Joachim Swoboda | Stephan Spitz | Michael Pramateftakis

Kryptographie und IT-Sicherheit

Aus dem Programm IT-Sicherheit und Datenschutz

IT-Sicherheit mit System
von Klaus-Rainer Müller

Der IT Security Manager
von Heinrich Kersten und Gerhard Klett

IT-Sicherheit – Make or Buy
von Marco Kleiner, Lucas Müller und Mario Köhler

Quantum Computing verstehen
von Matthias Homeister

IT-Sicherheit kompakt und verständlich
von Bernhard C. Witt

Elektronische Signaturen in modernen Geschäftsprozessen
von Volker Gruhn, Vincent Wolff-Marting, André Köhler, Christian Haase und Torsten Kresse

Joachim Swoboda | Stephan Spitz |
Michael Pramateftakis

Kryptographie und IT-Sicherheit

Grundlagen und Anwendungen

Mit 115 Abbildungen

STUDIUM

VIEWEG+
TEUBNER

Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2008

Lektorat: Sybille Thelen | Andrea Broßler

Der Vieweg+Teubner Verlag ist ein Unternehmen von Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: MercedesDruck, Berlin
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-0248-4

Vorwort

Dieses Buch entstand auf der Basis von Vorlesungen über Kryptographie und angewandte IT-Sicherheit, die seit Jahren in der Elektrotechnik und Informationstechnik (EI) der Technischen Universität München (TUM) gehalten werden, aber ebenso auf der Basis von industrieller Erfahrung auf diesem Gebiet. Wir wünschen Ihnen, verehrte Leserinnen und Leser dieses Buches, Gewinn und auch Freude.

Am Anfang des Vorhabens fragten wir uns: Wozu noch ein Buch über Kryptographie schreiben, wenn man fast alle Informationen dazu schon im Internet oder anderen Büchern findet? Wo können wir Studenten und Lesern dieses Buchs mehr bieten als Wikipedia oder existierende Literatur? Man findet zwar im Netz viele und gute Einzeldarstellungen. Ein Buch hat jedoch die Chance einer einheitlichen und ausgewogenen Darstellung. Es behandelt sowohl die Sicherheits-Technologien als auch die technischen und mathematischen Grundlagen.

Dieses Buch wurde von Ingenieuren für Ingenieure und Informatiker geschrieben. Die moderne Kryptographie benötigt diskrete Mathematik für endliche Zahlenmengen (Modulo-Arithmetik). Sie wird hier jedoch nur als Hilfsmittel in einer pragmatischen Weise benutzt, so dass man die Verfahren der Kryptographie und die darauf aufbauenden Sicherheits-Technologien verstehen kann. Beweise stehen im Hintergrund. Im Vordergrund steht das Verständnis für die Leistung kryptographischer Verfahren und deren Anwendung in der Informationstechnologie.

Kryptographie, die Verschlüsselung von Information, war lange Zeit eine Sache der Geheimdienste. Mit der Verbreitung des Internet wurde die Nutzung von Kryptographie eine Sache von jedermann: Bei Online-Banking ist sicherzustellen, dass wir PINs und TANs nicht einer vorgespiegelten Bank übermitteln (Authentizität), dass eine Überweisung nicht verändert wird (Integrität) und auch nicht abgehört werden kann (Vertraulichkeit). Bei einem Kauf über das Internet sollen die Kundendaten durch Dritte nicht beobachtbar sein.

Allgemein sind kryptographische Verfahren unverzichtbar bei der Realisierung von elektronischen Geschäftsprozessen. In Mobilfunknetzen sichern sie die Abrechnung. Kryptographische Verfahren sind eine Basis für Sicherheit im Internet und in Endgeräten oder für die Vergabe elektronischer Lizenzen.

Seit der Entwicklung des Internet wurde in den 1970er Jahren eine der wichtigsten Erfindungen seit Jahrtausenden der Kryptographie gemacht: Mit den asymmetrischen Schlüsseln, die aus einem geheimen, privaten Schlüssel und einem zugehörigen öffentlichen Schlüssel bestehen, ist es nicht mehr erforderlich, einen geheimen (symmetrischen) Schlüssel im Agentenkoffer zu übertragen. Diese Aufgabe kann heutzutage eine Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers leisten.

In *Kapitel 1 „Ziele und Wege der Kryptographie“* werden Sicherheitsdienste und Sicherheitsmechanismen begrifflich eingeführt und einfache kryptographische Mechanismen anhand historischer Verfahren veranschaulicht. Was muss für die praktische Sicherheit beachtet werden und was versteht man unter perfekter Sicherheit.

Kapitel 2 „Symmetrische Chiffren“ beginnt mit endlichen Zahlenmengen und Restklassen. Es wird dabei Wert auf Anschaulichkeit gelegt und die Mathematik auf den Bedarf der Folgekapitel beschränkt. Man kann damit die Mathematik in kleinen Portionen und nahe zur Anwendung „verdauen“. Es folgen die aktuell wichtigen symmetrischen Verschlüsselungsverfahren, wie

die Blockchiffren DES, Triple-DES und AES als Nachfolger von DES sowie die Stromchiffren RC4 und A5. Ein vorgeschalteter Abschnitt über Erweiterungskörper dient nur einem tieferen Verständnis von AES und kann auch übergangen werden.

„Hash-Funktionen“ in Kapitel 3 erzeugen für ein Dokument einen charakteristischen Fingerabdruck, der als Hash-Wert bezeichnet wird. Hash-Funktionen sollen kollisionsresistent sein. Das heißt, es soll nicht möglich sein, unterschiedliche Dokumente mit gleichem Hash-Wert zu finden. Hash-Funktionen können mit Hilfe von Blockchiffren oder eigenständig konstruiert werden. Eine Hash-Funktion kann auch mit einem geheimen Schlüssel kombiniert werden, um damit einen „Message Authentication Code“ (MAC) auf Basis einer Hashfunktion zu bilden (HMAC).

Für *„Asymmetrische Chiffren“ in Kapitel 4* wird das Rechnen mit Potenzen modulo n benötigt. Mit anschaulichen Beispielen wird erleichtert, diese Grundlagen zu verstehen. Die Verfahren mit asymmetrischen Schlüsseln RSA und ElGamal sind inzwischen die Klassiker für die Übertragung von symmetrischen Sitzungsschlüsseln und für die digitale Signatur. Neuere Verfahren auf der Basis von elliptischen Kurven kommen mit kürzeren Schlüsseln aus. Zu ihrem Verständnis wird in möglichst anschaulicher Weise in die erforderliche Mathematik eingeführt. „Elliptic Curve Cryptography“ (ECC) eignet sich besonders für Realisierungen auf Chipkarten.

„Authentifikations-Protokolle“ in Kapitel 5 dienen dazu, um Sicherheit über die Identität des Kommunikationspartners zu erhalten. Ein wichtiges Verfahren ist die „Challenge-Response-Authentifikation“, die eine aktuelle Antwort auf eine spezielle Frage anfordert. Für die Authentifikation werden meist asymmetrische Schlüssel in Verbindung mit Challenge-Response benutzt.

Die beiden letzten Kapitel widmen sich dem Einsatz der zuvor dargestellten kryptographischen Verfahren und Protokolle in Anwendungen, die bereits seit längerem Einzug in den elektronischen Alltag gefunden haben. *Kapitel 6 „Sicherheitsprotokolle und Schlüsselverwaltung“* beschreibt, wie durch eine Schlüsselverwaltung der öffentliche Schlüssel einer Person verfügbar gemacht und bescheinigt wird, dass der öffentliche Schlüssel sicher zu einer bestimmten Person gehört. Diese sogenannten „Public Key Infrastrukturen“ (PKI) sind eine Grundlage für die Sicherheit im Internet. Sicherheitsprotokolle werden für drahtgebundene und für Funk-Netze besprochen. Gerade bei offenen Computer-Netzen spielen die in den vorherigen Kapiteln behandelten Verfahren für Authentifikation, Integrität und Vertraulichkeit eine wichtige Rolle.

Kapitel 7 „Chipkarten und Sicherheitsmodule“ bietet einen Einblick in deren Anwendung und Funktionsweise. Die häufigste Anwendung von Chipkarten ist die Authentisierung von Teilnehmern in Mobilfunksystemen. Mit mehreren Milliarden ausgegebenen SIM-Karten (UMTS, GSM) ist dieser Markt für Chipkarten der größte. Neuere Entwicklungen, wie Java-Chipkarten, oder ganz aktuelle Trends, wie Internet-Protokolle auf Chipkarten, werden vorgestellt. Eine weitere Anwendung der Chipkarten-Technologie liegt in dem Bereich „Trusted Computing“. Das hier eingesetzte „Trusted Platform Module“ (TPMs) ist aus technischer Sicht den Chipkarten sehr ähnlich.

Dieses Buch ist gedacht als eigenständiges Fachbuch für das Selbststudium oder als begleitende Unterlage zu einer Vorlesung. Übungsbeispiele mit Lösungen können zur weiteren Vertiefung herangezogen werden. Neben den grundlegenden kryptographischen Algorithmen, Mechanismen und Protokollen gibt das Buch Einblick in Anwendungsgebiete, wie Sicherheitsver-

fahren in Internet und Mobilfunknetzen, Betriebssysteme von Chipkarten, Trusted Computing und Public-Key-Infrastrukturen. Das Buch zielt auf eine kompakte und ausgewogene Einführung in die Kryptographie und deren aktuelle Anwendung. Dabei sind die neuesten und praktischen Erfahrungen eingeflossen, einerseits über Schlüsselverwaltung (PKI) und Sicherheitsprotokolle und andererseits über Chipkarten und Sicherheitsmodule (TPM).

Für weitergehende und spezielle Fragen bieten die angegebene Literatur und auch das Internet oft aktuelle Antworten. Zum Experimentieren mit den einzelnen Algorithmen kann das Werkzeug CrypTool (http://www.cryptool.de/) sehr empfohlen werden.

Wir danken Herrn Bernhard Esslinger für das umfangreiche fachliche Feedback und für das externe Vorwort. Unser Dank gilt ferner dem Vieweg-Verlag für eine vertrauensvolle Zusammenarbeit sowie Frau L. Heckmann für die redaktionelle Durchsicht des Skripts.

München und Athen, im Dezember 2007

Joachim Swoboda
Stephan Spitz
Michael Pramateftakis

Vorwort von Bernhard Esslinger

Die Autoren dieses Buches danken Herrn Bernhard Esslinger für dieses externe Vorwort. Herrn Esslinger braucht man nicht vorzustellen. Dennoch wollen die Autoren einige Worte zu seiner Einführung festhalten:

Hr. Esslinger hat intensive theoretische, praktische und berufliche Erfahrung auf dem Gebiet der IT-Sicherheit und Kryptographie. Er war Entwicklungsleiter der Sicherheitskomponenten des SAP-Systems R/3, Chief Information Security Officer (CISO) bei der SAP AG und Leiter IT-Sicherheit bei der Deutschen Bank AG. Derzeit leitet er bei der Deutschen Bank das Cryptography Competence Center, das dort weltweit für die angemessene Nutzung von Kryptographie zuständig ist. Außerdem hat Hr. Esslinger einen Lehrauftrag für IT-Sicherheit und leitet seit 10 Jahren das Open-Source-Projekt CrypTool, das das weltweit erfolgreichste Lernprogramm zum Thema Kryptologie erstellt. Hr. Esslinger schreibt dieses Vorwort als Privatperson.

Joachim Swoboda, Stephan Spitz, Michael Pramateftakis

In den letzten 10 Jahren gab es mehr und mehr Bücher zum Thema Kryptographie und IT-Sicherheit, und doch ist dies ein einzigartiges Buch, worauf ich am Ende meines Vorwortes noch eingehen möchte.

So wie die Bedeutung der EDV (oder neuer IT = Informationstechnologie) in der Gesellschaft in den letzten Jahren zunahm, so nehmen auch die Bedeutung von IT-Sicherheit und Kryptographie zu.

Unternehmen treffen ihre Entscheidungen basierend auf den Daten in ihren Computern, sie steuern Waren- und Geldströme damit, und das immer kurzfristiger. Gleichzeitig werden immer mehr Daten gesammelt, um fundiertere Entscheidungen zu treffen, besseren Service zu bieten oder vermeintlich besser Terroristen fangen zu können.

Die IT-Abhängigkeit ist den Firmen und Behörden bewusst: Regularien wie SOX (Sarbanes-Oxley Act), die sich eigentlich auf die Exaktheit der betriebswirtschaftlichen Daten beziehen, schließen inzwischen die EDV mit ein. Staaten weltweit definieren die „Kritischen Infrastrukturen“, und Behörden wie das BSI oder das NIST bieten hervorragende Maßnahmenkataloge, mit deren Hilfe man seine EDV sicher betreiben kann.

Aber auch wenn die Verfahren der Kryptographie und IT-Sicherheit eigentlich relativ gut verstanden und ausgereift sind, so werden sie doch immer wieder fehlerhaft oder nachlässig angewandt. Hierzu ein paar **Beispiele** (Namen werden nur bei schon in der Presse publizierten Fällen genannt):

- Im 4. Quartal 2007 gab es in Großbritannien drei große Skandale mit Datenverlusten bisher unbekannten Ausmaßes:
  Mitte November wurde bekannt, dass der britischen Behörde HM Revenues and Customs

zwei CDs beim Postversand verloren gingen, auf denen Personendatensätze mit Name, Adresse, Geburtsdatum, nationaler Versicherungsnummer und teilweise auch Kreditkartennummer gespeichert waren (angeblich Daten von 25 Millionen Menschen, die zu Familien mit Kindergeldempfängern gehörten).
Mitte Dezember wurde bekannt, dass dem Verkehrsministeriums durch Outsourcing der Datenspeicherung an eine US-Firma eine Festplatte mit Datensätzen von drei Millionen Fahrschülern abhanden gekommen ist.
Und kurz vor Weihnachten meldete der staatliche Gesundheitsdienst, dass „Tausende Patienteninformationen" verloren gegangen waren (laut Aufsichtsbehörde waren das allein im Osten Londons die Daten von 160.000 Kindern). Die Patientendaten von Erwachsenen und Kindern kamen neun Verwaltungszentren des britischen Nationalen Gesundheitssystems (NHS) abhanden. Wie immer hieß es auch vom britischen Gesundheitsministerium, es gebe keinen Hinweis darauf, dass sie in falsche Hände geraten seien.
Kritiker beanstandeten, dass die Regierung zu wenig für die Sicherheit sorgt, aber ständig neue Daten erhebt und speichert.
Warum brauchen untergeordnete Behörden Zugriff auf diese Datenmengen? Warum sind diese Daten beim Transfer nicht verschlüsselt? Warum werden zum Transfer CDs benutzt statt gesicherter TCP/IP-Verbindungen?

- Schlimmer noch als in UK, wo nur die Gefahr besteht, dass diese sensiblen Daten in die falschen Hände gelangen, ist ein Vorgang in Japan, der dort in der zweiten Jahreshälfte 2007 die Regierung erschütterte: Bei ungefähr einem Drittel der Rentenkonten können die Guthaben den Konten nicht korrekt zugeordnet werden. Laut Behördenangaben gingen Rentendaten von mindestens 8,5 Millionen Menschen verloren, und die Daten zu insgesamt 64 Millionen Anträgen auf Rente oder soziale Unterstützung konnten nicht mehr gefunden werden.
  Wo ist die Datensicherung? Wo sind die Signaturen, die die Verbindung herstellen könnten?
- In den USA sind bis Ende 2007 in den verschiedenen Datenbanken der Geheimdienste und des Department of Homeland Security mehr als eine halbe Million Personen gespeichert, die dort fälschlicherweise aufgenommen wurden. Verfahren zur vollständigen Löschung auch rehabilitierter Personen existieren nicht oder funktionieren nicht korrekt. Trotzdem ist die Konsequenz nicht das Aufräumen und Konsolidieren, sondern: Ende 2007 meldete das FBI, dass es rund eine Milliarde USD investieren will, um bis 2013 die weltweit größte Datenbank mit biometrischen Daten zu erstellen.
  Wo bleibt die alte Forderung, z.B. aus dem Datenschutz, nur notwendige Daten zu speichern, für alle Daten ein Verfallsdatum anzugeben und bei allen Daten die Nutzung nur für vorher explizit benannte Gründe zu zulassen?
- In Deutschland wurde bis Mitte 2007 bekannt, dass die Bundeswehr Daten mit Geheimdienstinformationen nicht mehr auf ihren Bändern lesen könne. Oder sollten diese Informationen nicht mehr auffindbar sein? Auf Daten, die explizit nur zur Erhebung von LkW-Maut gesammelt wurden, melden andere Behörden Ansprüche an.
- Aber auch im nichtpolitischen Bereich passieren Fehler mit manchmal schlimmen Folgen:
  - Nicht funktionierende Scanner für die Teile in einem Hochregallager führten fast zur Firmenpleite.
  - Kreditkartennummern, die verschlüsselt übertragen wurden, wurden danach in großem Stil von Webservern im Klartext abgezogen.

- Controller errechneten Kennzahlen für Managemententscheidungen mit Hilfe von Excel-Makros, obwohl nach unterschiedlichen Untersuchungen gerade die selbst erstellten Formeln in großen Excel-Tabellen immer wieder fehlerhaft sind.
- Die kompletten Kundendaten einer amerikanischen Großbank wurden regelmäßig als Backup auf Bänder gesichert, die von einer professionellen Firma zur Datensicherung und Datenspeicherung eingelagert wurden. Leider waren die Daten auf den Bändern nicht verschlüsselt, und manche Bänder gingen schon beim Transport verloren. Aber selbst bei den eingelagerten Bändern kann nicht sichergestellt werden, dass davon keine Kopien angefertigt werden.
- Bei der Einführung von Mitarbeiter-Smartcards und SecurID-Tokens wurden die Super-PINs zum Zurücksetzen der Smartcards auf CD geschickt – unverschlüsselt, ohne Schlüsselmanagement beim Kunden und ohne dass der Kunde die Super-PINs ändern konnte, so dass beim Hersteller theoretisch ebenfalls noch eine Kopie vorliegen kann, mit denen man die Kunden-Smartcards missbrauchen könnte.
- Applikationen verwenden moderne kryptografische Verfahren, aber alles basiert auf schwachen Passworten für Benutzer, Administratoren oder Super-User – ein Kartenhaus.
- Weil die modernen kryptografischen Verfahren inzwischen in Betriebssystemen zur Verfügung stehen, können sie leicht benutzt werden. Die Bedeutung von klar definierten Prozessen für ein gutes Schlüsselmanagement wird übersehen.
- Applikationen verwenden Protokolle, die die verwendeten Verfahren und die Mindeststandards nicht aushandeln können. Jede Umrüstung geht dadurch in die Millionen und wird entsprechend erst (zu) spät durchgeführt.

Das **Buch** bietet einen sehr breiten Überblick über den aktuellen Stand der Kryptographie und IT-Sicherheit und ist eher Praxis/Prozess-orientiert. Dazu definiert es die Ziele der IT-Sicherheit und erläutert, mit welchen kryptografischen Maßnahmen welche Ziele erreicht werden können. Es werden sowohl die Grundbegriffe der Sicherheitsmechanismen (wie beispielsweise Authentizität) als auch – wohl dosiert – die notwenigen mathematischen Grundlagen erläutert (z.B. welche Axiome der Arithmetik bei der Modulo-Operation erfüllt sind und immer wieder, warum dies von Bedeutung ist; siehe Kap. 2.1, 2.5 und 4.1). Die Algorithmen werden ausführlich genug besprochen, um sie nachvollziehen zu können.

Dabei wird der Inhalt stets mit Beispielen ergänzt: wo finden Verfahren wie z.B. AES und RSA Verwendung (z.B. Hybridverschlüsselung in dem E-Mail-Standard S/MIME oder in PGP) oder wie steht es um ihre Anwendbarkeit (z.B. Performance und Patentsituation bei Elliptischen-Kurven-Systemen). Immer wird auch der wichtige kryptoanalytische Aspekt behandelt.

Kapitel 5 (Authentifikationsprotokolle) enthält eine sehr schöne Zusammenstellung, wie die Authentisierung z.B. mit Passwort, mit Challenge-Response-Verfahren, mit digitalen Signaturen, etc. funktioniert.

Abgerundet wird das Buch mit den Kapiteln 6 und 7: Diese erläutern, wo die zuvor genannten Verfahren eine Anwendung finden. Natürlich muss hier eine Auswahl getroffen werden, welche Themen ausführlich besprochen und welche nur kurz angeschnitten werden. Darin enthalten sind aktuelle Themen, die über die einfachen Kryptoalgorithmen (kryptografische Primiti-

ve) hinausgehen: PKI, Sicherheitsprotokolle (wie Kerberos, SSL, IPsec, Protokolle zur IP-Telefonie, WLAN), Chipkarten und ihre Anwendungen (z.B. Verschlüsselung und Authentisierung in GSM-Netzen, Nutzung von SIM-Karten, TPM oder so moderne Tokens wie Internet-Smartcards, für die man keine Treiber mehr braucht, weil sie auf dem Chip selbst den nötigen TCP/IP-Stack implementieren).

Da das Buch als Zielgruppe den versierten Anwender und den Ingenieur hat, liegt der Schwerpunkt nicht auf der puren Mathematik, sondern auf der ausführlichen und klaren Vermittlung des Verständnisses der Grundlagen, der richtigen Anwendung und der korrekten und ausführlichen Darstellung der vorhandenen technischen Möglichkeiten.

Ich halte das Buch für ein schönes Nachschlagewerk und eine sehr gute Grundlage, um sich einen Überblick über das große Thema Kryptographie und IT-Sicherheit zu verschaffen. Vor allem gefiel mir die wohl dosierte Beschreibung der mathematischen Grundlagen sehr gut.

Die anwendungsbezogene Darstellung gelingt so gut, dass ich dem Buch sehr gerne eine gute Aufnahme bei den Lesern wünsche. Und wie die obigen Beispiele zeigen, ist dieses Wissen und die nötige Sensibilität für dieses Thema notwendiger denn je.

Bernhard Esslinger, Dezember 2007

Inhaltsverzeichnis

1 Ziele und Wege der Kryptographie

Was ist Kryptographie?

Wer erinnert sich nicht an einen Seeräuberroman mit einer verschlüsselten Botschaft über einen geheimen Schatz oder (vor der Erfindung von SMS) an verschlüsselte Liebesbotschaften in der Schule. In beiden Fällen soll eine Nachricht geheim bleiben und nur von einem bestimmten Adressaten gelesen werden können.

Kryptographie ist die Wissenschaft der Verschlüsselung von Information durch *Geheimschriften* bzw. *Chiffren* (griechisch: *kryptós* „verborgen“ und *gráphein* „schreiben“). Dabei werden meist geheime Schlüssel benutzt. Die Kryptographie umfasst nicht nur die Anwendung, sondern auch die Entwicklung von Verfahren mit Verschlüsselung. Daneben bezeichnet die *Krypto-Analyse* (auch: Kryptanalyse) sowohl die Untersuchung von Verschlüsselungsverfahren auf ihre Resistenz gegenüber Sicherheitsangriffen als auch das Herausfinden von geheimen Schlüsseln. Kryptoanalyse wird auch *Brech*en oder *Knacken* einer Verschlüsselung genannt. Die Kryptographie bildet mit der Kryptoanalyse zusammen die *Kryptologie*.

Die ältesten Chiffren

Chiffren wurden bereits in Sparta (die Skytale) und dem alten Rom (Caesar-Chiffre) benutzt. Der griechische Historiker Plutarch beschreibt den Einsatz der Skytale während des Peloponnesischen Krieges (431 - 404 v.Chr.) gegen die Perser und Gaius Julius Caesar (100 - 44 v.Chr.) hat die nach ihm benannte Caesar-Chiffre zur geheimen Kommunikation für seine militärische Korrespondenz verwendet. Geheimschriften wurden sicherlich seit frühesten Zeiten benutzt. Es ist zu erwarten, dass Geheimschriften ähnlich alt sind wie die Entwicklung symbolischer Zeichen als eine Form von Schrift. Skytale, Caesar-Chiffre und weitere historische Verfahren werden unten in Kap. 1.1 beschrieben.

Steganographie

Neben der Verschlüsselung gibt es auch die Möglichkeit, die Existenz einer geheimen Botschaft zu verbergen. Solche Verfahren heißen *Steganographie* (griechisch: στεγανός „schützend, verdeckt“). Klassisches Beispiel ist das Schreiben mit Zitronensaft als Tinte, die über der Flamme einer Kerze sichtbar gemacht werden kann. Eine geheime Botschaft kann auch in einem Bild versteckt werden, z.B. codiert durch die Länge von Grashalmen einer Wiese. In digitalen Audio- oder Videodateien lassen sich geheime Botschaften verstecken, indem dafür die niederwertigen Bits der Audio- oder Videodaten genutzt werden, was kaum hörbar oder sichtbar ist. Wenn die versteckten Daten verschlüsselt wurden, dann können diese nur mit Kenntnis des Schlüssels erkannt werden. Versteckte Daten in Audio- oder Videodateien werden z.B. genutzt, um durch digitale Wasserzeichen unrechtmäßig kopierte Dateien zu verfolgen. Das Gebiet der Steganographie ist nicht Gegenstand dieses Buches.

Anwendung der Kryptographie

Kryptographie war lange Zeit eine Sache von Feldherren, Seeräubern und Geheimdiensten. Z.B. nannte sich das heutige Bundesamt für Sicherheit in der Informationstechnik (BSI) noch in

den 1980er Jahren „Zentralstelle für das Chiffrierwesen“ und war von einem Schleier militärischer Geheimhaltung umgeben. Erst mit der verbreiteten Benutzung von PCs und dem Internet rückte die Kryptographie in die allgemeine und zivile Anwendung. Die Anwendung der Kryptographie wird oft kaum bemerkbar, z.B. wenn bei Kauf über einen Web-Service die Kundendaten verschlüsselt übertragen werden.

Heutzutage benutzte Verfahren der Kryptographie haben meist eine mathematische Basis und sind meist standardisiert. Die Sicherheit der Verfahren beruht darauf, dass die Verfahren weltweit von Kryptologen untersucht und eventuelle Schwächen öffentlich bekannt gemacht werden. Falls neue Verfahren der Kryptographie erforderlich werden, hat es sich neuerdings besonders bewährt, dass zur Entwicklung eines neuen Verfahrens weltweit aufgerufen wird, die Vorschläge veröffentlicht werden und ihre Qualität weltweit untersucht wird (Beispiel AES, Kap. 2.6).

Sicherheit der Kryptographie

Die Sicherheit eines kryptographischen Verfahrens liegt also gerade nicht darin, sich ein skurriles Verfahren auszudenken und dieses geheim zu halten, sondern darin, dass die Menge der möglichen Schlüssel für ein Verfahren so groß ist, dass ein Angreifer sie nicht durchprobieren kann. Bei einer Schlüssellänge von z.B. 80 Bit gibt es insgesamt 2^{80} mögliche Schlüssel. Wenn ein Angreifer je Sekunde eine Milliarde (10^9) Schlüssel durchprobieren kann, dann benötigt er $2^{80}/10^9$ sec $\approx$ 38 Millionen Jahre. Diese Aufgabe ist praktisch nicht durchführbar. Jede Verlängerung des Schlüssels um 1 Bit verdoppelt den Aufwand für den Angreifer, d.h. bei 10 Bit Verlängerung vergrößert sich der Aufwand für den Angreifer jeweils ca. um den Faktor 1000.

Symmetrische und asymmetrische Verfahren

Historische Verfahren der Kryptographie sind *symmetrisch*, d.h. Sender und Empfänger benutzen den gleichen Schlüssel für die Verschlüsselung und die Entschlüsselung. In den 1970er Jahren wurden *asymmetrische* Verfahren der Kryptographie erfunden. Sie benutzen ein Schlüsselpaar, das aus einem öffentlichen Schlüssel und einem dazugehörigen privaten Schlüssel besteht. Der private Schlüssel ist geheim, nur sein Besitzer hat Zugang zu ihm.

Asymmetrische Verfahren der Kryptographie brachten — nach Jahrtausenden der symmetrischen Kryptographie — völlig neue Möglichkeiten: (1.) Zum Verschlüsseln braucht kein geheimer Schlüssel mehr übertragen zu werden. Der Sender benutzt dazu den öffentlich bekannten *öffentlichen Schlüssel* des Empfängers. Es muss nur sichergestellt sein, dass der benutzte öffentliche Schlüssel zu dem gewünschten Empfänger gehört. (2.) Asymmetrische Schlüssel erlauben *digitale Signaturen* bzw. *digitale Unterschriften*. Dazu benutzt die unterschreibende Person ihren *privaten Schlüssel*. Mit seinem öffentlichen Schlüssel kann jeder diese digitale Signatur nachprüfen. Da nur die unterschreibende Person Zugang zu ihrem privaten Schlüssel hat, kann sie die digitale Signatur nicht abstreiten. Die digitale Signatur ist also verbindlich.

Sicherheitsdienste

Die Ziele, die man durch kryptographische Verfahren erreichen will, werden als *Sicherheitsdienste* bezeichnet. Die Verbindlichkeit einer digitalen Signatur ist ein solches Ziel. Das bekannteste Ziel ist die Vertraulichkeit, d.h. nur ein bestimmter Adressat kann eine verschlüsselte Botschaft lesen. Weitere *Sicherheitsdienste* neben *Vertraulichkeit* und *Verbindlichkei*t sind

Authentizität, *Integrität*, *Anonymität* und *Zugriffskontrolle*. Sicherheitsdienste geben also die Ziele an, die ein Benutzer erreichen möchte. Neben kryptographischen Verfahren können Sicherheitsziele auch auf anderem Weg erreicht werden, z.B. die Vertraulichkeit durch einen Panzerschrank oder durch einen verlässlichen Boten. Sicherheitsdienste werden in Kap. 1.2 noch im Detail diskutiert.

Sicherheitsdienste werden durch *Sicherheits-Mechanismen* bereitgestellt. Z.B. bietet Verschlüsselung (ein Sicherheitsmechanismus) den Sicherheitsdienst der Vertraulichkeit. Sicherheits-Mechanismen sind die prinzipiellen technischen Mittel, welche die spezielle Wahl noch offen lassen, z.B. Caesar-Chiffre als Verschlüsselungs-Algorithmus. Die Diskussion von Sicherheits-Mechanismen (Kap. 1.3) hat den Vorteil, dass gemeinsame Eigenschaften von unterschiedlichen Sicherheits-Algorithmen zusammengefasst werden können.

Sicherheit und Angriffe, perfekte Sicherheit

Die Sicherheit von kryptographischen Verfahren hängt nicht zuletzt von den möglichen Angriffen ab. Sicherheit und Angriffe sowie der Begriff der perfekten Sicherheit werden in Kap. 1.4 diskutiert.

1.1 Historische Verfahren

Im Lauf der Geschichte ist eine große Vielfalt von Verschlüsselungsverfahren erdacht und benutzt worden. Hier werden nur einige der bekanntesten Vertreter angesprochen. Historische Verfahren sind aus heutiger Sicht einfache Beispiele, um die Prinzipien der Verschlüsselung und deren Resistenz gegen Angriffe anschaulich zu verstehen. Für weitergehende Darstellungen werden [B97], [CrypTool] und insbesondere [K67] empfohlen.

1.1.1 Skytale

Die Skytale wurde seit ca. 500 v.Chr. in Sparta benutzt. Das Gerät für die Verschlüsselung und Entschlüsselung ist ein Holzstab mit je gleichem Umfang. Um diesen wird ein Band aus Pergament oder Leder gewickelt und die geheime Botschaft in Längsrichtung des Stabes geschrieben. Im abgewickelten Zustand zum Transport der Botschaft steht auf dem Band eine unsinnige Folge von Buchstaben. Der Empfänger kann die Botschaft entschlüsseln, indem er das Band auf seinem Stab mit dem gleichen Umfang wieder aufwickelt, Abb. 1-1.

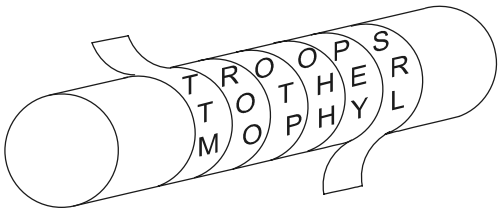

Abb. 1-1: Skytale, ca. 500 v.Chr. in Sparta.

Bei der Skytale handelt es sich um eine *Transpositions-Chiffre*. D.h. die Zeichen selbst sind unverändert, sie befinden sich nur in anderen Positionen. Formal kann man die Skytale durch eine Matrix beschreiben: Die Zahl der Zeilen entspricht dem Umfang und die Zahl der Spalten entspricht der Zahl von Umwindungen. Die Matrix wird im Klartext zeilenweise beschrieben und für die Übertragung als Folge der Spalten ausgelesen.

Eine Transpositions-Chiffre lässt sich verallgemeinern, indem in der genannten Matrix ihre Elemente zeilen- oder spaltenweise vertauscht werden. Diese Permutation der Matrixelemente ist dann der Schlüssel. Ein Angreifer kann bei einer Transpositions-Chiffre versuchen, aus dem Vorrat der (originalen) Zeichen der verschlüsselten Botschaft vermutete Wörter zu bilden und sie in eine sinnvolle Reihenfolge zu bringen. Er hat über seinen Erfolg jedoch keine Sicherheit. Ein Angriff kann beliebig erschwert werden, wenn die Matrix genügend groß gewählt wird. Bei einer Transpositions-Chiffre kann die Häufigkeitsverteilung der Zeichen nicht für einen Angriff genutzt werden, wie dies bei der Caesar-Chiffre der Fall ist, denn die Häufigkeit der Zeichen entspricht genau der des ursprünglichen Klartextes (und damit der der verwendeten Sprache), da nur die Reihenfolge des Zeichen vertauscht wurde.

1.1.2 Caesar-Chiffre

Die Caesar-Chiffre arbeitet zeichenweise, wobei jeder Buchstabe durch den drittnächsten Buchstaben im Alphabet ersetzt wird. Ein Klartext-Buchstabe „a“ wird beim Verschlüsseln durch einen Chiffretext-Buchstaben „D“ ersetzt, ein Klartext „b“ durch ein Chiffre-Text „E“ usw. In Tab. 1-1 steht unter jedem der 26 Klartext-Buchstaben der zugehörige Chiffretext-Buchstabe. In der unteren Zeile sind die Chiffretext-Buchstaben gegenüber der oberen Zeile um 3 Positionen zyklisch nach links verschoben, d.h. auf „Z“ folgen „A“, „B“ und „C“.

Tab. 1-1: Caesar-Chiffre
als Tabelle zum Verschlüsseln: ↓ in: Klartext, out: Chiffre-Text
Entschlüsseln: ↑ in: Chiffre-Text, out: Klartext

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
Chiffre-Text	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

Beim Entschlüsseln wird die Tabelle in umgekehrter Weise benutzt, d.h. ein Chiffretext-Buchstabe wird durch den darüber stehenden Klartext-Buchstaben ersetzt.

Beispiel:
```
this is a plaintext   (Klartext)
WKLV LV D SODLQWHAW   (Chiffre)
```

Für Klartext bzw. Chiffretext wird Klein- bzw. Großschreibung benutzt. Dies ist für die Verschlüsselung unerheblich und dient nur der leichten Unterscheidung.

Alternativ zu Tab. 1-1 kann die Caesar-Chiffre durch Chiffrier-Scheiben mechanisiert werden, Abb. 1-2. Die 26 Buchstaben stehen zyklisch in 26 Sektoren. Die zwei Scheiben für Input und Output sind um 3 Buchstabenpositionen gegeneinander verdreht und fixiert. Die zyklische Verschiebung ergibt sich bei dem Zyklus der Scheiben von selbst. Auf der Input-Scheibe sind außen zusätzlich Nummern den Buchstaben zugeordnet.

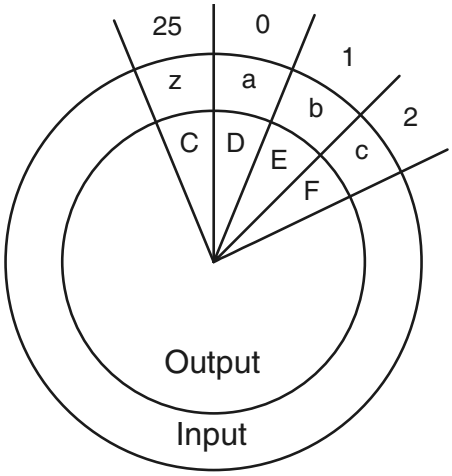

Abb. 1-2: Caesar-Chiffre, als Chiffrier-Scheibe

Die Caesar-Chiffre wird entsprechend der Verschiebung der Scheiben als *Verschiebe-Chiffre* (displacement cipher) sowie als *monoalphabetische Substitutions-Chiffre* bezeichnet: Es wird ein Klartext-Buchstabe durch einen Chiffretext-Buchstaben ersetzt bzw. „substituiert". Dabei wird eine einzige Alphabet-Zuordnungsliste benutzt („monoalphabetisch").

1.1.2.1 Verallgemeinerung der Caesar-Chiffre

Die Caesar-Chiffre kann verallgemeinert werden, indem statt einer fest eingebauten Verschiebung um 3 Buchstaben jeder Wert aus [0, 25] als Verschiebe-Schlüssel k gewählt wird. Caesar soll k=3 gewählt haben, weil C (Caesar) der 3. Buchstabe ist. Augustus soll k=1 gewählt haben, weil A (Augustus) der 1. Buchstabe ist. Zur formalen Beschreibung einer allgemeinen Verschiebung k ist es zweckmäßig, den Buchstaben eine Buchstaben-Nummer zuzuordnen:

Buchstaben-Zeichen B	a b c d e ... ... x y z
Buchstaben-Nummer BN	0 1 2 3 4 ... ... 23 24 25

BN_m Buchstabennummer im Klartext m (message)
BN_c Buchstabennummer im Chiffretext c
k Schlüssel, k=3 für die Caesar-Chiffre, allgemein: $k \in [0, 25]$

$$\left.\begin{aligned} \text{Verschlüsselung:} \quad & BN_c = (BN_m + k) \bmod 26 \\ \text{Entschlüsselung:} \quad & BN_m = (BN_c - k) \bmod 26 \end{aligned}\right\} \qquad (1.1\text{-}1)$$

Durch die Modulo-Bildung (mod 26) in (1.1-1) wird der ganzzahlige Rest bei Division durch 26 gebildet, oder alternativ, das Ergebnis durch „+26" oder „−26" in den Bereich [0, 25] gebracht. Anschaulich gesprochen sorgt die Modulo-Bildung für die zyklische Zuordnung, wie sie von der Chiffrier-Scheibe direkt realisiert wird.

(Beispiele: Verschlüsselung von „y“: „y“+“k“=24+3=27≡1=“B“ (mod 26); Entschlüsselung von „C“: „C“−“k“=2−3=−1≡25=“z“ (mod 26). Das Zeichen „≡“ wird als *Kongruenz* bezeichnet. Sie bedeutet eine Gleichheit in einem Zyklus mit n=26 Werten. Die Rechnung modulo n wird ausführlich in Kap. 2.1 dargestellt. Die Nummerierung der Buchstaben mit [0, 25] statt mit [1, 26]) vereinfacht die formale Darstellung in (1.1-1).

Die Caesar-Chiffre kann nochmals verallgemeinert werden, indem die Buchstabenpositionen der unteren Zeile in Tab. 1-1 beliebig permutiert werden. Bei 26 Buchstaben gibt es 26! mögliche Permutationen und damit 26! verschiedene Schlüssel. Diese Verallgemeinerung ist keine Verschiebe-Chiffre mehr, wohl aber eine monoalphabetische Substitutions-Chiffre. (Anm.: Das Symbol „!“ bedeutet „Fakultät“, 26!=1·2·3·…·25·26).

1.1.2.2 Kryptoanalyse der Caesar-Chiffre

Eine Verschiebe-Chiffre ist aus heutiger Sicht sehr einfach zu brechen. Sie hat ihren Dienst erfüllt, als zu Zeiten Caesars die meisten Menschen Analphabeten waren. Eine Verschiebe-Chiffre kann gebrochen werden, indem der Angreifer die 26 Möglichkeiten für den Schlüssel k durchprobiert, bis ein sinnvoller Klartext erscheint. Noch schneller geht es, wenn man von den unterschiedlichen Häufigkeiten der Buchstaben in einem natürlich sprachlichen Text Gebrauch macht. In der deutschen Sprache tritt der Buchstabe „e“ mit 17,4 % auf gegenüber einer mittleren Häufigkeit für alle Buchstaben von 1/26 = 3,8 %. (In der englischen Sprache hat „e“ die Häufigkeit von 12,7 %). Bei einer Verschiebe-Chiffre braucht ein Angreifer nur den häufigsten Buchstaben im Klartext ermitteln. Der Abstand zwischen dem Buchstaben „e“ und dem häufigsten Buchstaben im Chiffretext ergibt mit hoher Sicherheit den Schlüssel k.

Ein Beispiel für die Häufigkeit der Buchstaben, die für eine natürliche Sprache charakteristisch ist, findet sich in Abb. 1-3. Das Histogramm wurde gewonnen aus dem einführenden Text von Kap. 1, der mit dem Werkzeug CrypTool [CrypTool] analysiert wurde.

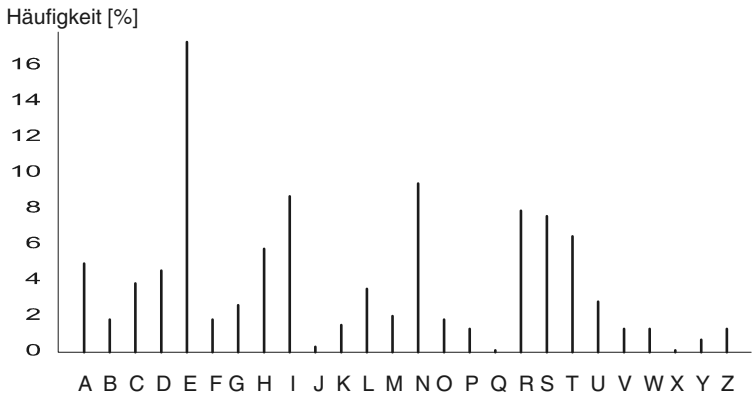

Abb. 1-3: Histogramm (Häufigkeitsverteilung) der Buchstaben eines Textes in deutscher Sprache.

Monoalphabetische Substitutions-Chiffren mit einer gegenüber Tab. 1-1 permutierten Zuordnungsliste sind durch Häufigkeitsanalyse ebenfalls leicht zu brechen: Im Chiffre-Text werden die häufigsten, die zweithäufigsten, die dritthäufigsten usw. Buchstaben festgestellt. Entsprechend der bekannten Häufigkeit in der verwendeten natürlichen Sprache können die Chiffre-Buchstaben durch Klartextbuchstaben probeweise ersetzt werden. Weitere Ersetzungen können durch den Kontext vermuteter Klartextwörter gefunden werden.

Die Verschlüsselung mit der Caesar-Chiffre und die Häufigkeitsanalyse können mit dem empfehlenswerten Werkzeug „CrypTool“ [CrypTool] demonstriert und nachvollzogen werden. Das Werkzeug umfasst eine große Vielfalt von kryptographischen Verfahren, die durch die Demonstration begreifbarer werden.

1.1.3 Vigenère-Chiffre

Blaise de Vigenère (1523-1596) war ein französischer Diplomat und Kryptograph. Basierend auf den Ideen, die er bei einem diplomatischen Aufenthalt in Rom kennen gelernt hatte, beschrieb er 1585 u.a. die nach ihm benannte Vigenère-Chiffre. Sie wurde erst 3 Jahrhunderte später von Charles Babbage (1854) und Friedrich Wilhelm Kasiski (1863) systematisch gebrochen.

Die Vigenère-Chiffre ist eine Verallgemeinerung der Caesar-Chiffre, wobei statt eines Schlüssels k eine Folge von Schlüsseln k: k_1, k_2, ... k_r periodisch benutzt wird. Bei einer Periode von z.B. r=5 lautet die Schlüsselfolge k: $k_1\ k_2\ k_3\ k_4\ k_5 \mid k_1\ k_2\ k_3\ k_4\ k_5 \mid k_1\ k_2\ k_3\ k_4\ k_5 \mid ... \mid ...$ Der 1. Buchstabe des Klartextes wird mit k_1, der zweite Buchstabe mit k_2 usw. verschlüsselt. Bei der Periode r=5 wird der 6. Buchstabe wieder mit k_1 verschlüsselt, der 7. Buchstabe mit k_2 usw. Die Verschlüsselung der einzelnen Buchstaben ist wie bei der Caesar-Chiffre: Es können die Chiffrier-Scheibe von Abb. 1-2 mit variablen Verdrehungen k_i oder die Formel (1.1-1) verwendet werden.

Die Vigenère-Chiffre ist, wie die Caesar-Chiffre, eine Verschiebe-Chiffre (displacement cipher), denn Klartextbuchstabe und Chiffretextbuchstabe sind um k_i Buchstaben im Alphabet zyklisch verschoben. Darüber hinaus ist die Vigenère-Chiffre eine *polyalphabetische Substitution*, denn es gibt, entsprechend den Werten der Schlüssel k_i, 26 verschiedene Alphabet-Zuordnungslisten.

1.1.3.1 Hilfsmittel zur Vigenère-Chiffre

Neben der Chiffrier-Scheibe und der Formel (1.1-1) ist als Hilfsmittel für die Verschlüsselung und Entschlüsselung das sog. Vigenère-Quadrat bekannt. Es ist eine Verallgemeinerung der Tab. 1-1 für die Caesar-Chiffre, wobei statt der 2. Zeile in Tab. 1-1 hier in Tab. 1-2 alle 26 Möglichkeiten der Verschiebungen aufgelistet sind. In dem Vigenère-Quadrat von Tab. 1-2 enthält die linke Spalte die Schlüssel, die oberste Zeile die Klartextbuchstaben und der Kreuzungspunkt den Chiffretextbuchstaben. Beispiel: Schlüssel k_i=13=n, Klartextbuchstabe B_m=“e“, Chiffretextbuchstabe B_c=“R“.

Tab. 1-2: Vigenère-Quadrat,
Links: der Schlüssel k_i, oben: der Klartexbuchstabe, im Kreuzungspunkt: der Chiffretextbuchstabe.
Der Chiffretext ist durch Großbuchstaben dargestellt.

	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	← Klartext
0=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	
1=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	
2=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	
3=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	
4=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	
5=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	
6=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	
7=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	
8=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	
9=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	
10=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	
11=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	
12=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	
13=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	
14=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	
15=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	
16=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	
17=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	
18=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	
19=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	
20=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	
21=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	
22=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	
23=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	
24=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	
25=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	

↑ Schlüssel k_i

Die Verschlüsselung und Entschlüsselung durch polyalphabetische Substitution ist in Abb. 1-4 als Blockschaltbild dargestellt. Auf den Klartext (hier „this is...“) wird eine Folge von Schlüsseln (hier „cxfk go...“) angewendet. Der verschlüsselte Text (hier „VENC OG...“) wird auf der Empfängerseite mit der gleichen Schlüsselfolge („cxfk go...“) wieder korrekt entschlüsselt. Das Blockschaltbild ist im Prinzip nur eine bildliche Darstellung der Formel (1.1-1), wobei als Schlüssel k eine Folge k: k_1 k_2 k_3 k_4... von Schlüsseln benutzt wird. Für die Verschlüsselung und Entschlüsselung in Abb. 1-4 muss die Schlüsselfolge nicht nur gleich, sondern auch synchron zu Klar- und Chiffretext sein.

In dem Beispiel von Abb. 1-4 sind in dem Chiffretext die Leerzeichen zwischen den Wörtern zu erkennen. Man kann dies vermeiden, indem entweder die Leerzeichen weggelassen werden oder indem man das Leerzeichen als 27. Buchstaben auffasst und die Operationen modulo 27 durchführt.

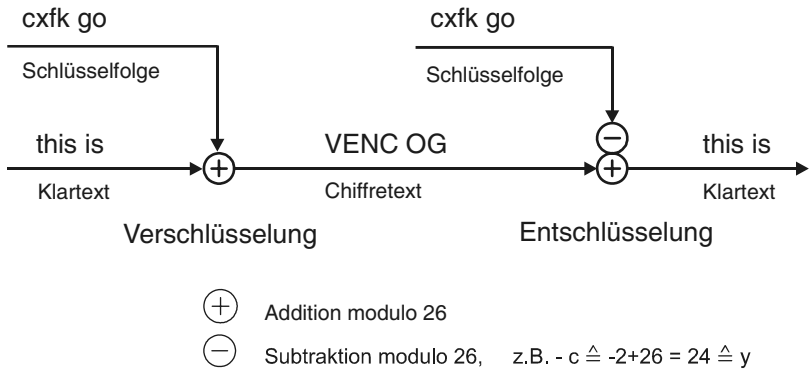

Abb. 1-4: Polyalphabetische Substitution, Erweiterung der Vigenère-Chiffre, Blockschaltbild für Verschlüsselung und Entschlüsselung mit einer Folge von Schlüsseln k: k_1 k_2 k_3 k_4 ...

1.1.3.2 Angriff auf die Vigenère-Chiffre

Für einen Angriff auf die Vigenère-Chiffre sind die von der Caesar-Chiffre bekannten Methoden nicht direkt anwendbar. Bei einem Durchprobieren aller Schlüssel sind bei der Vigenère-Chiffre nicht nur die 26 Möglichkeiten von k_1, sondern 26^r Möglichkeiten für eine Schlüsselperiode zu prüfen. Wenn die Schlüsselperiode r genügend groß gewählt wurde, ist diese Aufgabe praktisch nicht durchführbar.

Auch ist eine Häufigkeitsanalyse der Buchstaben im Chiffretext nicht direkt anwendbar. Denn bei den unterschiedlichen Teilschlüsseln k_i (i=1...r) der Schlüsselfolge k: k_1 k_2 k_3 k_4...k_r vermischen sich die charakteristischen Häufigkeiten im Chiffretext und ein Rückschluss auf einen bestimmten Teilschlüssel k_i ist nicht möglich.

Ein erfolgreicher Angriff kann gefahren werden, wenn die Schlüsselperiode r bekannt ist. Für die Buchstabenpositionen i-j·r (i=1...r, j=0, 1, 2, ...), d.h. die Positionen, die zueinander den Abstand der Schlüsselperiode r haben, wurde für die Verschlüsselung jeweils der gleiche Teilschlüssel k_i verwendet. Mit einer Häufigkeitsanalyse der Positionen i-j·r (j=0, 1, 2, ...) kann der Teilschlüssel k_i ermittelt werden. Bei einer Schlüsselperiode r sind also r getrennte Häufigkeitsanalysen durchzuführen. Der für den Angriff verfügbare Chiffretext muss genügend lang sein (lang im Vergleich zur Schlüsselperiode), um eine signifikante Statistik zu ermöglichen.

Für eine Ermittlung der Schlüsselperiode r gibt es unterschiedliche Möglichkeiten:

(1.) Man versucht es mit einer Schlüssellänge $r_{Versuch}$ und führt Häufigkeitsanalysen im Chiffretext für die Buchstabenpositionen i-j·$r_{Versuch}$ (j=0, 1, 2, ...) durch, d.h. für alle Buchstabenpositionen, die den Abstand $r_{Versuch}$ zueinander haben. Falls $r_{Versuch}$=r war, dann zeigt die Häufigkeitsverteilung der Buchstaben die charakteristischen Unterschiede in den Häufigkeitswerten, und die Analyse war erfolgreich.

(2.) Wenn der Klartext zufällig gleiche Wörter im Abstand r oder einem Vielfachen der Schlüsselperiode r enthält, dann werden diese mit der gleichen Teilschlüsselfolge verschlüsselt und

ergeben gleiche Muster von aufeinander folgenden Buchstaben im Chiffretext. Man sucht deshalb im Chiffretext nach gleichen Mustern von 2, 3 oder 4 aufeinander folgenden Buchstaben. Mit Wahrscheinlichkeit sind die Abstände zwischen diesen Mustern gleich der Schlüsselperiode r oder einem Vielfachen von ihr. Die Schlüsselperiode r ergibt sich mit Wahrscheinlichkeit aus den Primfaktoren, die in allen Abständen auftreten. Dieser Test wurde von Kasiski 1863 veröffentlicht (Friedrich Wilhelm Kasiski, 1805-1881).

(3.) Ein weiterer Test wurde 1925 von Friedman entwickelt (William Frederick Friedman, 1891-1969, Kryptologe der US Army). Der Test beruht auf der Eigenschaft, dass in einer natürlichen Sprache gleiche Buchstaben mit einer charakteristischen Häufigkeit sich wiederholen. Das wiederholte Auftreten gleicher Buchstaben wird als *Koinzidenz* bezeichnet. Eine Koinzidenz gleicher Buchstaben bleibt im Vigenére-Chiffretext erhalten, wenn der Abstand der Koinzidenz die Schlüsselperiode trifft. In dem Friedman-Test wird aus dem Chiffretext ein so genannter Koinzidenzindex ermittelt, aus dem die Schlüsselperiode r näherungsweise berechnet wird. Eine weiterführende Darstellung findet sich in [B97] oder [BNS05].

Die drei beschriebenen Methoden, die Periode zu ermitteln, werden zweckmäßigerweise kombiniert. Der Kasiski-Test (2.) liefert mit etwas Glück (wenn man sich wiederholende Buchstabenmuster findet) Primfaktoren der Schlüsselperiode, der Friedman-Test (3.) kann mit seinem Näherungswert eine Auswahl treffen und die Häufigkeitsanalyse (1.) gibt schließlich Sicherheit über die Schlüsselperiode und die Möglichkeit, die Teilschlüssel k_1, k_2, ... k_r zu ermitteln.

1.1.3.3 Ausblick

Die Vigenère-Chiffre kann verallgemeinert werden, indem die Schlüssellänge r ebenso lang gewählt wird wie der gesamte Klartext. Damit wiederholt sich die Schlüsselfolge k: k_1, k_2, ... k_r nicht. Wenn außerdem die Teilschlüssel der Folge zufallsmäßig und gleich verteilt ausgewählt werden, dann wird sogar perfekte Sicherheit erreicht. Diese Eigenschaft wird später noch in Kap. 1.4 diskutiert.

1.1.4 Vernam-Chiffre

Gilbert S. Vernam (1890-1960) arbeitete als Ingenieur bei AT&T (Bell Labs) und erfand 1917 die nach ihm benannte Chiffre. Sie kann als Spezialisierung / Erweiterung der Vigenère-Chiffre angesehen werden: Die Spezialisierung betrifft das Alphabet, das nicht mehr mit 26 Buchstaben, sondern mit nur 2 Buchstaben {0, 1} arbeitet. Aus heutiger Sicht ist uns die binäre Arbeitsweise vertraut. Vernam kannte sie aus der Telegraphentechnik. Die Erweiterung betrifft die Schlüsselfolge, die ebenso lang ist wie die Nachricht und nur ein einziges Mal verwendet werden darf (one-time pad). Die Verwandtschaft der Vernam-Chiffre mit der Vigenère-Chiffre ist auch in dem Blockschaltbild Abb. 1-5 im Vergleich zu Abb. 1-4 zu sehen. Die polyalphabetische Substitution der Vernam-Chiffre wird auch als *Strom-Chiffre* bezeichnet (siehe dazu auch Kap. 2.4).

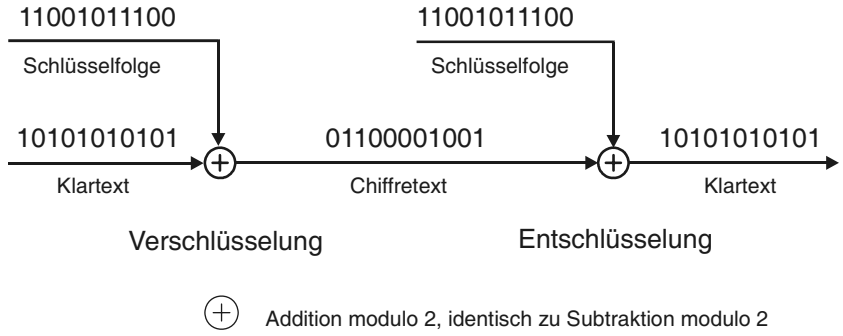

Abb. 1-5: Vernam-Chiffre, Blockschaltbild. Die Folge der Schlüssel ist zufallsmäßig gewählt, sie ist bei Sender und Empfänger gleich, und sie wird nur ein einziges Mal benutzt (one-time pad). Die Vernam-Chiffre liefert *perfekte Sicherheit*.

Statt modulo 26 wird hier die Addition und Subtraktion, den 2 Buchstaben {0, 1} entsprechend, molulo 2 ausgeführt. Die Addition mod 2 ist identisch der bitweisen XOR-Verknüpfung. Addition und Subtraktion modulo 2 sind identisch und müssen nicht unterschieden werden.

$\oplus$: Addition modulo 2:

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

Die Schlüsselfolge wird zufallsmäßig und gleich verteilt gewählt, d.h. jede Binärstelle der Schlüsselfolge wird gewürfelt. Die Werte „0“ und „1“ sollen die gleiche Wahrscheinlichkeit von 1/2 haben. Dieses Würfeln entspricht dem Werfen einer Münze. Die Schlüsselfolge muss als Geheimnis vor ihrer Benutzung auf einem vertraulichen Wege zu Sender und Empfänger übertragen werden. Auf dem vertraulichen Wege könnte man statt der Schlüsselfolge natürlich gleich die Nachricht selbst übertragen. Die Schlüsselfolge kann jedoch vorher bei einer günstigen Gelegenheit übergeben werden, z.B. durch Austausch eines Lochstreifens bei einem Treffen von Geheim-Agenten.

Die Vernam-Chiffre liefert *perfekte Sicherheit*: Ein Wert „1“ im Chiffretext kann entstanden sein durch eine „0“ im Klartext und eine „1“ in der Schlüsselfolge oder durch eine „1“ im Klartext und eine „0“ in der Schlüsselfolge. In der Schlüsselfolge haben die Werte „1“ und „0“ die gleiche Wahrscheinlichkeit, und somit haben im Klartext die Werte „0“ und „1“ für einen Angreifer die gleiche Wahrscheinlichkeit. Für den Angreifer sind die Annahmen „0 im Klartext“„ und „1 im Klartext“ gleich wahrscheinlich. Er hat damit keinerlei Information. Für einen Wert „0“ im Chiffretext gilt Entsprechendes.

Die Schlüsselfolge darf nur ein einziges Mal verwendet werden. Andernfalls könnte ein Angreifer Schlüsselfolgen ausprobieren. Wenn sich für verschiedene Chiffretexte, die mit der gleichen Schlüsselfolge erzeugt wurden, jeweils sinnvolle Texte ergeben, dann war die angenommene Schlüsselfolge offenbar die richtige. Weiteres zum Thema der perfekten Sicherheit findet sich in Kap. 1.4.