Rezension zu

Christian Karpfinger, Hubert Kiechle
Kryptologie
2010
261 Seiten, Flexcover, 24,90 Euro
ISBN-13: 978-3-8348-0884-4
VIEWEG+TEUBNER

Das vorliegende Buch reiht sich ein in die Vielzahl von Lehrbüchern zur Kryptologie und gibt eine Übersicht über alle klassischen und aktuellen Verschlüsselungsverfahren. Es richtet sich an Studenten der Mathematik und Informatik, die mit den Grundbegriffen der linearen Algebra bereits vertraut sind. Die zusätzlich benötigten mathematischen Grundlagen werden jeweils bereitgestellt, so dass sich das Buch gut zum Selbststudium eignet.

Die einzelnen Kapitel behandeln jeweils verschiedene Verfahren: klassische Chiffren, Blockchiffren, symmetrische Authentifikation, Exponentiationschiffren, das RSA-Verfahren, Primzahltests, die Verfahren von Diffie-Hellman und ElGamal, den diskreten Logarithmus, Faktorisierungsalgorithmen, Signaturverfahren, Elliptische Kurven und deren Anwendungen. In vielen Kapiteln finden sich anschauliche Beispiele und einige Übungsaufgaben (jedoch ohne Lösungen). Auch wenn es nur sehr wenige Abbildungen gibt, ist das Buch sehr angenehm zu lesen und verständlich geschrieben. Alle verwendeten Resultate werden ausführlich bewiesen.

Die Inhalte des Buches bilden in etwa den Stoff einer vierstündigen Vorlesung und ermöglichen damit eine fundierte Kenntnis wichtiger Methoden der Kryptologie. Das Werk eignet sich damit sehr gut sowohl für Dozenten als auch für Studenten, die sich für diskrete Mathematik interessieren. Aktuelle Anwendungen stehen hier nicht im Vordergrund, was aber auch nicht der Anspruch des Buches ist. Es ist also ein gelungenes, empfehlenswertes Stück in der großen Auswahl an Büchern zur Kryptologie.