Albrecht Beutelspacher
Jörg Schwenk
Klaus-Dieter Wolfenstetter

Moderne Verfahren der Kryptographie

Aus dem Programm
Mathematik

Diskrete Mathematik
von M. Aigner

Diskrete Mathematik für Einsteiger
von A. Beutelspacher

Lineare Algebra
von A. Beutelspacher

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

Projektive Geometrie
von A. Beutelspacher und U. Rosenbaum

Kryptologie
von A. Beutelspacher

Algorithmische Zahlentheorie
von O. Forster

Algebraische Algorithmen
von A. Pethö

Codierungstheorie
von R.-H. Schulz

Algebraische Grundlagen der Informatik
Zahlen – Strukturen – Codierung – Verschlüsselung
von Kurt-Ulrich Witt

vieweg

Albrecht Beutelspacher
Jörg Schwenk
Klaus-Dieter Wolfenstetter

Moderne Verfahren der Kryptographie

Von RSA zu Zero-Knowledge

4., verbesserte Auflage

Die Deutsche Bibliothek – CIP-Einheitsaufnahme
Ein Titeldatensatz für diese Publikation ist bei
Der Deutschen Bibliothek erhältlich.

Prof. Dr. *Albrecht Beutelspacher*
Justus-Liebig-Universität Gießen
Mathematisches Institut, Arndtstraße 2
D-35392 Gießen
E-Mail: albrecht.beutelspacher@math.uni-giessen.de

Prof. Dr. *Jörg Schwenk*
Fachbereich Informatik
Georg-Simon-Ohm-Fachhochschule Nürnberg
Keßlerplatz 12
D-90489 Nürnberg

Klaus-Dieter Wolfenstetter
Technologiezentrum in der T-Nova/T-Systems
Am Kavalleriesand 3
D-64295 Darmstadt
E-Mail: klaus-dieter.wolfenstetter@t-systems.de

1. Auflage 1995
2., verbesserte Auflage 1998
3., verbesserte Auflage 1999
4., verbesserte Auflage Juni 2001

Der Verlag Vieweg ist ein Unternehmen der Fachverlagsgruppe BertelsmannSpringer.
www.vieweg.de
vieweg@bertelsmann.de

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Konzeption und Layout des Umschlags: Ulrike Weigel, www.CorporateDesignGroup.de

ISBN 978-3-528-36590-5 ISBN 978-3-322-96961-3 (eBook)
DOI 10.1007/978-3-322-96961-3

Vorwort

Es gibt zwei Welten der Kryptographie.
Der *einen* Welt scheint, von außen betrachtet, ein Hauch von Abenteuer und Romantik anzuhaften. Man denkt an Sherlock Holmes und James Bond, sieht Massen von Menschen mit Codebüchern operieren und lange Buchstabenkolonnen statistisch untersuchen; es ist die Welt der ENIGMA und anderer Chiffriermaschinen, bei deren Anblick das Herz jedes Antiquitätensammlers höher schlägt. Dies ist die Welt der „klassischen" Kryptographie.
Demgegenüber ist die *andere* Welt, die der modernen Kryptographie, bestimmt durch Stichworte wie e-Commerce, Public Key-Infrastuktur, digitale Signatur oder Chipkarte. Die Menschen, die man hier trifft, sind Medienexperten, Banker, Mathematiker und Informatiker.
Dieses Buch handelt von der modernen Kryptographie.

Die Unterscheidung in zwei Welten ist nicht nur äußerlich, sondern auch entscheidend durch die innere Entwicklung der Kryptologie geprägt. Für die moderne Kryptographie sind die Jahreszahlen 1976 und 1985 wichtig.
Im Jahre 1976 veröffentlichten Whitfield Diffie und Martin Hellman das Prinzip der Public-Key-Kryptographie. Mit ihrer bahnbrechenden Arbeit (und dem zwei Jahre später veröffentlichten RSA-Algorithmus) wurde ein jahrtausendealtes „unlösbares" Problem denkbar elegant gelöst: Während in der Welt der alten Kryptologie je zwei Teilnehmer, die geheim miteinander kommunizieren wollten, schon *vorher* ein gemeinsames Geheimnis haben mußten (ihren „geheimen Schlüssel"), ist dies in der Public-Key-Kryptographie nicht mehr der Fall: Jeder, auch jemand, der mit mir noch nie Kontakt hatte, kann mir eine verschlüsselte Nachricht schicken, die nur ich entschlüsseln kann.
Das zweite wichtige Datum ist die Entdeckung der Zero-Knowledge-Protokolle durch Shafi Goldwasser, Silvio Micali und Charles Rackoff im Jahre 1985 (und die sich daran anschließende Veröffentlichung des Fiat-Shamir-Algorithmus). Diese Protokolle lösen ein noch paradoxer erscheinendes Problem: Ich kann jedermann von der Existenz eines Geheimnisses überzeugen, ohne ihm das Geringste zu verraten. Anders gesagt: Ein Zero-Knowledge-Protokoll ist eine Unterhaltung, an deren Ende mein Gegenüber davon überzeugt ist, daß ich ein Geheimnis kenne, sonst aber nichts erfahren hat; insbesondere weiß er nichts, aber auch gar nichts über das Geheimnis.
Zero-Knowledge-Verfahren benutzen Basistechniken der Public-Key-Kryptographie; zum Beispiel ist die verwendete Mathematik die gleiche. Entscheidend kommt aber jetzt der Protokollaspekt hinzu: In einem Zero-Knowledge-Protokoll müssen die Partner nicht nur etwas berechnen, sondern sie müssen sich gemäß genau festgelegter, ausge-

klügelter Regeln unterhalten. Das Ziel wird nur durch diese Kombination erreicht: Die Mechanismen der Public-Key-Kryptographie sind die Bausteine, die Protokolle sind die Bauregeln für komplexe Verfahren.
Kurz gesagt: Moderne Kryptologie ist „Public-Key, Zero-Knowledge und die Folgen". Davon handelt dieses Buch.

Unser Ziel ist es, entscheidende Entwicklungen der letzten Jahre konzentriert und verständlich darzustellen. Im einzelnen geht es um folgende Themen:
Kapitel 1 und 2 können als schnelle Einführung in die Kryptologie betrachtet werden. Die dort vorgestellten Begriffe und Ergebnisse sind für das ganze Buch wichtig.
Im dritten Kapitel werden die grundlegenden („klassischen") Protokolle der modernen Kryptographie dargestellt: Challenge-and-Response, Diffie-Hellman-Schlüsselvereinbarung und blinde Signaturen.
Kapitel 4 ist zentral, denn dort werden nicht nur die berühmten Zero-Knowledge-Protokolle vorgestellt, sondern auch die darauf aufbauenden Entwicklungen der letzten Jahre, wie etwa Witness-Hiding und nichtinteraktive Zero-Knowledge-Protokolle, präsentiert.
Im fünften Kapitel geht es um Verfahren, wie zwei oder mehr Parteien etwas gemeinsam berechnen können, und zwar so, daß dabei niemand betrügen kann. Zum Beispiel wird das Problem, mit verschlüsselten Daten zu rechnen, gelöst. Besonders spektakulär ist die Frage, ob es bei elektronischer Kommunikation auch möglich ist, Skat zu spielen, das bedeutet die Karten so zu verteilen, daß sich anschließend niemand beschweren kann.
Das sechste Kapitel behandelt Fragen der Anonymität. Kann man über Computer anonym kommunizieren oder ist der Computer notwendigerweise der „Big Brother", der alles beobachtet?
Schließlich werden in Kapitel 7 noch einige wichtige Fragen studiert, nämlich Schlüsselmanagement und „oblivious transfer". Nicht zuletzt findet sich hier auch eine Einführung in das faszinierende Gebiet der Quantenkryptographie.
Im letzten Kapitel wird die benötigte Mathematik zusammengestellt und Bezeichnungsweisen festgelegt; in diesem Kapitel können Sie auch eventuell unklare mathematische Begriffe nachlesen.

Wie ist das Buch geschrieben?
Obwohl wir versuchen, den wissenschaftlichen Fortschritt der letzten Jahre vorzustellen, ist das Buch leicht und weitgehend ohne spezielle Voraussetzungen lesbar. Dazu dienen vor allem drei Mittel.

- Zunächst werden alle benötigten Ergebnisse über Mathematik und Kryptologie innerhalb des Buches bereitgestellt.
- Des weiteren haben wir einen modularen Aufbau gewählt. Das bedeutet, daß die einzelnen Kapitel weitgehend unabhängig voneinander gelesen werden können. Es ist sogar möglich, einzelne Abschnitte herauszugreifen. Dadurch können Sie sich schnell über ein bestimmtes Stichwort informieren.

- Schließlich haben wir die Themen auf verschiedenen Ebenen dargestellt, die jeweils mit Gewinn gelesen werden können. Jedes Thema wird zunächst möglichst anschaulich erklärt. Dazu gehört in der Regel ein nichtmathematisches Beispiel und häufig ein Bild. Die zweite Ebene ist die mathematisch präzise Darstellung, wobei wir auch hierbei keinem übertrieben Formalismus frönen. Insbesondere formulieren wir die Ergebnisse nicht auf der sprachlichen Ebene der Turingmaschinen. Schließlich erfolgt in vielen Fällen eine Analyse, die Stärken und Schwächen des behandelten Protokolls aufzeigt.

Für wen ist dieses Buch?

Aus der obigen Beschreibung wird deutlich, daß sich das Buch für eine große Leserschaft mit unterschiedlichen Ansprüchen, Zielen und Voraussetzungen eignet.

- Auf dem Weg in die Informationsgesellschaft sind vielfältige Sicherheitsprobleme zu lösen. In diesem Buch finden Techniker, Manager, Anwender und andere technisch und organisatorisch Verantwortliche aufbereitete Informationen über die wichtigsten Entwicklungen der letzten zehn Jahre.
- Für Studierende der Mathematik, Informatik und Elektrotechnik ist das Buch eine ideale Ergänzung zum Standardlehrstoff; es zeigt deutlich, daß zur Lösung praktischer Probleme Mathematik und theoretische Informatik mit Erfolg eingesetzt werden können.
- Schließlich wendet sich das Buch an all diejenigen, die sich über eine der faszinierendsten Entwicklungen der Mathematik und Informatik der letzten Jahre kundig machen wollen.

Einige Bemerkungen zum Text.

Sie werden relativ häufig englische Ausdrücke finden: Zero-Knowledge, oblivious transfer, challenge and response, ... Das liegt einfach daran, daß sich diese Ausdrücke eingebürgert haben, so daß sich jeder Versuch einer Übersetzung lächerlich anhört. Wir bitten alle Sprachpuristen um Nachsicht.

Um Nachsicht bitten wir auch in einer anderen Sache. Man kann sich stundenlang und erbittert streiten über mögliche Unterschiede der Begriffe „Kryptographie“ und „Kryptologie“ sowie „Authentikation“, „Authentifikation“, „Authentisierung“ usw. Wir machen diesen Streit nicht mit. In diesem Buch verwenden wir die Kr-Begriffe und die Au-Begriffe synonym. Dies wird nicht zu sachlichen Schwierigkeiten führen.

Protokolle sind geregelte Unterhaltungen zwischen Personen oder Instanzen. In vielen Fällen geht es um zwei Parteien, die sich manchmal vor einer gefährlichen dritten Partei schützen wollen. In der englischsprachigen Literatur werden die zwei oft mit Alice und Bob bezeichnet; dabei ist Alice diejenige, die etwas sendet und Bob ist der Empfänger. Auch bei uns treten diese Personen auf. Manchmal heißen sie nur A und B; aber auch dann ist A weiblich und B männlich. Die böse dritte Partei ist meist männlich, manchmal aber auch (Gnade!) weiblich.

Dieses Buch wäre ohne die tatkräftige Unterstützung zahlreicher Kolleginnen und Kollegen nicht, oder jedenfalls nicht so, zustande gekommen. Wir danken ganz besonders Klaus-Cl. Becker, Jörg Eisfeld, Klaus Huber, Annette Kersten, Ute Rosenbaum, Frank Schaefer-Lorinser, Alfred Scheerhorn, Beate Schwenk und Friedrich Tönsing für ihre aufmunternden, bösartigen, charmanten, detaillierten, emotionalen, fehlenden, globalen, hämischen, indiskutablen, jammervollen, kryptischen, langweiligen, mathematischen, nichtssagenden, offenen, positiven, quälenden, ratlosen, soliden, treffenden, unsachlichen, vernichtenden, witzigen und zynischen Bemerkungen.

Inhaltsverzeichnis