

Vorwort

Das vorliegende Buch gibt eine Einführung in die Fehlerkorrektur und Verschlüsselung digitaler Daten bei der Übertragung über einen Kanal. Ersteres, die Codierungstheorie, beschäftigt sich mit der Korrektur von Fehlern, die in einem unzuverlässig arbeitenden Kanal passieren. Zweiteres, die Kryptographie, hat die Verschlüsselung der Daten zum Inhalt, so dass sie weder gelesen noch manipuliert werden können. Das Buch ist gedacht für Studierende des Bachelor-Studiengangs Mathematik, Informatik oder Elektrotechnik, die bereits mit den Methoden der Linearen Algebra vertraut sind. An einigen wenigen Stellen benötigen wir elementare Sachverhalte aus der Wahrscheinlichkeitstheorie, die man etwa in dem Band *Elementare Stochastik* der gleichen Buchreihe nachlesen kann, sowie etwas Kombinatorik – dies beschränkt sich auf einfaches Abzählen, welches man auch als Anfänger gut nachvollziehen kann. Weitere zum Verständnis notwendige Grundlagen aus Gruppentheorie, Zahlentheorie, Algebra und Komplexitätstheorie haben wir in einem Anhang zusammengestellt, jedoch nur so weit, wie sie benötigt werden. Hier sollte man beim Studium der Codierungstheorie und Kryptographie nachlesen, wenn etwas unverstanden bleibt. Beide Kapitel sind in sich geschlossen, so dass sie unabhängig voneinander studiert werden können.

Um den Inhalt des Buches kompakt zu halten, werden ausgewählte Facetten der beiden Themenkreise behandelt werden. Wir haben daher den Stoff auf das aus heutiger Sicht Wesentliche beschränkt. So sagen wir zum Beispiel nichts über Verschlüsselungsmethoden aus der Vergangenheit, die aus historischer Sicht interessant sind, heute jedoch keine Rolle mehr spielen, sondern konzentrieren uns weitgehend auf die moderne Public-Key-Kryptographie. Die Abschnitte über LDPC-Codes und den AKS-Algorithmus, sowie die teilweise Behandlung von Edwardskurven und Schrijvers Optimierungsmethode geben dem Stoff eine zeitgemäße Prägung.

Hin und wieder sind im Text weitergehende, insbesondere auch neuere Resultate und offene zentrale Probleme eingestreut. Sie sollen einen tieferen Einblick in das Dargestellte vermitteln und zur weiteren Beschäftigung mit den Fragestellungen anregen.

Die in den einzelnen Abschnitten gestellten Aufgaben, für die wir teilweise am Ende des Buches Lösungen angegeben haben, sind zur Selbstkontrolle gedacht. Sie sind teils theoretischer Natur, teils aber auch einfach Rechenaufgaben, in denen Algorithmen nachvollzogen werden sollen. Mitunter treten dabei, aber auch in den Beispielen zu kryptographischen Verfahren, Rechnungen mit großen Zahlen auf, so dass die Verwendung eines Computer-Algebrasystems hilfreich, wenn nicht unerlässlich ist.

Beim ersten Auftreten des Namens einer bedeutenden Persönlichkeit haben wir in einer Fußnote die Lebensdaten, die Wirkungsstätte und deren Beiträge zur Forschung angegeben.

Besonderer Dank gebührt an dieser Stelle Christian Bey, Gohar Kyureghyan und Ralph August, die weite Teile des Buches gelesen und bei der Erstellung der Zeichnungen geholfen haben. Ihr Engagement hat erheblich zur Verbesserung des Textes beigetragen. Ferner danke ich den Herausgebern und dem Birkhäuser Verlag für wertvolle Hinweise bei der Entstehung des Buches.

Magdeburg, im Februar 2008

Wolfgang Willems



<http://www.springer.com/978-3-7643-8611-5>

Codierungstheorie und Kryptographie

Willems, W.

2008, XII, 152 S., Softcover

ISBN: 978-3-7643-8611-5

A product of Birkhäuser Basel