Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 56 (2001)

Rubrik: Bücher und Computersoftware

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 11.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Elem. Math. 56 (2001) 44 – 44
0013-6018/01/010044-1 $ 1.50+0.20/0

© Birkhäuser Verlag, Basel, 2001

Elemente der Mathematik

Bücher und Computersoftware

J. Buchmann: Einführung in die Kryptographie. xiv + 230 Seiten, sFr. 46.–. Springer, Berlin u.a. 1999; ISBN 3-540-66059-3.

Dieses Buch wendet sich in erster Linie an Mathematik- und Informatikstudenten. Es eignet sich aber für einen grösseren Kreis von Lesern, welche über mathematische Grundkenntnisse verfügen, da Grundlagen von Algebra, Zahlentheorie und Wahrscheinlichkeitsrechnung im Buch eingeführt werden, soweit sie für die behandelten kryptographischen Themen von Bedeutung sind.

Das Buch behandelt zuerst verschiedene Verschlüsselungsverfahren allgemein, bevor der Begriff der perfekten Sicherheit besprochen wird. Ein Kapitel ist dem DES als Beispiel eines Block Ciphers gewidmet. Da für Public-Key Systeme grosse zufällige Primzahlen benötigt werden, wird in einem weiteren Kapitel die Primzahlerzeugung besprochen. Ein grösseres Kapitel behandelt Public-Key Verschlüsselung, und insbesondere das RSA-Verfahren, den Diffie-Hellman-Schlüsselaustausch und das ElGamal-Verfahren.

Da die Sicherheit des RSA-Verfahrens auf der Schwierigkeit der Faktorisierung grosser Zahlen beruht, ist ein weiteres Kapitel der Faktorisierung gewidmet. Ebenso wird das diskrete Logarithmusproblem behandelt, da sowohl das Diffie-Hellman- als auch das ElGamal-Verfahren auf der Schwierigkeit dieses Problems basieren.

Eine wichtige Anwendung der Public-Key Kryptographie sind digitale Signaturen, welche in einem weiteren Kapitel behandelt werden. Um längere Meldungen zu signieren, werden kryptographische Hashfunktionen benötigt, welche ebenfalls besprochen werden. Hierauf wird das Problem der Identifikation kurz angesprochen und Zero-Knowledge-Beweise werden sehr kurz skizziert. Der bis hierhin behandelte Stoff gehört mittlerweile zum Standard einer Kryptographie-Vorlesung. Was hingegen auffällt, ist die knappe, aber trotzdem präzise Darstellungsweise, die manchen Leser ansprechen wird. Weiter schliesst das Buch mit einem lesenswerten Kapitel über Public-Key-Infrastrukturen, einem Thema, das in der Praxis an Bedeutung gewonnen hat.

Das Buch beinhaltet lohnenswerte Übungen samt Lösungen. Wer Lust hat, die C^{++}-Bibliothek LiDIA vom Internet herunterzuladen, kann versuchen, einige der Übungsaufgaben mit diesem Zahlentheoriepaket zu lösen.

W. Meier, Brugg-Windisch

Typesetting & Layout: *mathScreen online, CH-4123 Allschwil*