K. G. Saur Verlag, München, 1993

Friedrich L. Bauer, Kryptologie: Methoden und Maximen, Springer-Verlag, Berlin, 1993, 357 Seiten, DM 48,-

Die Kryptologie als Wissenschaft ist zumindestens in unserem Jahrhundert von einem Schleier des Geheimnisvollen umgeben. Zum Einen weil sie selbst natürlich verwendet wird, um Informationen geheim zu halten, zum Anderen gehört sie im professionellen Einsatz zum typischen Arbeitsgebiet der Geheimdienste, die sich für gewöhnlich mit einem solchen Schleier umgeben. Es wundert daher nicht so sehr, wenn Friedrich L. Bauer im Vorwort zu seinem Buch Kryptologie bemerkt, daß er im Somersemester 1981 an der Universität München die vermutlich erste offene Vorlesung in Europa über dieses Thema gehalten hat. Aus einer Reihe solcher Vorlesungen entstand schließlich das vorliegende Buch, dem man die langjährige Beschäftigung des Autors mit dem Thema anmerkt. Belegt wird das Interesse des Autors auch durch die wesentliche Mitarbeit beim Aufbau des kryptologischen Kabinetts im Deutschen Museum München. Obwohl der Autor niemals einem „Dienst" angehört hat, ist er vier Jahrzehnte seinem Interesse an der Kryptologie nachgegangen und hat dabei neben seiner großen Fachkenntnis vor allem einen schier unerschöpflichen Fundus aus Anekdoten und historischen Beispielen zusammengetragen.

Durch das ganze Buch hindurch versteht er es glänzend, die mathematisch fundierte Darstellung der Wissenschaft Kryptologie durch historische Bezüge aufzulockern, so daß nie Langeweile beim Leser aufkommt. Für das Verständnis setzt er nur elementare mathematische Kenntnisse und Begriffe voraus (einfache Gruppentheorie, Abbildungen und dergleichen) und verweist im Zweifelsfall auf weitergehende Literatur (z. B bei Sätzen aus der Zahlentheorie). Der Leser sollte allerdings keine Scheu vor der mathematischen Notation besitzen, da ihm sonst wesentliche Teile der Darstellungen verschlossen bleiben. Während die verwendeten Begriffe aus der Mathematik vorausgesetzt werden, werden die Fachbegriffe der Kryptologie nach und nach systematisch eingeführt und durch eine Vielzahl von Beispielen beschrieben. Über die rein wissenschaftliche Darstellung hinaus geht der Autor aber auch an vielen Stellen, sowohl auf allgemeine Grundregeln der Kryptographie als auch auf politische und gesellschaftliche Auswirkungen ein.

Das 340-seitige Buch gliedert sich in zwei etwa gleich umfangreiche Teile über Kryptographie und Kryptanalyse, womit der Autor die beiden typischen Sichtweisen zu diesem Thema einnimmt. Die Kryptographie bezeichnet das Vorgehen desjenigen, der eine Nachricht möglichst unentzifferbar verschlüsseln will, die Kryptanalyse beschreibt das Vorgehen eines potentiellen Gegenspielers, der, ohne dazu befugt zu sein, versucht, diese Verschlüsselung zu brechen. Die beiden Teile des Buchs sind jeweils übersichtlich in elf Kapitel unterteilt. Im kryptographischen Teil beschreibt er nach einer sehr kurzweiligen Einleitung nacheinander die Verschlüsselung durch einfache Zeichen-Substitutionen, die polygraphischen Substitutionen, bei denen mehrere Zeichen gleichzeitig ersetzt werden, die Transpositionen von Zeichen im Text und die polyalphabetischen Chiffrierungen mit mehreren Alphabeten. Darauf aufbauend geht er weiter bis hin zu Verfahren wie DES, einem genormten Verfahren, das beim UNIX-Betriebssystem eingesetzt wird oder RSA, einem Verfahren, das auf der Benutzung sehr großer Primzahlen aufbaut und gelegentlich (bei neuen Primzahlrekorden) in der allgemeinen Presse erwähnt wird. Er beschreibt aber keineswegs nur die verwendeten Verfahren, sondern geht auch ausführlich auf allgemeine Grundsätze und Hinweise zu Chiffrierung ein und beleuchtet kritisch die politischen Interessen und Anforderungen in Abwägung zu privaten Interessen.

Im kryptanalytischen Teil wird zunächst die Problematik des vollständigen Durchprobierens aller Möglichkeiten (Exhaustionsmethode) als Grundlage für die allermeisten Entschlüsselungsverfahren beschrieben. Hier werden auch Begriffe wie die Unizitätslänge, ab der eine eindeutige unberufene Entschlüsselung erst möglich wird, eingeführt. Praktisch alle anderen Ansätze zur Entschlüsselung beruhen auf Eigenheiten der menschlichen Sprache, die durch eine Chiffrierung erhalten bleiben und somit einen Ansatzpunkt zur unbefugten Dechiffrierung bieten. Im Buch wird nun eingegangen auf Häufigkeitsverteilungen von Buchstaben und Buchstabengruppen und Sprachmuster bis hin zu allgemeineren sprachlich-statistischen Parametern. Alle beschriebenen Verfahren werden wieder an Beispielen vorgeführt. Bei diesen überläßt der Autor z. B. schon einmal die endgültige Entschlüsselung eines Geheimtextes dem Leser zur Übung und gibt nur Hinweise auf die verwendete Literaturstelle. Er versteht es dabei, wie schon im ganzen Buch, das Interesse des Lesers nicht nur an der Wissenschaft der Kryptographie, sondern gerade auch an der Kunst der Kryptographie zu wecken. Wenn er nach einigen Bemerkungen zur moralischen Bewertung der Kryptographie als moderner Wissenschaft mit folgendem Zitat von Babbage endet, so möchte ich jedem potentiellen Leser nur raten, daß er nach dem Genuß dieses Buches selbst acht geben muß, daß es ihm nicht ähnlich ergeht:

„Deciphering is, in my opinion, one of the most fascinating of arts, and I fear I have wasted upon it more time than it deserves."

Dr. E. Strohmaier, Universität Mannheim

A. Schill: DCE Das OSF Distributed Computing Environment Einführung und Grundlagen Springer Verlag Heidelberg, 1993, 249 Seiten, DM 78,—

Die Vorteile, Probleme mit Hilfe eines verteilten DV-Systems zu lösen, wird kaum noch jemand ernsthaft bestreiten – im Gegenteil, bei vielen Gelegenheiten findet man Diskussionspartner, die einem geradezu missionarisch diesen Weg empfehlen. Am bekanntesten sind in diesem Rahmen natürlich Client-Server-Modelle – vielleicht deshalb, weil sie sich eingängig auf die jeweils bekannte Anwendung mehr oder weniger mit Zug und Druck übertragen lassen.

Etwas schwieriger wird es beim Verständnis dieser Vorgehensweise, wenn das Bedürfnis existiert, die zugrundeliegenden Mechanismen für diese Art der verteilten DV kennenzulernen und darüberhinaus auch noch die Frage nach einer einheitlichen Umgebung, bei einer heterogenen Rechnerlandschaft, zufriedenstellend beantwortet zu bekommen.

Läßt man die übliche Standardfloskel „Unix ist doch praktisch überall verfügbar" noch gelassen über sich ergehen, so ist es mit dieser Haltung spätestens nach der Folgemunition DCE & Co, inklusive Abkürzungsrattenschwanz,vorbei.

Dieses, von der Open Software Foundation (OSF) entwickelte Konzept für das „Distributed Computing Environment (DCE)" gilt nämlich in eingeweihten Kreisen und auch nach dem Klappentext des vorliegenden Buches von A. Schill als ein heißes Thema, von dem sich niemand mehr ohne Gesichtsverlust abkoppeln darf. Vielleicht reicht auch deshalb das Spektrum der Adressaten dieses Werkes von Studenten und Dozenten bis hin zu Programmierern, Software-Ingenieuren und Projektleitern. Man täusche sich aber nicht, dieses Versprechen wird wie viele nur halb, und bei genauerem Hinsehen noch weniger gehalten.

So ist es weder eine Einführung, welche