Albrecht Beutelspacher
Heike B. Neumann
Thomas Schwarzpaul

Kryptografie in Theorie und Praxis

Aus dem Programm
Mathematik/Kryptografie

Diskrete Mathematik
von M. Aigner

Diskrete Mathematik für Einsteiger
von A. Beutelspacher und M.-A. Zschiegner

Lineare Algebra
von A. Beutelspacher

Lineare Algebra Interaktiv (CD-ROM)
von A. Beutelspacher und M.-A. Zschiegner

Kryptologie
von A. Beutelspacher

Moderne Verfahren der Kryptographie
von A. Beutelspacher, J. Schwenk und K.-D. Wolfenstetter

Verschlüsselungsalgorithmen
von G. Brands

Algebraische Grundlagen der Informatik
von K.-U. Witt

Mathematik für Informatiker
von P. Hartmann

vieweg

Albrecht Beutelspacher
Heike B. Neumann
Thomas Schwarzpaul

Kryptografie in Theorie und Praxis

Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk

vieweg

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

Prof. Dr. Albrecht Beutelspacher
Thomas Schwarzpaul
Universität Gießen
Mathematisches Institut
Arndtstraße 2
35392 Gießen

E-Mail: albrecht.beutelspacher@math.uni-giessen.de
thomas.schwarzpaul@math.uni-giessen.de

Dr. Heike B. Neumann
Mühlendamm 45 a
22087 Hamburg

E-Mail: heike.neumann@philips.com

1. Auflage Januar 2005

Alle Rechte vorbehalten
© Friedr. Vieweg & Sohn Verlag/GWV Fachverlage GmbH, Wiesbaden 2005

Lektorat: Ulrike Schmickler-Hirzebruch / Petra Rußkamp

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

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Umschlaggestaltung: Ulrike Weigel, www.CorporateDesignGroup.de

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

ISBN 978-3-528-03168-8 ISBN 978-3-322-93902-9 (eBook)
DOI 10.1007/978-3-322-93902-9

Vorwort

Kryptografie ist eine alte Kunst und eine moderne Wissenschaft. Die Anfänge der Kunst, geheime Nachrichten zu erzeugen, verlieren sich im Dunkel der Geschichte. Schon 500 v. Chr. haben die Spartaner die Skytala benutzt, und vor 2000 Jahren hat Julius Cäsar im Gallischen Krieg schon die Cäsar-Chiffre eingesetzt. Die Skytala war ein Zylinder, um den ein Band gewickelt wurde, auf den der Klartext längs geschrieben wurde; das Band konnte ohne Gefahr übermittelt werden, und nur ein Empfänger mit einem Zylinder richtiger Größe konnte den Text entziffern. Bei der Cäsar-Chiffre benutzt man das normale Alphabet, unter dem ein um einige Stellen verschobenes Alphabet steht. Verschlüsselt wird, indem ein Buchstabe des Klartextalphabets durch den darunter stehenden Buchstaben des Geheimtextalphabets ersetzt wird. Die Bedeutung der Skytala und der Cäsar-Chiffre liegen u.a. darin, dass sie die Prototypen einer Transpositions- bzw. einer Substitutions-Chiffre sind. Bis vor wenigen Jahrzehnten war ernsthafte Kryptografie eine Domäne der Politiker, Diplomaten und Militärs und der entsprechenden Institutionen. Das Ziel war stets, Verfahren zu entwickeln und zu verwenden, die vom Gegner nicht gebrochen werden konnten bzw. die Verfahren der Gegner zu brechen. Die Tatsache, dass heute die Kryptografie eine nie zuvor gekannte Bedeutung hat, liegt entscheidend an der Entwicklung des Computers und der Computernetze, insbesondere des Internets. Die ersten Computer wurden gegen Ende des 2. Weltkriegs entwickelt, um Geheimcodes brechen zu können, und zwar ging es um die effiziente Verarbeitung der abgefangenen Geheimtexte. Viel später, in den 70er Jahren des vergangenen Jahrhunderts wurden Rechner eingesetzt, um komplexe Verschlüsselungsverfahren realisieren zu können. Der übergang von den mechanischen und elektromechanischen Verschlüsselungsgeräten (wie zum Beispiel ENIGMA) zu den in Soft- und Hardware ausführbaren Codes, wie etwa dem DES, stellt einen enormen Sprung in der Qualität der Kryptosysteme dar. Das Internet und andere Netze, wie etwa das Mobilfunknetz, haben diese Tendenzen noch einmal verstärkt. Zunächst sind die Angriffsmöglichkeiten durch die Möglichkeit der effizienten Zusammenarbeit von sehr vielen Rechnern enorm gestiegen. In der Tat wurden zum Beispiel einige Faktorisierungsversuche erst durch einen massiven Verbund von Rechnern im Internet möglich. Andererseits hat das Internet die Entwicklung von Algorithmen und v.a. Protokollen notwendig gemacht. Denn zunächst waren in den Internetprotokollen keinerlei Sicherheitsmechanismen vorgesehen, aber es ist klar, dass man für Anwendungen wie Abruf sensibler Daten (z.B. Passwörter, medizinischer Daten oder Konstruktionsunterlagen) oder Bezahlvorgänge Sicherheit mit sehr guter Qualität braucht. Spätestens bei solchen Anwendungen wird auch klar, dass zu dem Ziel der Geheimhaltung ein weiteres Hauptziel der Kryptografie hinzukommt, nämlich die Authentifikation, d.h. die Echtheit von Daten.

Spätestens seit den Arbeiten von Claude Shannon, mit denen er Ende des

2. Weltkriegs die Kryptografie neu begründet hat, ist diese eine mathematische Wissenschaft geworden. Natürlich gehört zu einer Realisierung einer kryptografischen Anwendung die Arbeit der Informatiker, Ingenieure usw., aber ohne die mathematische Fundierung bei der Konstruktion und Analyse von Sicherheitsverfahren stünden alle auf tönernen Füßen. Die 70er und 80er Jahre des 20.Jahrhunderts waren gekennzeichnet durch die Entdeckung und Entwicklung vieler neuer Verfahren, die die Kryptografie revolutioniert haben: Neben dem schon erwähnten DES ist dies v.a. die Entdeckung der Public-Key-Kryptografie mit den zugehörigen Algorithmen RSA und ElGamal, sowie der Zero-Knowledge-Verfahren. Heute befinden wir uns in einer Konsolidierungsphase, die gekennzeichnet ist durch systematische Aufbereitung, Klärung der Begriffsstruktur und weitgehende mathematische Durchdringung der Verfahren. Damit werden zum ersten Mal Lehrbücher der Kryptografie möglich. Die Bücher der letzten Jahrzehnte waren Forschungsberichte, stellten einzelne Teilgebiete vor oder dienten schlicht dazu, dieses Gebiet bekannt zu machen.

Dieses Buch ist ein Lehrbuch der Kryptografie, das auf vielen Vorlesungen der Autoren an der Universität Gießen beruht. Wir haben versucht, alle wesentlichen Aspekte der Kryptografie darzustellen. Dabei haben wir uns um eine Balance bemüht, die allen Aspekten der Kryptpgrafie gerecht wird: Symmetrische und asymmetrische (public key) Kryptografie werden beide ausführlich dargestellt. Innerhalb der Gebiete werden Algorithmen ihrer Bedeutung gemäß dargestellt. Schließlich behandeln wir nicht nur Algorithmen, sondern auch Protokolle. Im Einzelnen geht es dabei um folgende Themen:

Kapitel 1 ist eine kurze Einführung in die Kryptografie und stellt die wichtigsten Begriffe, die in den folgenden Kapiteln benötigt werden, vor. Das Buch gliedert sich dann in drei Teile, wobei im ersten Teil, den Kapiteln 2 bis 8, die symmetrischen Verfahren behandelt werden. In Kapitel 2 werden historische Verfahren, wie die bereits erwähnte Cäsar-Chiffre und Vigenère-Chiffre dargestellt. Die grundlegenden Begriffe der symmetrischen Kryptografie werden in den Kapiteln 3 bis 5 dargestellt. Im Vordergrund stehen dabei das formale Modell zur Beschreibung kryptografischer Verfahren von Shannon und die Begriffe perfekte Sicherheit und effiziente Sicherheit. Kapitel 6 und 7 zeigen, wie man praktische symmetrische Verfahren konstruiert. In Kapitel 6 werden die Stromchiffren, Verfahren die etwa im Mobilfunk eingesetzt werden, vorgestellt. Ein weiterer Schwerpunkt dieses Kapitels ist die Analyse linearer Schieberegister, die man zur Konstruktion von Stromchiffren verwenden kann. Kapitel 7 behandelt die zweite Klasse symmetrischer Verfahren, die Blockchiffren. Es werden die beiden prominentesten Vertreter, der DES und sein Nachfolger der AES, ausführlich dargestellt. Abgeschlossen wird das Gebiet der symmetrischen Verfahren durch Kapitel 8, in dem die wichtigsten Betriebsmodi vorgestellt werden. Betriebsmodi beschreiben, wie man eine Blockchiffre auf lange Nachrichten anwendet.

Der zweite Teil des Buches gilt den Publi-Key-Verfahren. Kapitel 9 gibt eine kurze Einführung in die Public-Key-Kryptografie, so wie einen Vergleich mit den symmetrischen Verfahren. Kapitel 10 und 11 beschäftigen sich mit den beiden

wichtigsten Public-Key-Verfahren, dem RSA-Algorithmus bzw. dem ElGamal-Verschlüsselungsverfahren. Im zwölften Kapitel werden weitere Public-Key-Verfahren, wie das Rabin-Verschlüsselungsverfahren vorgestellt. Um die Sicherheit von Public-Key-Verschlüsselungsverfahren formal beschreiben zu können, werden in Kapitel 13 die Begriffe polynomielle Ununterscheidbarkeit und semantische Sicherheit eingeführt. Die Sicherheit der RSA- und der ElGamal-Signatur wird in Kapitel 14 diskutiert.

Der dritte Teil des Buches beschäftigt sich mit kryptografischen Anwendungen. Kapitel 15 behandelt die Konstruktion von Hashfunktionen und das Problem der Nachrichtenauthentizität. Kapitel 16 ist von besonderer Bedeutung, da dort die Zero-Knowledge-Protokolle behandelt werden, die einen wichtigen Baustein für komplexere kryptografische Protokolle bilden. Die Schlüsselverwaltung ist das zentrale Thema des siebzehnten Kapitels, dem sich ein Kapitel über Teilnehmerauthentifikation anschließt. In Kapitel 19 werden die wichtigsten Schlüsseletablierungsprotokolle dargestellt und im zwanzigsten Kapitels geht es um Protokolle, an deren Durchführung mehr als zwei Parteien beteiligt sein können. Beispielsweise um ein Geheimnis aufzuteilen. Kapitel 21 geht der Frage nach, wie man Anonymität in kryptografischen Anwendungen erreichen kann. Zwei der wichtigsten Anwendungen, das elektronische Geld und die elektronischen Wahlen, werden hier dargestellt. Internetsicherheit ist das Thema von Kapitel 22. Hier werden das Secure Sockets Layer Protokoll und Pretty Good Privacy vorgestellt. Im abschließenden letzten Kapitel findet sich eine Einführung in das Gebiet der Quantenkryptografie und des Quantencomputing.

Das Buch ist ein Buch, das sich zum Selbststudium, aber auch zum Gebrauch neben Vorlesungen eignet. Obwohl die Kryptografie eine mathematische Disziplin ist, benötigt man nur relativ wenige explizite mathematische Vorkenntnisse. Man braucht ein bisschen Algebra und Zahlentheorie (vor allem bei den Public-Key-Algorithmen) und in manchen Kapiteln Grundkenntnisse der Stochastik. Die meisten benötigten Begriffe und Ergebnisse werden in diesem Buch noch einmal erarbeitet, aber natürlich setzen wir eine gewisse Routine bei der mathematischen Argumentation voraus. Die Übungsaufgaben dienen zur Vertiefung des Stoffes.

Gießen, im November 2004

Albrecht Beutelspacher
Heike Neumann
Thomas Schwarzpaul

Inhaltsverzeichnis