Vorwort

Mathematische Verschlüsselungssysteme spielen für die Sicherheit der Kommunikation und der Abwicklung von Geschäften auf elektronischem Weg eine entscheidende Rolle. Die den Verfahren zugrunde liegende Mathematik wird zum Teil seit Jahrhunderten studiert, konkrete Anwendungen sind aber bis auf einfache, manuell meist recht mühsam durchzuführende Fälle erst seit relativ kurzer Zeit mit Hilfe von Rechnern möglich. Mit der nunmehr breiten Nutzungsmöglichkeit entwickelt sich schnell eine Vielzahl unterschiedlicher Anforderungen, die die neue Technik erfüllen soll. Eine Grundkenntnis der verschiedenen mathematischen Prinzipien ist für die Entwicklung spezieller Verfahren und die Abwägung der mathematischen Risiken notwendig, Entwurf und Implementation von Algorithmen und Protokollen sind recht anspruchsvolle Aufgaben.

Das vorliegende Buch ist anhand von Vorlesungen und Projekten an einer Fachhochschule für den Studiengang Informatik im Hauptstudium entstanden. Die Mathematik gehört (leider) nicht gerade zu den bevorzugten Fächern der meisten Fachhochschulstudenten. Aus diesem Grund habe ich besonderen Wert auf einen experimentellen Zugang gelegt: ohne von einer exakten Darstellung der Mathematik abzurücken (bis auf wenige Ausnahmen werden alle Sätze ausführlich bewiesen), werden viele Themen durch rechnergestützte Experimente vor- oder aufbereitet bzw. anschaulich gemacht. Allerdings wird auch die eine oder andere mathematische Formulieren dem reinen Mathematiker etwas umständlich erscheinen. Das hat aber rein didaktische Gründe, um dem Ungeübten den Einstieg zu erleichtern. Durch die Verknüpfung von Theorie und Praxis ist das Buch sicher auch für Informatiker oder Mathematiker an Universitäten als Einführung oder Begleitung von praktischen Übungen hilfreich. Vorkenntnisse der Einführungsveranstaltungen in Analysis und linearer Algebra sowie einer Programmiersprache sollten vorhanden sein.

Thematisch ist das Buch in vier Hauptabschnitte eingeteilt. Im ersten Teil wird die grundlegende Mathematik (*Gruppentheorie und Zahlentheorie*) für die Konstruktion von Verschlüsselungssystemen vorgestellt. Die algebraischen Grundlagen werden weitgehend auf die Gruppentheorie beschränkt und auch hier wiederum auf Themen, die für die zu bearbeitenden Fragestellungen von Bedeutung sind. Sofern bei einigen speziellen Anwendungen weitere algebraische Begriffe und Beziehungen für das Verständnis oder den Beweis notwendig sind, werden diese gezielt und begrenzt eingeführt. Sätze werden meist mit größerer Ausführlichkeit dargestellt, als dies in der mathematischen Literatur üblich ist.

Im Anschluss an die mathematischen Grundlagen werden verschiedene Algorithmen und Sicherheitsprotokolle detailliert dargestellt und die Wirkungsweise an Beispielen demonstriert. Die Algorithmen beschränken sich nicht auf solche aus der Zahlentheorie. Auch symmetrische Verschlüsselungs- und Hash-Algorithmen werden diskutiert, wobei besonderer Wert auf die Begründung des „Warum ?" gelegt wird. Sicherheitsprotokolle beschreiben Gesamtabläufe zum Erreichen eines vorgegeben Kommunikationsziels.

Im dritten Teil werden bestimmte Zahleneigenschaften untersucht. Neben die strenge mathematische Betrachtung tritt hier zunehmend eine praxisorientierte, „ingenieurmäßige" Betrachtungsweise mit statistischen Abschätzungen und Messungen, die innerhalb eines vorgegebenen

Rahmens ein kontrolliertes Arbeiten ermöglicht. Praktische Ergebnisse sind Möglichkeiten zum Erzeugen von Zufallzahlen, zum Erkennen von Primzahlen bestimmter Qualität sowie der Kontrolle der korrekten Auswahl geheimer oder öffentlicher Parameter. Darüber hinaus wird der Leser mit Strukturen im System der ganzen Zahlen vertraut gemacht, die vielleicht zu eigenen weitergehenden Experimenten anregen.

Ein Kapitel über Angriffsmöglichkeiten auf Verschlüsselungssysteme rundet die Betrachtung ab. Neben einfachen Basismethoden wird das quadratische Sieb für den Angriff auf RSA-ähnliche Verschlüsselungssysteme ausführlich vorgestellt. Parallel zur Entwicklung der Mathematik ist der Leser hier zum Entwurf und zur Implementierung von Algorithmen aufgerufen. Bei der behandelten Spannweite der Themen und des begrenzten Umfangs dieses Buches ist aber auch eine Einschränkung der Stoffauswahl nicht zu vermeiden. Einige interessante Themen wie ASN.1, elliptischen Funktionen, das Zahlenkörpersieb und andere können daher nur am Rand erwähnt werden.

Aufgaben befinden sich nicht am Ende eines jeden Kapitels, wie einige Leser das sicher von anderen Büchern gewohnt sind, sondern sind in die Stoffentwicklung integriert. Neben einigen mathematischen Aufgaben ist der Leser überwiegend aufgefordert, parallel zur Mathematik Algorithmen zu entwerfen und zu implementieren, um die theoretischen Erkenntnisse direkt in die Praxis umzusetzen. Als Programmiersprache empfehle ich C++ , da hier eine Reihe von Bibliotheken über das Internet zugänglich sind, die sowohl Basisalgorithmen als auch Sammlungen von Verschlüsselungsalgorithmen für weiterführende eigene Arbeiten beinhalten.

Literaturhinweise habe ich auf allgemeine Lehrbücher beschränkt und auf das Zitieren von Literaturstellen zu den diskutierten speziellen Verschlüsselungsalgorithmen verzichtet. Da die Diskussion vieler wichtiger algebraischer Begriffe auf das für den hier behandelten Stoff notwendigste beschränkt wird, ist ein Griff zu einem Lehrbuch über Algebra für eine Vertiefung an der einen oder anderen Stelle hilfreich, und den einen oder anderen Leser wird es vielleicht erstaunen, wie einzelne bislang nicht verstandene oder überlesene Kapitel auf einmal einen neuen Sinn bekommen. Hinsichtlich der speziellen Algorithmen bereitet es überhaupt kein Problem, sich über eine Suchmaschine im Internet in kurzer Zeit so viel „Vertiefungsstoff" zu beschaffen, dass das Problem nicht planbarer Freizeitbeschäftigung auf Jahre aus dem Weg geräumt ist.

Abschließend möchte ich anmerken, dass mit „dem Leser" im Text keine geschlechtsspezifische Eigenschaft verbunden ist. Dass „der Leser" als Synonym für „das lesende Individuum" in der deutschen Sprache nun einmal mit dem maskulinen Artikel vergesellschaftet ist, sollte ruhig einmal als historische Sprachentwicklung hingenommen und nicht durch Platzfresser wie „Leserinnen und Leser" oder „Leser und Leserinnen", abgekürzt „LeserInnen", substituiert werden. In diesem Sinn sei der Leser auch herzlich eingeladen, sich mit Anregungen, eigenen Ergebnissen oder Problemen mit mir in Verbindung zu setzen (Web-Seiten: http://www.ewetel.net/~gilbert.brands/ , EMail gilbert.brands@ewetel.net oder über die Web-Seiten der Fachhochschule Oldenburg-Ostfriesland-Wilhelmshaven).

Pewsum, im Sommer 2002

Gilbert Brands