Rezension zu

Albrecht Beutelspacher, Heike B. Neumann, Thomas Schwarzpaul
Kryptografie in Theorie und Praxis
2. Auflage, 2010
324 Seiten, Flexcover, 26,95 Euro
ISBN-13: 978-3-8348-0977-3
VIEWEG+TEUBNER

Zur Theorie der Verschlüsselung gibt es unzählige Bücher und Aufgabensammlungen. Wie man es aber von Albrecht Beutelspacher gewohnt ist, ist dieses Buch besonders übersichtlich, leicht und angenehm zu lesen, ohne dabei jedoch den hohen mathematischen Anspruch aus den Augen zu verlieren. „Kryptografie in Theorie und Praxis“ behandelt alle wichtigen Verschlüsselungsverfahren, bietet dem Leser nach jedem Abschnitt passende Übungsaufgaben zum Stoff an und widmet sich umfassend den Anwendungen der Methoden.

Nach einer Einleitung zur Motivation, wichtigen Begriffen und Zielen in der Kryptografie werden im ersten Kapitel symmetrische Verfahren vorgestellt. Dazu zählen z.B. Vigenère-Chiffren, Stromchiffren, Blockchiffren und Kaskadenverschlüsselungen. Eine Vielzahl von Abbildungen erleichtert das Verständnis. Im folgenden Kapitel zur asymmetrischen Kryptografie werden der RSA-Algorithmus, der diskrete Logarithmus und ElGamal-Systeme bis hin zu Kryptografie mit elliptischen Kurven behandelt. Auch viele weniger bekannte Verfahren wie Rabin-Verfahren und Paillier-Verschlüsselungen werden aufgegriffen. Im dritten Kapitel geht es dann um die Anwendungen. Themen wie Hashfunktionen, Zero-Knowledge-Protokolle, Schlüsselverwaltung, Anonymität, Internet- und Mobilfunksicherheit sowie das Quantencomputing werden in einzelnen Abschnitten diskutiert.

Das Buch ist ein gelungenes Lehrbuch zur Kryptografie, das sowohl Studenten der Mathematik und Informatik als auch Dozenten als Vorlesungsleitfaden zu empfehlen ist. Inhaltlich geht es sogar weit über das hinaus, was man in einer normalen Kryptografie-Vorlesung schaffen kann. Durch die Vielzahl der vorgestellten Verfahren und die gute Gliederung des Buches in Teilabschnitte würde es sich auch für mathematische Seminare eignen. Das Werk ist auf dem neuesten Stand und stellt alle modernen Verschlüsselungstechniken vor. Die mathematische Theorie wird im Lehrbuchstil durch Definitionen, Sätze und Algorithmen dargestellt, die Beweise sind ausführlich und übersichtlich. Zu den vorgestellten Übungsaufgaben finden sich zwar keine Lösungen, dennoch ist das Buch für alle an Kryptografie interessierten Leser uneingeschränkt zu empfehlen.