HANSER

Vorwort

Rolf Socher

Algebra für Informatiker

Mit Anwendungen in der Kryptografie und Codierungstheorie

ISBN (Buch): 978-3-446-43257-4

ISBN (E-Book): 978-3-446-43312-0

Weitere Informationen oder Bestellungen unter

http://www.hanser-fachbuch.de/978-3-446-43257-4

sowie im Buchhandel.

Vorwort

In einer Zeit wachsender Globalisierung und steigender Vernetzung hat das Thema Sicherheit in der Informatik eine herausragende Bedeutung erlangt. Ein Aspekt dieses Themas betrifft den Schutz sensibler Daten gegen unerwünschten Zugriff oder Manipulation. Ziel der *Kryptografie* ist die Entwicklung von Verfahren und Algorithmen, um Daten zugriffssicher zu verschlüsseln.

Ein zweites Gebiet der Informationssicherheit betrifft die Integrität von Daten. Dazu zählt unter anderem der Schutz von Daten gegen zufällig auftretende Fehler, etwa bei der Datenübertragung oder bei der Speicherung auf Medien. Die *Codierungstheorie* beschäftigt sich mit Verfahren, Daten so zu codieren, dass zufällige Fehler erkannt und möglichst auch korrigiert werden können.

Sowohl Kryptografie als auch Codierungstheorie beruhen in hohem Maße auf Erkenntnissen der Algebra, also der Theorie algebraischer Strukturen wie Gruppen, Ringe, Körper und Polynomringe. Das vorliegende Buch behandelt in den ersten vier Kapiteln diese Strukturen in der Tiefe, wie sie für die Anwendungen in der Kryptografie und Codierungstheorie benötigt werden. Das fünfte und sechste Kapitel geben jeweils eine Einführung in die Grundbegriffe und die wichtigsten Methoden der Kryptografie beziehungsweise der Codierungstheorie, sodass die Leserin oder der Leser in der Lage ist, sich die weiterführende Literatur zu diesen beiden Themen selbstständig zu erarbeiten.

Das Buch richtet sich an Studierende von Masterstudiengängen der Informatik an Hochschulen oder Universitäten. Es setzt Grundkenntnisse der linearen Algebra, wie sie in Bachelorstudiengängen der Informatik vermittelt werden, voraus. Die benötigten Grundlagen der elementaren Zahlentheorie und modularen Arithmetik sind im Anhang zu diesem Buch kompakt zusammengefasst.

Die Lösungen zu den Aufgaben finden sich auf der Webseite zu diesem Buch:

http://informatik.fh-brandenburg.de/~socher/AfI

Ich danke allen, die zur Entstehung dieses Buchs beigetragen haben. Mein besonderer Dank gilt Susanne Hohmann, Jakob Rittberg, Martin Schiemann-Lillie und Manfred Schmidt-Schauß, die das Manuskript sehr sorgfältig Korrektur gelesen haben und denen ich viele nützliche Hinweise und Verbesserungsvorschläge verdanke. Ferner danke ich dem Carl Hanser Verlag, insbesondere Christine Fritzsch (Lektorat) und Katrin Wulst (Herstellung), für die gewohnt gute und vertrauensvolle Zusammenarbeit.

Berlin, im April 2012 *Rolf Socher*