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

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*