Vorwort

Kryptologie ist eine Wissenschaft, die sich mit dem Verschlüsseln geheimer Informationen beschäftigt. Schon im 17. Jahrhundert wurden mechanische Chiffriermaschinen gebaut. Diese Maschinen ermöglichen es, einen „Klartext" einfach und schnell zu verschlüsseln, oder umgekehrt, einen chiffrierten Text zu entschlüsseln. Anfangs funktionierten diese Maschinen rein mechanisch, später elektrisch oder sogar elektronisch. Heute gibt es spezielle Mikrochips, deren einzige Aufgabe es ist, schnell und zuverlässig Daten zu chiffrieren und dechiffrieren.

Aber ebenso, wie man sich bemühte, immer bessere Chiffriermaschinen zu konstruieren, so hat man sich auch bemüht, Analysemethoden und Maschinen zu entwickeln, um Chiffren zu brechen. Das spektakulärste Beispiel für erfolgreiche Kryptoanalyse ist die sogenannte „Turing-Bombe", ein Verfahren, das von Polen und Engländern entwickelt wurde und mit dem es noch während des 2. Weltkriegs gelang, die Chiffren der Deutschen Wehrmacht, erfolgreich zu entschlüsseln. Die deutsche Chiffriermaschine „ENIGMA" galt, nach Meinung der führenden Experten, als „absolut sicher"! Bemerkenswert ist auch die Tatsache, daß das Analyseverfahren erst nach 1967 veröffentlicht wurde. Bis dahin war die Kryptologie eine Domäne militärischer Forschungseinrichtungen.

Mit fortschreitender Entwicklung der Informatik ergaben sich, außer weiteren militärischen Anwendungen, auch zivile Anwendungsgebiete für die Kryptologie. Heute werden kryptographische Methoden im elektronischen Zahlungsverkehr und vielen anderen Bereichen eingesetzt. Mit zunehmender Vernetzung der Computer werden neue Methoden gebraucht, um Daten sicher vor den Augen Unbefugter zu übertragen und zu speichern. Viele Probleme sind noch ungelöst.

In diesem Buch wird die Entwicklung (im Sinne von Evolution) symmetrischer Kryptosysteme vorgestellt. Dabei werden die wichtigsten Chiffren ausführlich beschrieben. Außerdem wird auf ausgewählte Techniken der Kryptoanalyse eingegangen. Diese Techniken werden jeweils so detailliert beschrieben, daß der Leser alle Informationen erhält, die zur Implementierung der Analyseverfahren notwendig sind. Alle Definitionen, Sätze und deren Beweise sind gründlich ausgeführt, so daß sie auch ohne Spezialkenntnisse oder weiterführende Literatur nachvollziehbar sind. Die mathematischen Grundlagen werden erklärt.

Es ist möglich, das Buch innerhalb eines Semesters durchzuarbeiten. Dazu benötigt man etwa vier Vorlesungsstunden pro Woche. Da alle Inhalte sehr ausführlich beschrieben sind, ist das Buch aber auch zum Selbststudium geeignet.

Danksagung

Ein mathematisches Buch zu schreiben beansprucht viel Zeit und als Autor empfinde ich das nicht als Belastung. Als freizeitliebender Mensch und als Ehemann tut es mir jedoch um jede Stunde leid, die ich nicht mit den wirklich wichtigen Dingen verbringe. Trotzdem hat es einen Weg zu diesem Buch gegeben, und dafür danke ich meiner Frau Pia, ohne deren Verständnis und Ermutigungen das alles nicht möglich gewesen wäre.