Albrecht Beutelspacher

Kryptologie

Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen

10. Auflage

SACHBUCH

Springer Spektrum

Kryptologie

Albrecht Beutelspacher

Kryptologie

Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen

10., aktualisierte Auflage

Springer Spektrum

Albrecht Beutelspacher
Mathematisches Institut
Justus-Liebig-Universität Gießen
Gießen, Deutschland

ISBN 978-3-658-05975-0 ISBN 978-3-658-05976-7 (eBook)
DOI 10.1007/978-3-658-05976-7

Springer Spektrum

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer Spektrum ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-spektrum.de

Ohne alle Geheimniskrämerei, aber nicht ohne hinterlistigen Schalk,
dargestellt zum Nutzen und Ergötzen des allgemeinen Publikums.

Vorwort

Aut prodesse volunt aut delectare poetae
aut simul et iucunda et idonea dicere vitae.
(Nützen oder erfreuen wollen die Dichter,
oder, was zugleich erfreulich und nützlich fürs Leben ist, sagen)
(Horaz).

Seit es mit Sprache begabte Lebewesen gibt, gibt es auch vertrauliche Mitteilungen. Das sind Mitteilungen, die nur für eine einzige Person oder nur für einen klar definierten Personenkreis bestimmt sind, und von denen Außenstehende keine Kenntnis erhalten sollen.

Wie kann eine Nachricht „sicher" übermittelt werden? Also so, dass nur der berechtigte Empfänger die Nachricht dechiffrieren kann? Fast noch wichtiger: Wie kann man erreichen, dass die Nachricht wirklich beim Empfänger ankommt, und zwar genauso, wie man sie losgeschickt hat?

Es gibt grundsätzlich verschiedene Möglichkeiten, diese Probleme zu lösen. Die erste Methode besteht darin, die Existenz der Nachricht zu verheimlichen. Man könnte die vertrauliche Nachricht zum Beispiel mit unsichtbarer Tinte schreiben. Oder man könnte in einem unverfänglichen Brief gewisse Buchstaben markieren, indem man zum Beispiel mit einer Stecknadel ein kleines Loch darunter macht; die markierten Buchstaben ergeben die eigentliche Nachricht. Man spricht von Methoden der Steganographie.

Man kann auch versuchen, das Problem organisatorisch zu lösen. Etwa, indem man die Mitteilung durch eine vertrauenswürdige Person überbringen lässt. Zu allen Zeiten haben heimlich Verliebte solche Methoden eingesetzt– und fast alle klassischen Tragödien zeugen vom letztlichen Scheitern dieser Bemühungen.

Eine ganz andersartige Methode besteht darin, vertrauliche Nachrichten zu verschlüsseln. In diesem Fall verheimlicht man nicht ihre Existenz. Im Gegenteil: Man übermittelt die Nachricht über einen unsicheren Kanal, aber so „chiffriert", dass niemand – außer dem wirklichen Empfänger – die Nachricht „dechiffrieren" kann. Dies ist eine ganz perfide Herausforderung des Geg-

ners; solche Herausforderungen wurden in der Regel auch angenommen – und nicht selten wurde der Spieß umgedreht.

Wir werden uns in diesem Buch hauptsächlich mit dieser letzten Methode, also der Verschlüsselung der Nachrichten zum Zwecke der Geheimhaltung beschäftigen.

Ein zweiter Schwerpunkt des Buches ist die Integrität und Authentifikation. Hier geht es nicht darum, eine Nachricht gegen unberechtigtes Lesen zu schützen, sondern vor unberechtigter Änderung. Dieses Problem hat in den letzten Jahren große praktische Bedeutung erworben.

Bis vor einem halben Jahrhundert waren die Militärs die einzigen, die sich professionell mit Kryptologie beschäftigt haben. Nur im militärischen Bereich gab es genügend Motivation – und ausreichende Mittel –, um die damaligen Chiffriermaschinen, diese ausgeklügelten mechanischen Wunderwerke, zu entwickeln, zu bezahlen und zu benützen. Besonders berühmt war die ENIGMA (griechisch für „Rätsel"), die im 2. Weltkrieg von der deutschen Wehrmacht benutzt wurde. Systematische Angriffe auf die ENIGMA wurden bereits vor dem Krieg in Polen und dann während des zweiten Weltkriegs im Britischen Dechiffrierzentrum in Bletchley Park unternommen. Den Briten gelang es dabei nicht nur, das ENIGMA-System zu knacken, sondern sie konnten diese Tatsache auch bis zum Ende des zweiten Weltkriegs vor den Deutschen geheim halten. Eine andere Maschine, der Geheimschreiber T-52 von Siemens & Halske, der zur Übermittlung streng geheimer Nachrichten eingesetzt wurde, blieb während dieser Zeit sicher.

Es gibt eine interessante Verbindung zwischen diesen Angriffen auf Chiffriermaschinen und den Anfängen der Computerentwicklung. Während des zweiten Weltkriegs entwickelten die Engländer elektromechanische und elektronische Maschinen, um die deutschen verschlüsselten Nachrichten zu knacken. Die berühmteste dieser Maschinen, die Röhrenrechenanlage COLOSSUS, kann als der erste digitale Computer angesehen werden. Es ist bemerkenswert, dass der englische Mathematiker Alan M. Turing (1912–1954), der später als der Vater der theoretischen Informatik berühmt wurde, zwar eine entscheidende Rolle im Dechiffrierteam von Bletchley Park gespielt hat, nicht aber an der Entwicklung des COLOSSUS beteiligt war.

Die Tatsache, dass die Kryptologie bei der Geburt der modernen Computer Pate stand, hat Symbolcharakter. Mit der überwältigenden Verbreitung der elektronischen Datenverarbeitung seit den 60-er Jahren des 20. Jahrhunderts ist die Kryptologie auf neue Füße gestellt worden. Dies hat verschiedene Gründe. Einige seien hier genannt:

Beim Versuch, ein gegnerisches System zu brechen, müssen Unmengen von Daten, zum Beispiel Buchstabenketten und Zahlenkolonnen verarbeitet werden: Man muss Daten vergleichen, Mittelwerte, Standardabweichungen und vieles andere mehr berechnen – alles Dinge, die ein Computer sehr viel schneller und besser kann als der Mensch. Die Konsequenz ist, dass Kryptosysteme, die heute mit Erfolg eingesetzt werden sollen, wesentlich komplexer sein müssen als ihre Vorgänger vor zwei oder drei Generationen.

Andererseits ermöglicht moderne Hard- und Software die Implementierung von komplexen und anspruchsvollen mathematischen Algorithmen. Mit diesen erreicht man einen Grad von Sicherheit, zu dem es in der Geschichte keine Parallele gibt: Ein kleiner Zuwachs in der Komplexität eines Algorithmus führt zu einem überdimensionalen Anwachsen der Ressourcen, die zum Brechen des Systems benötigt werden. Der Witz der modernen Kryptologie ist, dass der Computer nicht nur die Ursache vieler Probleme, sondern gleichzeitig der Schlüssel zur ihrer Lösung ist.

Durch das Vordringen elektronischer Datenverarbeitung und insbesondere von elektronischer Kommunikation in immer mehr Bereiche öffneten sich gänzlich neue Aufgabenfelder für die Kryptologie. Neben den „klassischen" Anwendungen im Militär- und Behördenwesen stellten sich ganz neuartige Herausforderungen an die Kryptologie. Große neuartige Anwendungen wie Mobilfunk, Internetkommunikation oder elektronischer Zahlungsverkehr sind ohne moderne Sicherheitsfunktionen unvorstellbar.

Die Gespräche, die Sie über Ihr Handy führen, können prinzipiell abgehört werden – jedenfalls zwischen dem Handy und der ersten Basisstation. Folglich müssen die Gespräche so chiffriert werden, dass ein Abhörer nur sinnlose Geräusche hören kann.

Wenn man den Internetverkehr verschlüsseln möchte, muss man mit einer riesigen Menge von Teilnehmern rechnen. Daher kann ein Schlüsselmanagement wie es noch vor fünfzig Jahren üblich war (je zwei Teilnehmer, die miteinander kommunizieren wollen, tauschen einen geheimen Schlüssel aus), schlechterdings nicht funktionieren. Hier setzt man die Methoden der Public-Key-Kryptographie ein.

Dass Geldüberweisungen elektronisch getätigt werden und nicht über papierene Überweisungsträger erfolgen, hat sich weitgehend durchgesetzt. Stichworte sind „Homebanking" und „electronic cash". Für solche Anwendungen wird ein elektronischer Ersatz für die herkömmliche handschriftliche Unterschrift benötigt. In vielerlei Hinsicht ist die so genannte elektronische Signatur besser als die vertraute handschriftliche Unterschrift.

Es gehört nicht viel Prophetengabe dazu, vorauszusagen, dass die Kryptologie, die sich erst in den letzten Jahrzehnten als seriöse Wissenschaft etabliert hat, auch in der Zukunft ihren rasanten Aufschwung beibehalten wird.

Hier ist ein Wort zur NSA und anderen Geheimdiensten angebracht. In der Tat ist es schockierend, wie viele Daten die NSA abhören und wie viele Kommunikationsverbindungen sie kontrollieren kann. Es scheint so zu sein, dass die Geheimdienste mit ihrer übermächtigen Computerpower alle Sicherheitssysteme aushebeln können. Hier soll nichts beschönigt oder verharmlost werden, zumal wir nicht hinter die Kulissen der Geheimdienste blicken können. Aber: Die einzige Chance, die wir Bürger haben, liegt in der Kryptographie. Gute kryptographische Algorithmen, die in verlässlicher Hard- und Software realisiert sind (hier liegt allerdings der Haken!) können auch scheinbar übermächtigen Gegnern Paroli bieten!

Wir werden auf dieses brisante Thema im Verlauf dieses Buches immer wieder zu sprechen kommen

Jeder, der mit solchen oder ähnlichen Anwendungen zu tun hat, wird zustimmend nicken: „Selbstverständlich brauchen wir Sicherheit! Aber – warum soll die Kryptologie das Allheilmittel sein? Gibt es nicht auch andere Methoden, um Sicherheit zu erreichen?“ Natürlich gibt es andere Methoden! Denken Sie zum Beispiel an die über Jahrhunderte entwickelten ausgefeilten Techniken, die dazu dienen, unsere Banknoten sicher zu machen: Spezialpapier, komplexe (manchmal sogar schöne) Bilder, Präzisionsdruck, Wasserzeichen, Silberdraht, und vieles andere mehr.

Also: Warum Kryptologie?

Die Antwort ist einfach: Kryptologie ist besser! Ein Grund dafür ist, dass Kryptologie eine mathematische Disziplin ist. Das mag übertrieben klingen, ist es aber nicht: Die Mathematik liefert die theoretische Rechtfertigung für die Stärke eines Verfahrens. Mit Mathematik kann man – im Idealfall – beweisen, dass ein kryptographischer Algorithmus ein gewisses Sicherheitsniveau hat. Und wenn die Sicherheit einmal mathematisch bewiesen ist, ist kein Zweifel mehr möglich, dass dieser Algorithmus wirklich sicher ist. Man muss sich dann nicht mehr auf (sich mitunter widersprechende) Expertenmeinungen verlassen, man braucht sich bei der Einschätzung der Sicherheit nicht auf die „heutige Technologie“, die morgen ganz anders sein kann, zu berufen usw.

Ich muss allerdings gestehen, dass solche Beweise bislang nur in sehr wenigen Fällen gelungen sind. Dennoch: Mathematik ist ein vertrauenswürdiges Instrument, um Kryptosysteme systematisch zu untersuchen (das heißt zu entwerfen und zu analysieren). Das ist der Grund, weshalb kryptologische Mechanismen im Zweifel anderen Sicherheitsmechanismen vorzuziehen sind: In dubio pro mathematica!

Die Wissenschaft, die sich mit all diesen Problemen beschäftigt, heißt Kryptologie oder Kryptographie. In den sechs Kapiteln dieses Buches werde ich ihnen die Themen vorstellen, die meiner Meinung nach wesentlich für das Verständnis der modernen Kryptologie sind. Wir werden also den Teil der Kryptologie behandeln, der zur mathematischen Allgemeinbildung gehört. Mein Ziel ist es, die Grundgedanken dieses Gebiets darzulegen. Das kann ich nicht leisten, ohne wenigsten ab und zu ein System im Detail zu behandeln. Aber ich habe versucht, einen lesbaren Text zu schreiben, der weitgehend ohne formalen Ballast auskommt.

Das erste Kapitel hat zwei Ziele. Zunächst betrachten wir einige monoalphabetische Algorithmen über dem natürlichen Alphabet, wie etwa die Cäsar-Chiffre. Es wird sich herausstellen, dass all diese Chiffrierungen relativ leicht zu brechen sind. Bei der Darstellung dieser Algorithmen werden wir uns zwanglos die grundlegenden kryptologischen Begriffe und Bezeichnungen klar machen.

Das zweite Kapitel ist polyalphabetischen Chiffrierungen über dem natürlichen Alphabet gewidmet. Diese sind komplizierter aufgebaut, und man benötigt daher auch präzisere Methoden, um sie zu brechen. Zwei solche Methoden, nämlich den Kasiski-Test und den Friedman-Test werden wir detailliert besprechen.

Das dritte Kapitel ist ein theoretisches Sahnehäubchen. Dort werden Sie nicht nur eine Erklärung des Begriffs „sicher“, sondern auch ein perfektes, also sogar theoretisch sicheres Chiffriersystem (das sogenannte One-Time-Pad) finden. Die zweite Hälfte dieses Kapitels dient dem Studium der „rückgekoppelten Schieberegister“, auf denen sehr viele moderne Algorithmen beruhen.

Im vierten Kapitel werden wir uns mit den Diensten „Integrität“ und „Authentizität“ beschäftigen. In diesem Gebiet der Kryptographie versucht man nicht, Daten geheim zu halten, sondern vielmehr, ihre Unversehrtheit zu garantieren und Gewissheit über den Datenursprung zu erhalten. Diese Problemstellung hat in den letzten Jahren der reinen Geheimhaltung der Daten den Rang abgelaufen und ist dafür verantwortlich, dass die Kryptologie nicht mehr auf den abgeschotteten Bereich der militärischen Anwendungen beschränkt ist, sondern sich im rauen Wind der freien Wirtschaft bewähren kann. An einem alltäglichen Beispiel wird die Bedeutung der Datenintegrität klar: Ich kann es zur Not verschmerzen, wenn ein Unbefugter erfährt, wie viel Geld mir mein Verlag als Honorar für dieses Buch jährlich überweist; mindestens einer der Beteiligten würde aber ziemlich unfreundlich reagieren, wenn der Unbefugte an den Überweisungen etwas verändern kann, sei es den Betrag, sei es die Kontonummer!

In diesem Kapitel werden wir auch die geheimnisvollen „Zero-Knowledge-Algorithmen“ kennen lernen. Dabei geht es um folgende Frage: Können

Sie mich davon überzeugen, ein bestimmtes Geheimnis zu haben, ohne mir auch nur das Geringste davon zu verraten? Diese Algorithmen haben in den letzten Jahren großes Interesse gefunden. Schließlich werden wir Chipkarten behandeln, die sich als das Werkzeug zur Realisierung von kryptographischen Diensten für jedermann als ideales Werkzeug anbieten.

Im fünften Kapitel werden wir die zukunftsweisenden Public-Key-Systeme („asymmetrische" Systeme) vorstellen, deren Einführung durch Diffie und Hellman 1976 eine Revolution der Kryptologie war. Dies zeigt sich zuletzt auch darin, dass seitdem die Kryptologie ein unverzichtbarer Bestandteil der Mathematik und der Informatik geworden ist. Die Eleganz der Public-Key-Algorithmen ist allerdings weit mehr als ein Spielzeug für Mathematiker: Ihre Erfindung war entscheidend durch praktische Probleme motiviert. Wir werden sehen, dass man mit solchen Algorithmen wichtige praktische Probleme auf sehr befriedigende Art und Weise lösen kann.

Im abschließenden sechsten Kapitel studieren wir ein Problem, das am Rande der Kryptologie liegt, nämlich Anonymität. In vielen rechnergestützten Systemen wird Sicherheit vor allem dadurch erreicht, dass alle relevanten Vorgänge aufgezeichnet und ausgewertet werden. Damit sind all diese Ereignisse rekonstruierbar, nichts bleibt verborgen: Der Computer spielt in gewisser Weise die Rolle Gottes: Er weiß alles. Frage: Ist es möglich, ein elektronisches System zu entwerfen (beispielsweise für elektronisches Bezahlen), das grundsätzlich nicht allwissend ist, aber dennoch die notwendige Sicherheit bietet? Anders gefragt: Widersprechen sich Sicherheit und Anonymität? Wir werden zwei Systeme vorstellen, bei denen sich diese beiden Qualitäten vereint sind. Insbesondere werden wir diskutieren, ob es ein elektronisches Äquivalent zum üblichen Münzgeld geben kann.

Sie merken: Das sind zum großen Teil neue, aufregende, sehr praxisbezogene Themen. Wenn Sie fürchten, dass alles sehr kompliziert und undurchschaubar wird, dann kann ich Ihnen sagen: Keine Angst: Die Kryptologie ist ein Glücksfall, da man gerade die neuen und zukunftsweisenden Dinge ziemlich anschaulich erklären kann. Ich habe versucht, alles möglichst verständlich, klar und – hoffentlich – unterhaltsam darzustellen.

Es ist nicht notwendig, die Kapitel der Reihe nach zu lesen. Erschrecken Sie nicht, wenn Ihnen die eine oder andere Stelle zunächst kryptisch vorkommt. In den allermeisten Fällen ist der folgende Text auch ohne Kenntnis dieser „schwierigen" Stelle verständlich.

Mein Rat: Überblättern Sie ruhig die eine oder andere Stelle – und tun Sie das guten Gewissens!

Am Ende jeden Kapitels finden sich Übungsaufgaben, insgesamt weit über 100. Alle Übungsaufgaben werden Ihnen, so hoffe ich, Spaß machen; die meisten sind einfach zu lösen. [Hinweis: Die schwierigeren Übungsaufgaben enthalten einen Hinweis zu ihrer Lösung.]

Einige wenige, etwas schwierigere Aufgaben sind durch das Symbol * gekennzeichnet. Sie werden auch Programmieraufgaben finden. Durch diese können Sie sich überzeugen, dass die dargestellten Verfahren auch wirklich funktionieren. Keine dieser Aufgaben, die man an dem „Klammeraffen" @ erkennt, ist besonders schwierig. Manche erfordern einige Zeit – wie das beim Programmieren so üblich ist.

Einige Aufgaben fordern Sie heraus, einen Geheimtext zu entschlüsseln. Wenn Sie kontrollieren wollen, ob Sie auf der richtigen Spur sind, haben Sie die Möglichkeit, im Anhang bei *Entschlüsselung der Geheimtexte* nachzuschauen.

Eine Erfahrung will ich Ihnen nicht vorenthalten: Ich habe von mehr als einer hübschen jungen Dame gehört, die es anregend fand, mit diesem Buch in die Badewanne zu steigen und sich dort der Lektüre hinzugeben. Ein schöneres Kompliment kann ich mir kaum vorstellen! Ich hoffe, dass auch Sie Spaß bei der Lektüre dieses Buches haben.

Mein Dank gilt allen, die dieses Buchprojekt unterstützten, kritisch begleiteten und förderten. Es sind zu viele, als dass ich sie hier alle nennen könnte.

An erster Stelle danke ich meinen nächsten Angehörigen, Monika, Christoph und Maria. Sie mussten nicht nur häufig als Versuchskaninchen herhalten, sondern haben mir auch mehrere Male großzügig Urlaub zum Bücherschreiben gewährt.

Ferner gilt mein Dank meinen Kollegen A, C, F, I, J, L, M, R, U – in alphabetischer Reihenfolge, wobei einige Buchstaben mehrfach zu zählen sind und mindestens einer fett zu drucken gewesen wäre. Sie haben das Entstehen dieses Buches auf mannigfaltige Weise gefördert: durch akribische Kritik, durch konstruktive Vorschläge, durch aufmunternde Gespräche, durch inspirierende Sitzungen, durch schnelles Beschaffen von Material usw. usw.

Ein besonderer Dank gebührt Frau Dr. Ute Rosenbaum, die sich in der letzten Phase der Herstellung dieses Buches engagiert und effizient alle möglichen technischen und nichttechnischen Probleme gelöst hat.

Dem Verlag Springer Spektrum danke ich für die langjährige problemlose, freundliche und geduldige Zusammenarbeit.

Inhaltsverzeichnis

1

Cäsar oder Aller Anfang ist leicht!

Ibich habibebi dibich,
Lobittebi, sobi liebib.
Habist aubich dubi mibich
Liebibä Neibin, vebirgibib.
Nabih obidebir febirn
Gobitt seibi dibir gubit.
Meibin Hebirz habit gebirn
Abin dibir gebirubiht
(Joachim Ringelnatz).

Es nicht immer leicht, jung und verliebt zu sein. Die klassische Literatur lehrt uns: Wenn immer eine Julia ihrem geliebten Romeo eine vertrauliche Botschaft übermitteln möchte, dann gibt es fast immer einen missgünstigen Bösewicht, der das junge Glück dadurch zu stören versucht, dass er den Brief abfängt (siehe Abb. 1.1).

Vielleicht möchte der Missgünstling die Nachricht „nur" lesen. Das Rezept gegen einen solchen *passiven Angriff* ist Verschlüsselung, das Thema dieses und der folgenden drei Kapitel. Gegen einen *aktiven Angreifer*, also einen Bösewicht, der die Nachricht zu verfälschen trachtet, ist ein anderes Kraut gewachsen: Romeo und Julia sollten die Methoden aus Kap. 4 und 5 studieren, um dagegen gewappnet zu sein.

Die Moral von der Geschicht für Verliebte, aber auch für Diplomaten, Internetbenutzer, Börsenspekulanten – kurz für alle, die vertrauliche Nachrichten verschicken müssen, muss lauten, geeignete Gegenmaßnahmen einzusetzen, die dem Angreifer die Suppe versalzen. Eine Möglichkeit ist die Verschlüsselung: Julia ersetzt die Buchstaben ihres heimlichen Briefchens durch andere Buchstaben oder Zahlen oder Symbole.

Es ist natürlich keine Kunst, eine Nachricht so zu verunstalten, dass überhaupt kein Mensch mehr etwas damit anfangen kann. Die Herausforderung für die Kryptologie besteht vielmehr darin, die Nachricht so zu transformieren, dass niemand außer dem berechtigten Empfänger diese entziffern kann. Daher muss der Empfänger dem Angreifer etwas voraushaben. Mit Hilfe die-

A. Beutelspacher, *Kryptologie*, DOI 10.1007/978-3-658-05976-7_1,

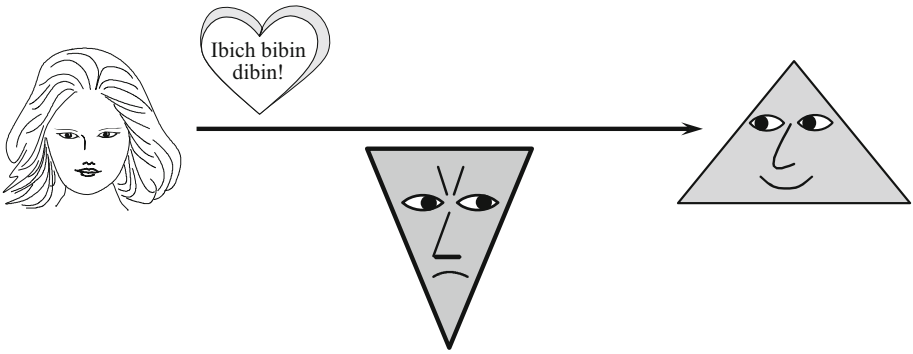


Abb. 1.1 Ein passiver Angreifer

ser Information kann der Empfänger entschlüsseln; sie darf keinem Angreifer zur Verfügung stehen, denn sonst könnte dieser die Nachricht genau so leicht wie der Empfänger entschlüsseln. Man nennt diese exklusive Information den *Schlüssel*. Die klassischen Verschlüsselungsverfahren sind so aufgebaut, dass Sender und Empfänger einen gemeinsamen geheimen Schlüssel besitzen, mit dem der Sender verschlüsselt und der Empfänger entschlüsselt. Da Sender und Empfänger über das gleiche Geheimnis verfügen, nennt man solche Verfahren *symmetrisch*. In Kap. 5 werden wir sehen, dass es auch asymmetrische Verschlüsselungsalgorithmen gibt: In solchen Systemen braucht nur der Empfänger einen geheimen Schlüssel.

In diesem Kapitel betrachten wir die in gewissem Sinne einfachsten symmetrischen Verschlüsselungsalgorithmen, nämlich solche, bei denen ein- und derselbe Buchstabe immer durch ein- und dasselbe Symbol ersetzt wird. Zum Beispiel könnte der Klartextbuchstabe e stets mit dem Geheimtextbuchstaben K chiffriert werden. Gegen Ende des Kapitels wird uns klar werden, dass solche Systeme in der Regel nicht allzu empfehlenswert sind.

Zunächst einige Worte zur Terminologie. Die Begriffe *Kryptologie* und *Kryptographie* sind aus den griechischen Wörtern $\kappa\rho\upsilon\pi\tau\omicron\sigma$ (geheim), $\lambda\omicron\gamma\omicron\sigma$ (das Wort, der Sinn), und $\gamma\rho\alpha\varphi\varepsilon\iota\nu$ (schreiben) gebildet. Beide bezeichnen die Kunst und die Wissenschaft, die sich damit beschäftigt, Methoden zur Verheimlichung von Nachrichten zu entwickeln. Manche Leute unterscheiden zwischen *Kryptographie*, der Wissenschaft von der Entwicklung von Kryptosystemen, *Kryptoanalyse*, der Kunst diese zu brechen und bezeichnen mit *Kryptologie* die Gesamtheit dieser Wissenschaften. Es besteht aber keine Gefahr von Missverständnissen, wenn man Kryptographie und Kryptologie

synonym benutzt. Ganz sicher ist der Bedeutungsunterschied dieser beiden Begriffe bei weitem nicht so groß wie bei Geologie und Geographie oder Philologie und Philosophie oder gar Astronomie und Astrologie.

Der Text, die Nachricht, die Buchstaben- oder Zeichenfolge, die wir übermitteln wollen, heißt der *Klartext*; wir werden den Klartext in der Regel durch kleine Buchstaben a, b, c, … darstellen. Die verschlüsselte Nachricht (also die Buchstaben- oder Zeichenfolge, die tatsächlich übermittelt wird) nennen wir den *Geheimtext* (in der älteren Literatur wird der Geheimtext auch *Kryptogramm* genannt); ihn werden wir in Großbuchstaben A, B, C, … schreiben. Den Verschlüsselungsvorgang nennen wir *Chiffrieren*, den Entschlüsselungsvorgang *Dechiffrieren*. Der Sender chiffriert also, während der Empfänger dechiffrieren muss, bevor er die Nachricht lesen kann.

Die Texte, die wir verschlüsseln werden, bestehen aus *Zeichen*; die Zeichen bilden insgesamt ein *Alphabet*. In den ersten beiden Kapiteln wird unser Alphabet meist das natürliche Alphabet {a, b, c, …, x, y, z} sein. Wir könnten aber als Zeichen z. B. auch die Zahlen 1, …, 26, die Bits 0 und 1 oder, wenn es für unsere Betrachtungen günstig ist, auch die binären Folgen der Länge 64 wählen. In diesem Fall ist das Alphabet die Menge

$$\{(a_1, ..., a_{64} | a_1 \in \{0,1\}\}.$$

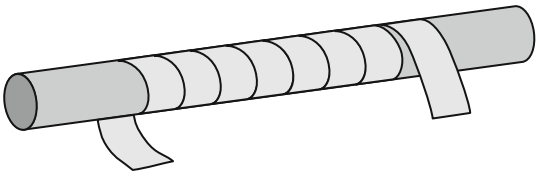
In der Tat arbeiten die heutigen Chiffrierverfahren auf Bits oder Folgen von Bits. In Abschn. 1.7 werden wir einige dieser Verfahren beschreiben.

Im Widerspruch zu der Ankündigung in der Überschrift beginnt die Geschichte der Kryptographie *vor* Cäsar.

1.1 Die Skytala von Sparta

Die Geschichte fängt vor ungefähr 2500 Jahren an. Wie wir von dem griechischen Historiker Plutarch wissen, benutzte die Regierung von Sparta folgende trickreiche Methode zur Übermittlung geheimer Nachrichten an ihre Generäle: Sender und Empfänger mussten beide eine so genannte *Skytala* (sprich: Skýtala) haben; das waren zwei Zylinder mit genau dem gleichen Umfang. Der Sender wickelte ein schmales Band aus Pergament spiralförmig um seine Skytala und schrieb dann der Länge nach seine Nachricht auf das Band (vergleiche Abb. 1.2). War das Band abgewickelt, konnte die Nachricht nur von einer Person gelesen werden, die einen Zylinder genau desselben Umfangs hatte – hoffentlich nur der Empfänger.

Abb. 1.2 Eine Skytala



Wir können uns eine Skytala-Verschlüsselung auch so vorstellen, dass man den Text spaltenweise (d. h. von oben nach unten) in einer bestimmten Anzahl von Zeilen aufschreibt.

Wir betrachten ein Beispiel in moderner Sprache. Stellen wir uns vor, wir hätten einen Papierstreifen abgefangen, auf dem wir die folgende Buchstabenfolge lesen:

S I H L T I T A D O C I U E L H S P R O E T T K G R D Z R I H A I Y E E S E P !

Die Skytala des Senders hat einen Umfang, den wir durch die Anzahl von Buchstaben ausdrücken können, die „einmal um die Skytala herum" passen. Mit anderen Worten: Die Zahl u ist die Anzahl der Zeilen, in die wir den Text anordnen. Zur Analyse probieren wir einfach verschiedene Umfänge u aus. Wenn wir u = 4 wählen, ergibt sich vollkommener Unsinn:

S T D U S E G R I S
I I O E P T R I Y E
H T C L R T D H E P
L A I H O K Z A E !

Wenn wir aber den Text in u = 5 Zeilen anordnen, wird die Botschaft klar:

S I C H E R H E
I T I S T D A S
H A U P T Z I E
L D E R K R Y P
T O L O G I E !

Algorithmus 1.1: Skytala-Verschlüsselung

Schlüssel:	Der Umfang u der Skytala bzw. die Anzahl der Zeilen.
Chiffrieren:	Man schreibt den Klartext zeilenweise in ein Schema mit genau u Zeilen; man erhält den Geheimtext, indem man den Text spaltenweise liest.
Dechiffrieren:	Man schreibt den Geheimtext spaltenweise in ein Schema mit genau u Zeilen; daraus erhält man den Klartext, indem man zeilenweise liest.

Die Skytala ist der Prototyp eine *Transpositionschiffre*; bei einer solchen bleiben die Buchstaben, was sie sind, aber nicht, wo sie sind. Ein Mathematiker würde eine Transpositionschiffre beschreiben als eine Permutation der Stellen des Klartextes. Viele populäre Algorithmen sind Transpositionschiffren. (Vergleiche zum Beispiel die Übungsaufgaben 6 und 26). Kapitel III des Buches [Smi71] enthält eine reiche Auswahl von „klassischen" Transpositionsalgorithmen.

Transpositionsalgorithmen sind ein wichtiger Baustein für moderne Algorithmen. Die andere Komponente sind die *Substitutionsalgorithmen*; bei diesen wird die Nachricht dadurch unlesbar gemacht, dass jeder Buchstabe zwar seine Position behält, aber durch einen anderen ersetzt wird.

Dies ist das Stichwort für den Auftritt Cäsars.

1.2 Verschiebechiffren

Einer der ersten, der kryptologische Techniken benutzt haben soll, war der römische Feldherr und Staatsmann C. Julius Cäsar (100 bis 44 v. Chr.). Bei Sueton (Caes. LVI) lesen wir:

> Exstant et [epistolae] ad Ciceronem, item ad familiares de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset; quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.

Übersetzt lautet dies etwa

> Es existieren auch [Briefe von Cäsar] an Cicero und an Bekannte über Dinge, in denen er, wenn etwas vertraulich übermittelt werden musste, in Geheimschrift schrieb. D. h. er veränderte die Ordnung der Buchstaben derart, dass