom{n_i}{2} = \frac{n_i(n_i-1)}{2}$ Möglichkeiten, in beiden Fällen den Buchstaben a_i zu wählen. Daher gilt:

$$IC(x) = \frac{\sum_{i=0}^{25} n_i(n_i - 1)}{n(n - 1)}.$$

Einen Näherungswert für $IC(x)$ erhält man bei ausreichend großer Länge der Zeichenfolge x , indem man die Wahrscheinlichkeiten p_i benutzt, mit der die Buchstaben a_i in der Sprache des Textes x vorkommen:

$$IC(x) \approx \sum_{i=0}^{25} p_i^2.$$

Die Wahrscheinlichkeit dafür, dass zwei zufällig ausgewählte Buchstaben beide gleich A sind, beträgt nämlich p_0^2 , dafür dass beide gleich B sind, ist sie p_1^2 , usw.

Beispiel 2.2 Man kann den Koinzidenzindex für Texte in englischer und deutscher Sprache auf Grundlage von Häufigkeitstabellen wie der vorn angegebenen berechnen:

Text in englischer Sprache: $IC(x) \approx 0,066$

Text in deutscher Sprache: $IC(x) \approx 0,076$.

¹William Frederick Friedman (1891–1969) war ein amerikanischer Kryptologe.

In der Literatur schwanken die Angaben für den Koinzidenzindex aufgrund unterschiedlicher Auszählungsgrundlagen zwischen 0,65 und 0,69 für Englisch und zwischen 0,75 und 0,83 für Deutsch.

Bei einem „zufälligen Text“ (d. h. alle Buchstaben kommen mit gleicher Wahrscheinlichkeit vor) über einem Alphabet mit 26 Buchstaben nimmt $IC(x)$ sein absolutes Minimum an.

$$\text{zufälliger Text} \quad IC(x) = \sum_{i=0}^{25} \left(\frac{1}{26} \right)^2 = 0,039.$$

Satz 2.2 *Der Koinzidenzindex bleibt bei MM-Substitutionen erhalten.*

Deshalb erhält man nach Auszählung der Häufigkeiten der Zeichen im verschlüsselten Text einen Näherungswert für den Koinzidenzindex der Sprache der Nachricht und kann damit – ohne den Sinn des Textes zu verstehen – auf die verwendete Sprache schließen (zumindest dann, wenn der verschlüsselte Text annähernd der typischen Häufigkeitsverteilung der Sprache entspricht).

Die monoalphabetischen Substitutionen haben sich also bereits als zu unsicher erwiesen. Um die Sicherheit der Verschlüsselung zu erhöhen, kann man zu *polyalphabetischen Substitutionen* übergehen, bei deren Anwendung sich die Häufigkeit der Einzelzeichen beim Übergang von der Nachricht zum verschlüsselten Text ändert.

2.3 Die Vigenère-Chiffre und deren Analyse

Die bekannteste polyalphabetische Chiffrierung ist die Vigenère-Chiffre.²

Sie ist eine *polyalphabetische monographische Substitution*.

Definition 2.4 *Man spricht von einer polyalphabetischen monographischen Substitution (PM-Substitution), wenn bei der Verschlüsselung Einzelbuchstaben ersetzt werden und für unterschiedliche Stellen im Text unterschiedliche Verschlüsselungsregeln für denselben Klartextbuchstaben zulässig sind.*

Dabei können auch verschiedene Alphabete für Zeichen des verschlüsselten Textes verwendet werden – das erklärt die Bezeichnung *polyalphabetisch*, auch wenn nicht verlangt ist, dass die Alphabete sich tatsächlich unterscheiden müssen. Das Ergebnis der Verschlüsselung eines Zeichens ist also bei PM-Substitutionen nicht nur vom Zeichen selbst, sondern auch von dessen Position im Text abhängig bzw. davon, mit welchem Schlüsselbuchstaben verschlüsselt wurde. Zur Verschlüsselung wird das Vigenère-Quadrat verwendet

²Blaise de Vigenère (1523–1596) war ein französischer Diplomat und kam mit den Kryptologen des Papstes in Kontakt, als er 1549 Aufgaben in Rom zu erfüllen hatte.

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

Beispiel:
Die Verschlüsselung des Klartextbuchstabens „N“ mit dem Schlüsselbuchstaben „M“ ergibt den Schlüsseltextbuchstaben „Z“.

Abb. 2.1 Vigenère-Quadrat

Nachricht	:	N	A	C	H	R	I	C	H	T	N	A	C	H	A	C	H	T	U	H	R
Schlüssel	:	M	O	N	D	M	O	N	D	M	O	N	D	M	O	N	D	M	O	N	D
Schlüsseltext	:	Z	O	P	K	D	W	P	K	F	B	N	F	T	O	P	K	F	I	U	U
																					Periodische Wiederholung des Schlüsselwortes→

Abb. 2.2 Beispiel für eine Verschlüsselung mit der Vigenère-Chiffre

(Abb. 2.1). In der ersten Zeile sind die Klartextbuchstaben angeordnet, in der ersten Spalte die Schlüsselbuchstaben. Die Zellen des Quadrates liefern die Schlüsseltextbuchstaben.

Beispiel 2.3 Sender und Empfänger der geheimen Nachricht müssen sich zunächst auf ein Schlüsselwort einigen, in unserem Beispiel MOND. Wir verschlüsseln damit den Text NACHRICHTNACHACHTUHR wie folgt: Der Schnittpunkt der Zeile M (1. Buchstabe des Schlüsselwortes) mit der Spalte N (1. Buchstabe der Nachricht) im Vigenère-Quadrat liefert Z als 1. Buchstaben des verschlüsselten Textes. Entsprechend erhält man den 2. Buchstaben O als Schnittpunkt der Zeile O (2. Buchstabe des Schlüsselwortes) mit der Spalte A (2. Buchstabe der Nachricht) usw. Ab dem 5. Buchstaben wird das Schlüsselwort periodisch wiederholt, so dass der 5. Buchstabe der Nachricht wieder mit M verschlüsselt wird, der 6. mit O usw. Insgesamt ist ZOPKDWPKFBNFTOPKFIUU der verschlüsselte Text (Abb. 2.2). Kennt der Empfänger dieses Textes das Schlüsselwort MOND, kann er leicht die ursprüngliche Nachricht rekonstruieren, indem er wieder das Vigenère-Quadrat benutzt.

PM-Substitutionen wurden lange als sichere Kryptosysteme angesehen, da sie statistische Eigenschaften wie Häufigkeitsverteilungen von Einzelbuchstaben, Buchstabenfolgen der Länge 2 usw. stark verändern. Wir werden am Beispiel der Vigenère-Chiffre zeigen, wie man solche Chiffrierungen brechen kann. Einen möglichen Angriffspunkt bildet die periodische Wiederholung des Schlüsselwortes. Wenn ein kurzes Schlüsselwort verwendet wird, hat ein Angreifer bei einem hinreichend langen verschlüsselten Text Möglichkeiten, das Schlüsselwort zu finden und damit den Inhalt der Nachricht zu erfahren.

Den ersten Schritt in den Überlegungen bildet die Bestimmung der Länge des Schlüsselwortes. Eine Möglichkeit dazu bietet der **Kasiski-Test**, benannt nach seinem Erfinder Friedrich Wilhelm Kasiski, der ihn 1863 publizierte.

Kasiski-Test

- Finde übereinstimmende Abschnitte möglichst großer Länge im Schlüsseltext und ermittle die Differenz zwischen den Anfangspositionen dieser Abschnitte. So erhält man Differenzen $d_1, d_2, \dots$
- Berechne den größten gemeinsamen Teiler $t := \text{ggT}(d_1, d_2, \dots)$ dieser Differenzen.
- Die vermutete Länge ℓ des Schlüsselwortes ist $\ell = t$.

► **Anmerkung** Es kann auch sein, dass die wie oben beschrieben ermittelte Zahl t nicht die tatsächliche Länge des Schlüsselwortes ist – man stellt das spätestens dann fest, wenn der Versuch der Entschlüsselung mit der beschriebenen Methode nicht zum Erfolg führt. Dann muss man noch einmal von vorn beginnen, den größten gemeinsamen Teiler nur für eine Teilmenge der Differenzen $d_1, d_2, \dots$ bestimmen und auf eine erfolgreiche Entschlüsselung hoffen. Bei der Auswahl der Differenzen d_i , zu denen der größte gemeinsame Teiler berechnet wird, sind solche Zahlen d_i stärker zu berücksichtigen, die sich durch übereinstimmende Zeichenfolgen großer Länge im Schlüsseltext ergeben haben – sie werden nur selten durch Zufall entstanden sein und deshalb auf identische Abschnitte im Klartext hindeuten, die mit identischen Abschnitten im Schlüsselwort verschlüsselt worden sind.

Da das Schlüsselwort periodisch verwendet wird, werden identische Abschnitte der Nachricht zu identischen Abschnitten des Schlüsseltextes verschlüsselt, wenn sich ihre Positionen in der Nachricht um ein Vielfaches der Länge des Schlüsselwortes unterscheiden. Natürlich können solche Wiederholungen im Schlüsseltext auch zufällig auftreten, doch die Wahrscheinlichkeit dafür sinkt mit zunehmender Länge der untersuchten Folge. Aus diesem Grund sollten die analysierten Folgen mindestens drei Zeichen lang sein. Da der Abstand zwischen identischen Schlüsseltextabschnitten, die nicht nur rein zufällig entstanden sind, ein Vielfaches der Schlüssellänge beträgt, kann diese mit Hilfe des größten gemeinsamen Teilers der Abstände abgeschätzt werden. Abbildung 2.3 illustriert das Vorgehen an einem kleinen Beispiel.

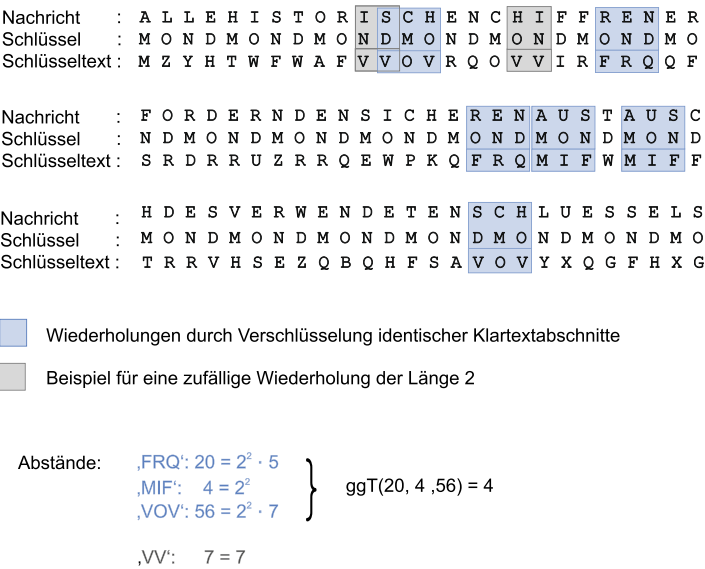
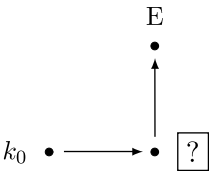


Abb. 2.3 Abschätzen der Schlüssellänge mit dem Kasiski-Test

Wir gehen jetzt von der Annahme aus, die Schlüsselwortlänge sei schon bekannt. Vermutet man zum Beispiel (wie in unserem Fall aus Abb. 2.2, wo identische Abschnitte im verschlüsselten Text mit den Abständen 12, 4 und 8 vorkommen), dass das Schlüsselwort die Länge 4 hat, d. h. $k = k_0k_1k_2k_3$, dann wurden der 1., 5., 9. und jeder vierte weitere Buchstabe aus der Nachricht mit dem Schlüsselwortbuchstaben k_0 verschlüsselt, der 2., 6., 10. und jeder vierte weitere Buchstabe mit dem Schlüsselwortbuchstaben k_1 usw. Den verschlüsselten Text $c_0c_1c_2 \dots$ trägt man am besten zeilenweise in eine Tabelle ein, in deren Eingangszeile das (unbekannte) Schlüsselwort $k_0k_1k_2k_3$ steht, so dass die Spalten der Tabelle das Ergebnis der Verschlüsselung mit jeweils einem festen Schlüsselwortbuchstaben enthalten (Abb. 2.5).

Jede Spalte der resultierenden Tabelle ist durch eine Verschiebechiffre (also eine spezielle MM-Substitution) aus deutschsprachigem Text entstanden. Die Häufigkeitsverteilung der Buchstaben in der Nachricht überträgt sich also bei der Vigenère-Verschlüsselung auf die Spalten dieser Tabelle. Wenn die Häufigkeitsverteilung der Buchstaben im Text der Nachricht bekannt ist, dann weiß man bei deutschsprachigen Texten zum Beispiel, dass der in Abb. 2.4 mit dem Symbol $\boxed{?}$ bezeichnete häufigste Buchstabe in der Menge der 1., 5., 9., 13., ... Buchstaben des verschlüsselten Textes (aus der ersten Spalte der Ta-

Abb. 2.4 Diagramm zur Vigenère-Chiffre



Schlüssel	k_0	k_1	k_2	...	k_{r-1}
Schlüsseltext	c_0	c_1	c_2	...	c_{r-1}
	c_r	c_{r+1}	c_{r+2}	...	$c_{r+(r-1)}$
	c_{2r}	c_{2r+1}	c_{2r+2}	...	$c_{2r+(r-1)}$
	c_{3r}	c_{3r+1}	c_{3r+2}	...	$c_{3r+(r-1)}$
	...	...	...	...	...

$IC_{min} = 0,0385$

$IC_{max} = 0,0762$

Abb. 2.5 Einordnen des Schlüsseltextes und Beziehungen zum Koinzidenzindex

belle) wahrscheinlich dem Buchstaben E im Nachrichtentext entspricht. Daraus erkennt man aber mit Hilfe des Vigenère-Quadrats leicht den Schlüsselwortbuchstaben k_0 :

Nach der gleichen Methode kann man die Schlüsselwortbuchstaben k_1, k_2, k_3 finden. Hat ein Angreifer auf diese Weise das Schlüsselwort gefunden, ist ihm die Rekonstruktion der Nachricht aus dem verschlüsselten Text ebenso möglich wie dem, für den die Nachricht eigentlich bestimmt ist.

Zur Ermittlung der Länge des Schlüsselwortes ist es neben dem Kasiski-Test auch hilfreich, den **Koinzidenzindex** zu betrachten und damit ein zuverlässigeres Ergebnis für die Länge des Schlüsseltextes zu erhalten. Wir werden sehen, dass er mit wachsender Länge r des Schlüsselwortes kleiner wird. Aus der Zahl, die wir berechnen, wird man nicht die exakte Länge des Schlüsselwortes ablesen können. Es wird aber ersichtlich sein, ob es sich um eine mono- oder polyalphabetische Chiffrierung handelt und ob ein langer oder kurzer Schlüssel verwendet worden ist. Dennoch lässt sich das Ausprobieren von Schlüsselwortlängen in der passenden Größenordnung nicht vermeiden – dass man die richtige Länge verwendet hat, erkennt man daran, dass sich beim Entschlüsseln ein sinnvoller Text ergibt.

Satz 2.3 Die Schlüsselwortlänge r ergibt sich wie folgt aus dem Koinzidenzindex $IC(x)$ und der Länge ℓ des verschlüsselten Textes:

$$r \approx \frac{0,037\ell}{(\ell - 1) \cdot IC(x) - 0,039\ell + 0,076}.$$

Diese Aussage wollen wir im Folgenden herleiten: Zunächst stellt man sich vor, der verschlüsselte Text $c_0c_1 \dots c_\ell$ sei wieder zeilenweise in eine Tabelle mit r Spalten eingetragen, in deren Eingangszeile das (unbekannte) Schlüsselwort $k_0k_1 \dots k_{r-1}$ steht. In jeder Spalte stehen $\approx \frac{\ell}{r}$ Buchstaben des verschlüsselten Textes, wobei der Rundungsfehler für hinreichend großes ℓ zu vernachlässigen ist (Abb. 2.5).

Das Ziel besteht nun darin, den Koinzidenzindex des verschlüsselten Textes der Länge ℓ in Abhängigkeit von r auszudrücken. Dazu werden wir zunächst den Erwartungswert EX für die Anzahl von Paaren aus gleichen Buchstaben (also für IC) ermitteln.

Um die Rechnung zu vereinfachen, setzen wir voraus, die Buchstaben des Schlüsselwortes seien zufällig und unabhängig gewählt. Um mit konkreten Zahlenwerten arbeiten zu können, gehen wir davon aus, dass eine deutschsprachige Nachricht chiffriert wurde (das Ergebnis lässt sich leicht für andere Sprachen anpassen).

Zunächst betrachten wir Paare von Buchstaben, die in derselben Spalte zufällig ausgewählt werden. Da jede Spalte z_i durch eine Verschiebechiffre aus deutschsprachigem Text entstanden ist, gilt $IC(z_i) \approx 0,076$ (die Wahrscheinlichkeit dafür, dass zwei in derselben Spalte ausgewählte Elemente übereinstimmen, beträgt also $\approx 0,076$).

Da der verschlüsselte Text die Länge ℓ hat, kann man $\frac{1}{2} \cdot \ell(\frac{\ell}{r} - 1)$ Paare von Buchstaben bilden, die beide in derselben Spalte stehen: Für die Wahl des ersten Buchstaben hat man ℓ Möglichkeiten. Der zweite Buchstabe muss in derselben Spalte stehen und vom ersten verschieden sein – dafür gibt es $\frac{\ell}{r} - 1$ Möglichkeiten. Damit hat man aber jedes Paar zweimal erhalten. Der Erwartungswert für die Anzahl von Paaren aus gleichen Buchstaben, die innerhalb der Tabelle in derselben Spalte stehen, ist also $\frac{1}{2} \cdot 0,076\ell(\frac{\ell}{r} - 1)$.

Nun werden die Buchstaben eines Paares in verschiedenen Spalten ausgewählt. Unter dieser Bedingung beträgt die Wahrscheinlichkeit für die Gleichheit der Buchstaben eines Paares nur noch $\frac{1}{26} \approx 0,039$.

► **Anmerkung** Das gilt streng genommen nur unter der Voraussetzung, dass das Schlüsselwort eine zufällige Buchstabenfolge ist. Wir können aber auch mit dieser Zahl als Näherungswert arbeiten, wenn wir von einem kurzen Schlüsselwort ausgehen.

Da der verschlüsselte Text die Länge ℓ hat, kann man $\frac{1}{2} \cdot \ell(\ell - \frac{\ell}{r})$ Paare von Buchstaben bilden, die nicht in derselben Spalte stehen: Für die Wahl des ersten Buchstaben hat man ℓ Möglichkeiten. Der zweite Buchstabe darf nicht in derselben Spalte stehen – dafür gibt es $\ell - \frac{\ell}{r}$ Möglichkeiten. Damit hat man aber jedes Paar zweimal erhalten. Der Erwartungswert für die Anzahl von Paaren aus gleichen Buchstaben, die innerhalb der Tabelle in verschiedenen Spalten stehen, ist also $\frac{1}{2} \cdot 0,039\ell(\ell - \frac{\ell}{r}) = \frac{1}{2} \cdot 0,039\ell^2(1 - \frac{1}{r})$.

Damit erhalten wir als Erwartungswert für die Anzahl von Paaren aus gleichen Buchstaben:

$$EX = \frac{1}{2} \cdot 0,076\ell\left(\frac{\ell}{r} - 1\right) + \frac{1}{2} \cdot 0,039\ell^2\left(1 - \frac{1}{r}\right).$$

Da man in einem Schlüsseltext der Länge ℓ insgesamt $\binom{\ell}{2} = \frac{\ell(\ell-1)}{2}$ Paare aus zwei Buchstaben auswählen kann, ergibt sich als Koinzidenzindex $IC(x)$ des verschlüsselten Textes x :

$$IC(x) \approx \frac{EX}{\binom{\ell}{2}}$$

Tab. 2.2 Koinzidenzindex

	deutscher Text	englischer Text
Koinzidenzindex für $r = 1$	$IC(x) \approx 0,076$	$IC(x) \approx 0,066$
Koinzidenzindex für $r = \ell$	$IC(x) \approx 0,039$ für großes ℓ	$IC(x) \approx 0,039$ für großes ℓ

$$\begin{aligned}
&\approx \frac{\frac{1}{2} \cdot 0,076\ell\left(\frac{\ell}{r} - 1\right) + \frac{1}{2} \cdot 0,039\ell^2\left(1 - \frac{1}{r}\right)}{\frac{\ell(\ell-1)}{2}} \\
&\approx \frac{1}{r(\ell-1)} (0,076(\ell-r) + 0,039\ell(r-1)) \\
&\approx \frac{1}{r(\ell-1)} (0,037\ell + r(0,039\ell - 0,076)) \\
&\approx \frac{0,037\ell}{r(\ell-1)} + \frac{0,039\ell - 0,076}{\ell-1}.
\end{aligned}$$

Löst man nach r auf, ergibt sich:

$$r \approx \frac{0,037\ell}{(\ell-1) \cdot IC(x) - 0,039\ell + 0,076}.$$

Ersetzt man in der Herleitung $IC(z_i) \approx 0,076$ durch $IC(z_i) \approx 0,066$, dann erhält man die entsprechenden Formeln für einen englischsprachigen Text.

Nun werden wir diese Ergebnisse interpretieren. Für $r = 1$ bzw. $r = \ell$ erhält man durch Einsetzen in die Formel die Werte aus Tab. 2.2.

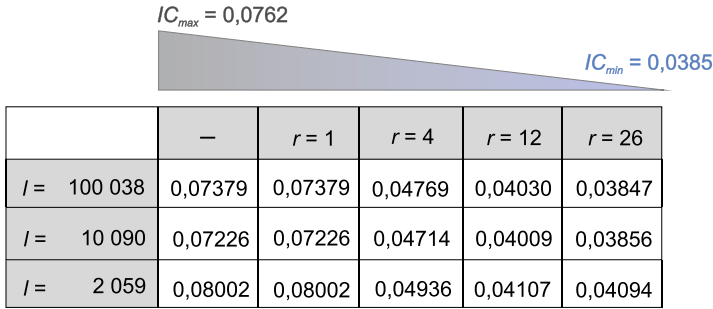
Da in den Tabellen jeweils der Koinzidenzindex für den verschlüsselten Text angegeben ist und der Koinzidenzindex für Texte in deutscher Sprache 0,076 und in englischer Sprache 0,066 beträgt, stellt man fest:

- Bei Chiffrierungen mit der Schlüsselwortlänge $r > 1$ verringert sich der Koinzidenzindex.
- Der Koinzidenzindex sinkt mit wachsender Länge r des Schlüsselwortes und nähert sich dem Wert eines zufälligen Textes (in dem eine Gleichverteilung der Buchstaben vorliegt).

Bei Chiffrierungen mit der Schlüsselwortlänge $r = 1$ handelt es sich um MM-Substitutionen – dass in diesem Fall der Koinzidenzindex unverändert bleibt, wurde schon im Anschluss an die Definition des Koinzidenzindex gezeigt.

Abbildung 2.6 zeigt einige Beispiele für den Koinzidenzindex auf Basis von Texten unterschiedlicher Länge. Für kürzere Texte sind dabei stärkere Schwankungen der Ergebnisse zu erwarten.

Die Länge des Schlüsselwortes ist ein wesentliches Kriterium für die Sicherheit. Man kann die Sicherheit der Vigenère-Verschlüsselung erhöhen, indem man längere Schlüsselwörter verwendet, die keinerlei statistische Gesetzmäßigkeiten erkennen lassen.



I ... Länge der ausgewerteten Texte (Texte in deutscher Sprache, Auswertung für die Buchstaben „A“ .. „Z“)

r ... Länge des verwendeten Schlüssels

Abb. 2.6 Koinzidenzindex für Beispieltexte

Ein weiteres Kriterium ist die Wahl der einzelnen Schlüsselwortbuchstaben. Die Schlüsselwörter dürfen insbesondere keine Wörter oder Texte einer natürlichen Sprache sein, sondern müssen als Zufallsfolgen von Buchstaben gewählt werden. Andernfalls führt ein Angriff von FRIEDMAN zur Entschlüsselung der Nachricht oder zumindest von Teilschnitten daraus. Um diesen Angriff zu verhindern, ist es auch wichtig, einen Schlüssel nicht mehrfach zu benutzen, wie wir gleich zeigen werden.

Diese Prinzipien werden bei der Vernam-Chiffre (*one-time pad*) realisiert, die in Abschn. 7.2.1 als Beispiel einer informationstheoretisch sicheren Verschlüsselung besprochen wird. Die Länge des Schlüsselwortes ist dabei gleich der Länge der Nachricht. Es erfüllt die Bedingung, dass aus dem verschlüsselten Text keinerlei Rückschlüsse auf die Nachricht gezogen werden können, auch wenn alle denkbaren wissenschaftlichen Erkenntnisse und unbeschränkte Rechenkapazitäten zur Analyse zur Verfügung stehen. Eine wesentliche Forderung für die Anwendung der Vernam-Chiffre ist es, jeden Schlüssel nur einmal zu verwenden. Wenn man den Aufwand zum Erzeugen und Austauschen der Schlüssel bedenkt, ist das zwar eine lästige Forderung. Die mehrmalige Verwendung von Schlüsseln bietet aber im Weiteren erläuterte Ansatzpunkte für die Kryptoanalyse.

Wird ein Schlüssel $k = k_0k_1 \dots k_{r-1}$ ein zweites Mal verwendet und sind beide Nachrichten in einer natürlichen Sprache abgefasst, kann man auf folgende Weise versuchen, den Inhalt der Nachrichten herauszufinden. Die Idee geht auf FRIEDMAN zurück, der auf diese Weise beschrieben hat, wie man bei der Vigenère-Chiffre zur Kryptoanalyse vorgehen kann, falls lange Schlüsselwörter verwendet wurden, die aus einer natürlichen Sprache stammen.

Im ersten Fall sei mit k die Nachricht $m = m_0m_1 \dots m_{r-1}$ zu $c = c_0c_1 \dots c_{r-1}$ verschlüsselt worden und im zweiten Fall $m' = m'_0m'_1 \dots m'_{r-1}$ mit k zu $c' = c'_0c'_1 \dots c'_{r-1}$ (siehe (1) in Abb. 2.7).

Abb. 2.8 Verdrahtung der Rotoren

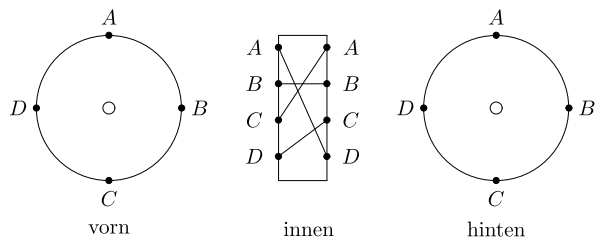


Abb. 2.9 Aufbau einer Rotormaschine

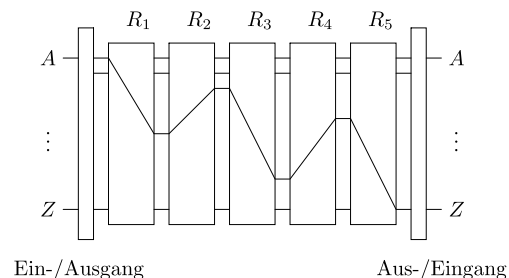
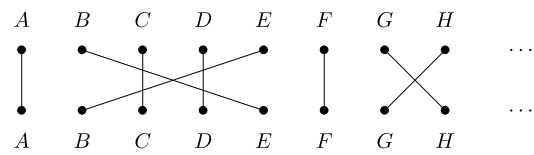


Abb. 2.10 Steckerbrett



Rückseite, die im Inneren des Rotors fest verdrahtet sind, und feststehendem Ein- und Ausgang. Die Rotoren verändern nach jeder Verschlüsselungsoperation automatisch ihre Stellung (Abb. 2.8 and 2.9).

Zum Chiffrieren bzw. Dechiffrieren durchlaufen die Texte die Rotormaschine in umgekehrter Reihenfolge. Parameter einer Rotormaschine sind Art, Anzahl, Reihenfolge und Ausgangsstellungen der Rotoren sowie der Rotormechanismus zum Fortschalten der einzelnen Rotoren.

Rotormaschinen wurden 1920 von mehreren Erfindern zum Patent angemeldet. Die ersten Modelle der Enigma waren Rotormaschinen mit 4 Rotoren. 1926 änderte man das Prinzip und es wurden nur noch drei Rotoren und eine „Umkehrwalze“ benutzt – mittels Steckverbindungen sind dabei die 26 Kontakte paarweise verbunden (man nennt diese „Umkehrwalze“ auch ein Steckerbrett, s. Abb. 2.10). Der Vorteil davon ist, dass man mit dem gleichen Verfahren Nachrichten verschlüsseln und verschlüsselte Texte entschlüsseln kann. Durch diese Besonderheiten in der Konstruktion der Enigma wissen Angreifer aber auch, dass kein Buchstabe in sich selbst übergehen kann (sonst gibt es einen Kurzschluss).

In der deutschen Wehrmacht wurde die Enigma I mit drei Rotoren verwendet, die aus einem Satz von 5 Rotoren ausgewählt werden konnten. Die Marine benutzte ab 1942 Modelle mit vier Rotoren. Ausgewählt werden konnten sie aus einem Satz von 5 Rotoren (1934), 7 Rotoren (1938) bzw. 8 Rotoren (1939).

Innerhalb der deutschen Wehrmacht wurde die Enigma als völlig sicher angesehen. Es kamen 40.000 bis 200.000 Maschinen zum Einsatz. Selbst die für damalige Verhältnisse gewaltige Anzahl von ca. $8 \cdot 10^8$ Schlüsseln konnte aber auf Dauer keine Sicherheit gewährleisten.

► **Anmerkung** Die Anzahl der möglichen Schlüssel bei der Heeres-Enigma, die drei Rotoren verwendet, ergibt sich wie folgt:

$$26^3 \cdot \binom{5}{3} \cdot 3! \cdot \frac{26!}{13! \cdot 2^{13}} \approx 8 \cdot 10^8$$

26^3 ... Anzahl der Rotorstellungen

$\binom{5}{3}$... Anzahl der Möglichkeiten für die Auswahl der Rotoren

$3!$... Anzahl der Möglichkeiten für die Reihenfolge der Rotoren

$\frac{26!}{13! \cdot 2^{13}}$... Anzahl der Möglichkeiten für das Bilden von Paaren auf dem Steckerbrett

Systematische Versuche, die Enigma-Verschlüsselung zu brechen, wurden vor dem Krieg in Polen und während des Krieges von den Engländern unternommen. Gerade an der Geschichte der Enigma (siehe [53]) kann man gut verdeutlichen, dass die Kryptoanalyse nicht nur durch systematisches Vorgehen zum Ziel führt. Sie wird auch von Zufällen und Fehlern beeinflusst und kann über Umwege und Irrtümer zum Ergebnis führen.

Die Kryptoanalyse der Enigma konnte beginnen, nachdem der polnische Zoll 1927 eine Enigma abgefangen hatte (auch wenn die Verdrahtung der Rotoren später noch geändert worden ist). Es wurden zwei wichtige Ansätze deutlich:

- Die Enigma-Verschlüsselung ist involutorisch, d. h. die zweimalige Anwendung der Verschlüsselung liefert wieder das Original.
- Bei der Enigma-Verschlüsselung wird kein Zeichen in sich selbst überführt.

Damit hat man einen Ansatzpunkt für die *negative Mustersuche*. Vermutet werden konnte zum Beispiel, dass die Buchstabenfolge OBERKOMMANDOWEHRMACHT (21 Zeichen) in der Nachricht vorkommt, allerdings an unbekannter Position. Bei einer Gleichverteilung der der Zeichen der Nachricht kann man $\approx 56\%$ aller denkbaren Zuordnungen

$$\begin{array}{llllll} \text{Nachrichtentext:} & \dots & m_1 & m_2 & \dots & m_{21} & \dots \\ \text{verschlüsselter Text:} & \dots & c_1 & c_2 & \dots & c_{21} & \dots \end{array}$$

ausschließen, denn es gilt $P(m_1 \neq c_1 \cap \dots \cap m_{21} \neq c_{21}) = P(\overline{m_1 = c_1}) \cdot \dots \cdot P(\overline{m_{21} = c_{21}}) = (1 - \frac{1}{26})^{21} \approx 44\%$. Nachrichtenabschnitte, die 100 Zeichen lang sind, liefern unter dieser Bedingung bereits mit 98 %-iger Wahrscheinlichkeit verbotene Stellungen.³

³ $1 - (1 - \frac{1}{26})^{100} \approx 98\%$.

Da vor dem Krieg in Ostpreußen mit der Enigma geübt wurde, war reichlich Untersuchungsmaterial für die Kryptoanalyse vorhanden. Ein Spion lieferte die Schlüssel von Oktober und November 1932 an die Franzosen, die sie an die Polen weitergaben, wodurch eine nachträgliche Entschlüsselung und damit auch eine tiefere Einsicht in das Verfahren möglich wurde.

Ein Schwachstelle, die nicht der Funktionsweise der Enigma selbst anzulasten ist, bestand in der Schlüsselverwaltung.

Bei der Enigma gab ein *Tagesschlüssel* die Art und Anordnung der Rotoren an – bei einer Enigma mit drei Rotoren bestand ein Tagesschlüssel demnach aus drei Buchstaben. Tagesschlüssel wurden monatsweise in einem Codebuch herausgegeben. Zusätzlich musste der Funker bei jeder einzelnen Nachricht einen aus drei Buchstaben bestehenden *Spruchschlüssel* festlegen, der die Ausgangsstellung der Rotoren bestimmt. Dieser Spruchschlüssel wurde zweimal hintereinander an den Anfang der Nachricht geschrieben und mit der Nachricht zusammen chiffriert. Die Wiederholung des Spruchschlüssels sollte sicherstellen, dass auch bei Übertragungsfehlern keine Rückfrage nötig wird. Die Funker machten den Fehler, als Spruchschlüssel in der Regel solche Buchstabenfolgen wie AAA, BBB usw. oder auf der Tastatur benachbarte Tasten wie QWE oder QAY zu verwenden, was die Kryptoanalyse sehr erleichtert hat, da das Durchprobieren aller Möglichkeiten stark eingeschränkt werden konnte.

Bereits 1937 konnten die Tagesschlüssel innerhalb von 10 bis 20 Minuten ermittelt werden. Bei der Kryptoanalyse hat auch geholfen, dass in den Nachrichten stereotype Formulierungen wie KEINEBESONDERENVORKOMMNISSE verwendet worden sind. Manchmal wurde der Klartext sogar „untergeschoben“: Zum Beispiel setzten deutsche Beobachter in der Regel die Meldung GARTENPFLEGE ab, wenn die englische Luftwaffe Planquadrate vermint. Oft wurde in einem solchen Fall die Nachricht mit verschiedenen Verfahren verschlüsselt weitergegeben, von denen manche noch unsicherer als die Enigma selbst waren. Einmal wurde eine Leuchttonne nur deshalb bombardiert, damit ein deutscher Beobachter den chiffrierten Funkspruch ERLOSCHENISTLEUCHTTONNE absendet, was daraufhin auch geschehen sein soll.

Die Tagesschlüssel konnten in einzelnen Fällen auch durch militärische Eroberungen bereitgestellt werden wie im Februar 1941 von einem schlecht bewaffneten Trawler in Nordnorwegen. Erbeutet wurden auch Codebücher mit Wetterkurzschlüsseln (Wettermeldungen wurden nur mit der 3-Rotor-Enigma verschlüsselt) und vom deutschen U-Boot U110 zahlreiche Codetabellen und Tagesschlüssel für einen längeren Zeitraum.

Obwohl 1940 das Spruchschlüsselverfahren noch einmal geändert worden ist, konnte A. TURING innerhalb kurzer Zeit für das neue Verfahren eine Dechiffriermethode entwickeln. Im britischen Dechiffrierzentrum Bletchley Park arbeiteten 7.000 bis 30.000 Beschäftigte rund um die Uhr an der Dechiffrierung der abgehörten Nachrichten. Durch die Anwendung selbstentwickelter Maschinen konnte die Suche so beschleunigt werden, dass für das Durchspielen der Fälle jeweils nur noch höchstens 110 Minuten benötigt worden sind. Bei der Übermittlung des Inhalts besonders wichtiger dechiffrierter Nachrichten an den britischen Premierminister wurden sie mit der Vernam-Chiffre verschlüsselt. So er-

reichten die Alliierten, dass die Deutschen bis zum Kriegsende nicht wussten, dass die Enigma-Verschlüsselung gebrochen worden ist.

Erst 1974 wurde die Kompromittierung der Enigma öffentlich bekannt. Auf dem heutigen Stand der Rechentechnik wäre es einfacher gewesen, die Enigma-Verschlüsselung durch Durchprobieren aller Möglichkeiten zu brechen.

Alle bisher erwähnten Verschlüsselungsverfahren haben die Gemeinsamkeit, dass vor der eigentlichen gesicherten Kommunikation eine „Schlüsselübergabe“ zwischen den Kommunikationspartnern stattfinden muss. Dieser Nachteil entfällt bei den asymmetrischen Verfahren, die seit 1977 angewendet und im Kap. 8 vorgestellt werden. Mit der Einführung solcher Verfahren hat sich die Kryptologie, die ursprünglich als Teilgebiet der Kodierungstheorie zählte, als eigenständiges Gebiet etabliert.

2.5 Zusammenfassung

Wir haben Beispiele für Permutationschiffren und monoalphabetisch-monographische Substitutionen kennengelernt. Bei den Permutationschiffren wird der Text verschlüsselt, indem die Zeichen der Nachricht in geänderter Reihenfolge notiert werden. Bei den monoalphabetisch-monographischen Substitutionen (kurz: MM-Substitutionen) werden Einzelbuchstaben der Nachricht nach einer festen Regel unabhängig von ihrer Position im Text durch ein Zeichen ersetzt, das diesem Einzelbuchstaben durch eine Verschlüsselungstabelle eineindeutig zugewiesen ist. Solche Verschlüsselungen wurden schon vor sehr langer Zeit verwendet und weisen eine Gemeinsamkeit auf, die sie für sichere Chiffrierverfahren ungeeignet macht: Die Häufigkeitsverteilungen der Buchstaben stimmen in der Nachricht und im verschlüsselten Text überein – daraus ergeben sich wirkungsvolle Ansatzpunkte für die Entschlüsselung der Nachricht durch unberechtigte Personen.

Ein wichtiger Parameter für die statistische Analyse der verschlüsselten Texte ist der Koinzidenzindex – darunter versteht man die Wahrscheinlichkeit dafür, dass zwei zufällig ausgewählte Zeichen des Textes gleich sind. Bei der Anwendung von MM-Substitutionen ändert sich der Koinzidenzindex nicht.

Sicherer als MM-Substitutionen sind polyalphabetische monographische Substitutionen (PM-Substitutionen) – dabei werden ebenfalls Einzelbuchstaben ersetzt, für unterschiedliche Stellen im Text sind jedoch unterschiedliche Verschlüsselungsregeln für denselben Klartextbuchstaben zulässig. Die bekannteste polyalphabetische Chiffrierung ist die Vigenère-Chiffre. Den verschlüsselten Text kann man bei der Vigenère-Chiffre aus einem Schema – dem sogenannten Vigenère-Quadrat – ablesen, nachdem man ein Schlüsselwort festgelegt hat, das periodisch wiederholt verwendet wird. Dieses Schlüsselwort nutzt der berechtigte Empfänger der Nachricht auch, um mit Hilfe des Vigenère-Quadrats aus dem verschlüsselten Text die ursprüngliche Nachricht zu rekonstruieren.

Auch die Vigenère-Chiffre hat sich als unsichere Verschlüsselung erwiesen, obwohl die Häufigkeitsverteilungen der Buchstaben in der Nachricht und im verschlüsselten Text unterschiedlich sind. Verwendet man ein kurzes Schlüsselwort, dann kann man (für hin-

reichend lange Nachrichten) die Länge dieses Schlüsselwortes ermitteln. Dazu eignen sich der KASISKI-Test oder auch eine Formel, in die der Koinzidenzindex des verschlüsselten Textes eingeht. Für lange Schlüsselwörter, die Texten aus einer natürlichen Sprache entnommen sind, hat FRIEDMAN eine Methode entwickelt, um Teilabschnitte der Nachricht zu entschlüsseln.

Eines der bekanntesten Beispiele aus der Geschichte der Kryptologie ist die Enigma-Verschlüsselung, die wir als Beispiel für sogenannte Rotormaschinen betrachtet haben. An der Geschichte der Enigma kann man gut erkennen, dass bei der Kryptoanalyse nicht nur systematisches Vorgehen zum Ziel führt, sondern dass sie auch von einer Reihe von Zufällen und Fehlern beeinflusst wird und über Umwege und Irrtümer zum Ergebnis führen kann.

Ein wichtiges Grundprinzip für alle heutigen Verschlüsselungsverfahren ist das Prinzip von KERCKHOFFS, nach dem die Sicherheit eines Kryptosystems allein in der Schwierigkeit liegt, den Schlüssel zu finden – sie darf nicht auf der Geheimhaltung des Systems beruhen.

2.6 Übungen

2.1 Wir betrachten folgenden Sonderfall einer Permutationschiffre: Für zwei natürliche Zahlen $m, n > 0$ wird die Nachricht zeilenweise in eine $m \times n$ -Matrix eingetragen, und der verschlüsselte Text wird spaltenweise aus dieser Matrix abgelesen. Zum Beispiel erhält man auf diese Weise für $m = 3, n = 5$ zur Nachricht VIGENERECHIFFRE den verschlüsselten Text VEIIRFGEFECRNHE. Texte der Länge > 15 werden blockweise verschlüsselt.

Entschlüsseln Sie den mit dieser Chiffriermethode und unbekannten Parametern m, n erzeugten verschlüsselten Text:

DCSIAAEERCFEHFMRITHESELSCEUSEIELSIMTNEFHIAENCS
BSEEPLIIIEIRVNIOENLURCTIHOSENHRVSLECHEENSLGSU.

2.2 Entschlüsseln Sie folgenden Text, der durch Anwendung einer Verschiebechiffre entstanden ist:

SVZZEMFCLKFIZJTYVETYZZWWIVEJZEUUVRCXFIZKYDVEQ
LDMVIJTYCLVJJVCELEUQLDVEKJTYCLVJJVCEZUVEKZJTY

2.3 Die folgenden Texte sind durch Anwendung von MM-Substitutionen aus deutschsprachigen Nachrichten entstanden. Entschlüsseln Sie jeweils den Text.

(a) XBBTI XACXAY WPE POQZTI

(b) DEBJ KGA HDG GEBJMC ECH KFFMC NEA HMCC HEFBJ GEBJMC
ECH KFFMC XMFCA YDC (*Goethe*)

2.4 Durch Anwendung der Vigenère-Chiffre mit einem Schlüsselwort der Länge 2 ist der Text

JDK DJZK AAZX YGN UIK OOHK KGY MZNO GPL YKI
GHKMOFGIONICKI QMEKZJRJMZT BOGHZXO BZXIGH FPXPKXQ

entstanden. Welche Nachricht wurde verschlüsselt?

Kryptographische Systeme

Baumann, U.; Franz, E.; Pfitzmann, A.

2014, XI, 301 S. 77 Abb., 60 Abb. in Farbe., Softcover

ISBN: 978-3-642-45332-8