Einführung in die Kryptologie

von Karin Freiermuth, Juraj Hromkovič, Lucia Keller, Björn Steffen

Broschiert: 407 Seiten
Verlag: Vieweg+Teubner; Auflage: 1., 2010
ISBN-13: 978-3-8348-1005-2

Rezensiert von Ute Schreiber

„Einführung in die Kryptologie“ ist ein Lehrbuch, welches sich den Grundlagen der Kryptologie, also den Grundlagen von Geheimschriften und Verschlüsselungen, widmet. Gerade in der heutigen Zeit der Rechentechnik und des Internets spielen sichere Verschlüsselungen von Nachrichten eine immens große Rolle. Aber auch schon in der Antike hat man versucht, Botschaften mit Geheimschriften zu verschicken. Wie man eine Sprache „gut“ verschlüsselt, also gegen eine Entschlüsselung besonders sicher macht, ist Inhalt dieses Buches.

Das Buch beginnt mit einem Kapitel über Geschichtliches und der Definition von Grundbegriffen. Im zweiten Kapitel werden mathematische Voraussetzungen (modulares Rechnen, Monoide, Gruppen, . . .) eingeführt. Kapitel 3 und 4 beschäftigen sich mit Mono- und Polyalphabetischen Systemen. Die weiteren Kapitel (5 bis 11) widmen sich an verschiedenen klassischen Beispielen der Sicherheit von Kryptosystemen; angefangen beim Kerkhoffs-Prinzip und der perfekten Sicherheit im statistischen Sinn, bis hin zum Sicherheitskonzept moderner Systeme wie des Public-Key-Systems beim RSA-Algorithmus. Jedes Kapitel endet mit einer Zusammenfassung, zahlreichen Kontrollfragen und Kontrollaufgaben.

„Einführung in die Kryptologie“ setzt weniges mathematisches Grundwissen aus Kombinatorik und Wahrscheinlichkeitsrechnung voraus. Außerdem sollte der Leser das Lösen von linearen Gleichungssystemen beherschen. Das Buch ist daher nicht nur für Studenten von Hoch- und Fachhochschulen geeignet, sondern auch in Schulen einsetzbar oder für andere interessierte Leser empfehlenswert. Mit großem didaktischen Geschick gelingt es den Autoren, die Grundlagen der heutzutage weit genutzten Public-Key-Kryptographie zu vermitteln. Das Buch zeichnet sich dabei insbesondere durch sein langsames Vorangehen aus, begleitet durch viele zum Teil populäre Beispiele und zahlreiche Aufgaben. Die präzise genutzen mathematischen Begriffe erleichtern dabei ebenfalls das Lesen. Hinweise zu optionalen Themen lassen Spielraum für mehr oder weniger zur Verfügung stehende Zeit beim Durcharbeiten.

Besonders empfehlenswert ist „Einführung in die Kryptologie“ allen Lehrkräften und Lehrern, auch wenn ihnen diese Thematik noch neu ist. Der rote Faden von der Geschichte zum Public-Key des modernen RSA-Algorithmus’, die vielen Aufgaben im laufenden Text mit ensprechenden Lösungen und die zahlreichen Hinweise für Lehrer machen „Einführung in die Kryptologie“ zu einer richtig runden Sache.