Zeitschrift: Technische Mitteilungen / Schweizerische Post-, Telefon- und Telegrafenbetriebe = Bulletin technique / Entreprise des postes, téléphones et télégraphes suisses = Bollettino tecnico / Azienda delle poste, dei telefoni e dei telegrafi svizzeri

Herausgeber: Schweizerische Post-, Telefon- und Telegrafenbetriebe

Band: 58 (1980)

Heft: 12

Buchbesprechung: Buchbesprechungen = Recensions = Recensioni

Buchbesprechungen – Recensions – Recensioni

Ryska N. und *Herda S.* (ed.) **Kryptographische Verfahren in der Datenverarbeitung.** = Informatik-Fachberichte, Band 24. Berlin, Springer-Verlag, 1980. 401 S., 123 Abb., 16 Tab. + V. Preis DM 46.50.

Mit der Entwicklung der Datenfernverarbeitung und der wachsenden Bedeutung des Datenschutzes gewinnen kryptographische Verfahren in der Datenverarbeitung immer mehr an Wichtigkeit. Nicht mehr nur im militärischen und diplomatischen, sondern auch im kommerziellen Bereich besteht das Bedürfnis, Informationen durch Geheimschriften dem Zugriff Unberechtigter zu entziehen, sei das über einen Passwortschutz oder durch eine Codierung der Daten selbst. Durch die Entwicklung der EDV ist auch die Anwendung von immer komplexeren und rechenintensiveren Algorithmen möglich geworden.

Die vorliegende Veröffentlichung gibt einen guten Überblick über die Gesamtproblematik der sicheren Kommunikation. Kryptographische Verfahren lassen sich vornehmlich in drei Bereichen der EDV — Datenübermittlung, Datenspeicherung und Authentifikation von Benutzern und Nachrichten — einsetzen. Das Buch ist in sieben Kapitel unterteilt, wobei im ersten die Begriffe definiert werden. Ein kurzer historischer Überblick sowie eine Standortbestimmung der Kryptographie im Rahmen des Datenschutzes vervollständigen diese Einleitung. Das zweite Kapitel ist den Sicherheitsrisiken bei der Datenverarbeitung gewidmet. Techniken des Missbrauchs sowie auch die möglichen Gegenmassnahmen werden aufgezeigt. In Kapitel 3 werden die verschiedenen Kryptosysteme analysiert und im Aufbau dargestellt. Dabei wird nicht nur auf «elementare» Kryptosysteme eingegangen (Sender und Empfänger können die Nachricht wieder entschlüsseln), sondern auch Kryptosysteme mit offenem Schlüssel (der Sender kann die Nachricht wohl verschlüsseln, aber nur der Empfänger kann sie wieder entschlüsseln) und Einwegfunktionen (die Nachricht kann nicht mehr entschlüsselt werden) werden ausführlich behandelt. Die letzteren Verfahren finden besonders bei der Speicherung von Passworten Verwendung. Bei der Analyse der Kryptoverfahren gehen die Autoren einseitig nur auf in englischer Sprache abgefasste Texte ein. Bei verschlüsselten deutschen Texten sind zur Analyse die zitierten englischen Sprachstatistiken keine Hilfe. Ausführlich kommentierte Beispiele sind leider sehr spärlich vorhanden. Die Integration von Kryptoverfahren in Computersysteme und Netzwerke ist Gegenstand der Untersuchungen der Kapitel 4 und 5. Die Implementation von Kryptosystemen in Datenbanken (Kapitel 6) bietet spezifische Schwierigkeiten bezüglich der Hierarchie von Schlüsseln und der möglichen Komplexität der Algorithmen, soll doch der Datentransfer durch die Entschlüsselung nur minimal verzögert werden. Kapitel 7 ist dem Problemkreis der Authentifikation in DV-Systemen gewidmet. Beispielsweise erfordert die Frage «Ist mein augenblicklicher Partner wirklich der von mir ursprünglich Gewählte oder hat sich ihm inzwischen jemand anderer substituiert?» zur Beantwortung ausgeklügelte Kommunikationsprotokolle, die besonders anhand klarer Grafiken verständlich erläutert werden.

Das Buch entspricht dem aktuellen Stand der Technik. Ein ausführliches Literaturverzeichnis sowie ein Abkürzungsverzeichnis schliessen das Werk ab. Als störend wird das Fehlen eines Stichwortverzeichnisses empfunden. Die Lesbarkeit des Textes wird durch die grafische Gestaltung erschwert. Das Werk richtet sich vor allem an DV-Spezialisten, wobei es zu seinem Verständnis gute mathematische Grundlagen erfordert. All denen, die sich lediglich einen Einblick in die Kryptographie verschaffen möchten, kann die Lektüre der zwei ersten Kapitel empfohlen werden. *M. Bütikofer*

Schoemaker S. (ed.) **Computer Networks and Simulation.** Amsterdam, North-Holland Publishing Co, 1978. XI + 256 S., zahlr. Abb. und Tab. Preis Dfl. 80.—.

Ce livre a été réalisé par un groupe d'experts en simulation de réseaux d'ordinateurs qui ont tenté de faire le point en 1978 sur l'état de cet art. Il ne contient donc pas les développements récents en ce domaine. Il suscite cependant un grand intérêt.

En méthodologie, les langages de simulation du type GPSS ou SIMULA sont comparés aux langages de programmation généraux et il est constaté que les outils de simulation de réseaux n'ont pas suivi le développement général en la matière. Il est mis en garde contre les dangers de la simulation par ordinateur à cause des difficultés d'établir un modèle qui corresponde à la réalité. Certaines méthodes de simulation en ligne, c'est-à-dire directement sur le réseau opérationnel, sont présentées.

Une brève incursion dans le domaine de la simulation du trafic téléphonique est également faite et l'état des travaux du CCITT en la matière est décrit. La majeure partie du livre traite cependant de la simulation sur ordinateur de réseaux d'ordinateurs. Les aspects principaux traités sont la simulation d'exactitude de protocoles et de leurs performances (débit, temps de transit) en fonction de différentes topologies de réseaux, l'optimisation globale de différentes ressources de réseaux (capacité de transmission, espace-mémoire), la simulation de stratégies de routage fixe ou adaptable (isolé, distribué et centralisé). Les problèmes d'interconnexion de réseaux d'ordinateurs sont également traités de manière approfondie.

Ce livre, d'un haut niveau moyen, s'adresse aux spécialistes responsables de la conception de réseaux informatiques aussi bien qu'à ceux dont la tâche est de simuler leur comportement. *J. Pitteloud*

Ullmann J. D. **Principles of Database Systems.** Potomac, Maryland, Computer Science Press Inc, 1980. 379 S., zahlr. Abb. und Tab. Preis unbekannt.

Ce livre a été composé à partir des notes d'un cours de l'auteur aux étudiants en «computer science» sur les systèmes de gestion de base de données (Data Base Management System = DBMS). Les DBMS sont d'abord décrits par trois niveaux d'abstraction: la *base de données physique,* présentée comme une collection de fichiers ou de structures de données mémorisée de façon permanente sur des mémoires de masse (disques, etc.); la *base de données conceptuelle,* décrite par l'intermédiaire d'un langage de définition des données (data definition language) comme un modèle abstrait, c'est-à-dire une représentation logique de la base de données physique; la *base de données* telle qu'elle est *perçue* par l'utilisateur, en fonctions des applications.

Après une présentation des méthodes d'organisation physique des données les plus courantes (fichiers indexés, fichiers à enregistrement variable, etc.), les trois grands modèles de données sont étudiés: le modèle *hiérarchique,* où les entités de la base (NOM, ADRESSE, etc.) sont représentées sous la forme de nœuds d'un arbre «généalogique», et où les enfants d'un nœud lui sont associés par des relations particulières; le modèle *réticulaire,* plus général, où les entités deviennent les

nœuds d'un graphe dirigé; le modèle *relationnel,* encore plus général, où les rapports entre entités et relations sont basés sur la théorie des ensembles.

Différents langages d'interrogation de données sont ensuite présentés pour le modèle relationnel: ISBL basé sur des notations algébriques, QUEL utilisant une technique appelé calcul du prédicat et enfin SQUARE et SEQUEL, langages intermédiaires entre les deux premiers. Ces langages abstraits n'ont à ce jour été implémentés totalement dans aucun DBMS existant, mais servent actuellement de référence pour l'évaluation de DBMS. Deux chapitres sont ensuite consacrés à la conception de bases de données relationnelles ainsi qu'à l'optimisation d'expressions d'algèbre et de calculs relationnels. Suivent deux chapitres plus concrets, l'un consacré aux langages de définition et de manipulation de données basées sur le modèle réticulaire, tels qu'ils sont proposés par le groupe de travail sur les bases de données (Data Base Task Group = DBTG) de l'organisme CODASYL (Conference on Data Systems Languages). Cette proposition, dont la première publication date de 1971, a été implémentée dans ses aspects essentiels sur les DBMS commercialisés: TOTAL, IDMS ou ADABAS entre autres. Le chapitre suivant présente le DBMS le plus répandu, basé sur le modèle de données hiérarchiques, c'est-à-dire IMS (Information Management System) d'IBM. Après une étude des problèmes de protection des DBMS contre leur mésusage (préservation de l'intégrité des données, contrôle des accès, etc.) sont décrits dans le dernier chapitre quelques algorithmes permettant l'exécution d'opérations concurrentes sur un DBMS (sérialisation des opérations, blocage d'écriture ou de lecture, etc.).

Cet ouvrage fournit une très bonne base théorique sur les DBMS. Non seulement les concepteurs mais également les spécialistes responsables de l'acquisition de systèmes à base de données ou de leur exploitation y trouveront quantité d'informations précieuses. *J. Pitteloud*

Seeger H. (ed.) **Technisches Design.** = Kontakt & Studium, Konstruktion, Band 54. Grafenau/Württ., Expert Verlag GmbH, 1980. 216 S., zahlr. Abb. und Tab. Preis DM 39.50.

Technisches Design wird definiert als das Entwickeln konstruktiver Lösungen für die Gebrauchsfunktionen von Geräten, Maschinen und Fahrzeugen nach ergonomischen Kriterien. Legt der Konstrukteur das Hauptgewicht auf physikalische, fertigungstechnische und wirtschaftliche Grundsätze, sind für den technischen Designer die gebrauchsgerechten und ergonomischen Elemente vordergründig. Beide arbeiten auf zweidimensionalen Unterlagen, der technische Zeichner oder Konstrukteur in drei Rissen, der technische Designer vorwiegend in perspektivischer Darstellung.

Der Verfasser hat das Ergebnis von vier Forschungsaufträgen über Maschinenarchitektur, konstruktive Form- und Tragwerkgestaltung sowie die Bedienungstechnik einerseits und von seiner Lehrtätigkeit an der Universität Stuttgart anderseits dem Buch zugrunde gelegt. Er setzt sich zum Ziel, das technische Design vollständig und sinnvoll in das methodische Konstruieren einzugliedern. Die einzelnen Kapitel sind einheitlich aufgebaut: Voraussetzungen, Konzept, Konstruktionsprinzipien, Bewertung, Zusammenfassung. Die theoretischen Betrachtungen werden mit praktischen Beispielen erläutert. Die Teilaufgabe des technischen Designs bei einer methodischen Produkteentwicklung (Kapitel 1) stützt sich auf bekannte Ablaufpläne und Methoden mit den Phasen: Planen, Konzipieren, Entwerfen und Ausarbeiten, wobei als Teilaufgabe die formale, erkennungs- und bedienungsgerechte Gestaltentwicklung nach Freiheitsgrad und Lösungstiefe betrachtet wird. In Kapitel 3 wird auf die Bedienungstechnik eingegangen. Technisch-, benützer- und marktorientierte Voraussetzungen bilden positive und negative Leitbilder der Bedienungstechnik. Die Lösungskriterien basieren auf Ergebnissen von Arbeitsgemeinschaften, Unfall- und Verhaltensforschung und auf der Zuhilfenahme von Arbeitsanalysen. Besonderes Gewicht wird beispielsweise auf die sichere und ermüdungsfreie Bedienung gelegt. Das Kapitel über die Kennzeichnungstechnik (mit über 50 Seiten) hat zum Ziel, ein Produkt nach Zweck, Bedienung, Leistung, Fertigung, Preis und Zeit zu beurteilen; es ist besonders reich mit Beispielen, Tabellen und Grafiken ausgestattet. Zur formalen Gestaltentwicklung (Kapitel 7) zählt die Form- und Farbgebung sowie die grafische Ordnung. Im letzten Kapitel stehen die Designkosten zur Diskussion.

Das Buch wirkt, wenn es nur überflogen wird, etwas theoretisch. Bei intensiverem Studium stellt man aber fest, dass die praxisbezogenen Beispiele den grössten Teil des Stoffes ausmachen. Es dient deshalb sowohl dem Ingenieur als auch dem Konstrukteur. *B. Gnehm*

Jecklin J. **Musikaufnahmen.** München, Franzis-Verlag, 1980. 208 S., 98 Abb., zahlr. Tab. Preis DM 34.—.

Musikaufnahmen setzen nicht nur musikalisches Grundwissen oder technisches Verständnis voraus, sondern sowohl Kenntnisse der elektrotechnischen Grundlagen als auch der Anwendungsmöglichkeiten elektroakustischer Geräte. Gelingt es einem Tonmeister, die ästhetischen und künstlerischen Gesichtspunkte mit der Technik in Einklang zu bringen, so wird ihm anhand der gebotenen Hilfsgeräte eine Wiedergabequalität möglich sein, die dem Original sehr nahe kommt. Verschiedentlich weist der Autor auf die Schwierigkeiten und technischen Mängel hin, die für eine vollendete und naturgetreue Wiedergabe hinderlich sind. Dabei sind auch die Akustik im Raum des kritischen Hörers sowie die von ihm gewählten Empfangs- und Wiedergabegeräte von Bedeutung, auf die ein Tonmeister keinen oder nur einen geringen Einfluss hat.

Der Inhalt des Buches ist in vier Hauptkapitel gegliedert: Grundlagen, Technik, Praxis und Aufnahmeprotokolle. Zuerst werden die Vorgänge im menschlichen Gehör erläutert; weiter sind die Grundprobleme der Elektroakustik, die Mikrofontechnik (einschliesslich Polymikrofonie), die einfache und professionelle Aufnahmetechnik, technische und künstlerische Aspekte sowie die Klangeigenschaften der Mikrofone, Musikinstrumente, Orchester und Musiker beschrieben, um dann mit einigen ausführlichen Aufnahmeprotokollen abzuschliessen. Mit einem Hinweis im Anhang auf die künftige digitale Aufnahmetechnik vermittelt der Autor dem Leser seine langjährigen praktischen Erfahrungen. Die Digitalisierung dieser Ausrüstungen steht aber heute noch in den Anfängen; es gibt in bezug auf die professionelle Anwendung noch einige Kriterien zu klären, die die Entwicklung beeinflussen können.

Es darf ohne Übertreibung gesagt werden, dass es dem Verfasser gelungen ist, mit diesem Werk eine Lücke in der Fachliteratur zu schliessen. Manch jungem Tonmeister und solchen, die es werden wollen, wird es deshalb eine geeignete Hilfe sein. *E. Kohler*

Hinweis auf eingegangene Bücher

VTT-Vergleichstabelle für europäische Transistoren: Datenvergleichstabelle. München, Franzis-Verlag, 1980. 413 S. Preis DM 34.—.

Dieses Tabellenwerk ist dem Praktiker bei der Ersatzbestückung eines Transistors dienlich. Einleitend vermittelt es Angaben über die elektrischen und mechanischen Eigenschaften eines Transistortyps, seine Hersteller und Vertreter. Daran schliessen sich umfangreiche Zusammenstellungen der Ersatztransistoren mit den Daten ihrer technischen Leistungen an. Zusätzlich findet der Benützer beim Ersatztyp Angaben über das Gehäuse und allfällige Abweichungen der elektrischen Daten vom Originaltyp. Durch Auswerten der Daten lässt sich so leicht ein Ersatz finden, weil bis zu sechs Ersatztypen angeführt werden, drei davon mit genauen Angaben der Unterschiede zum Originaltyp. In diesem Buch sind alle Si-Transistoren enthalten, die bei Pro Electron registriert worden sind. Die Ersatztypen sind natürlich unter Vorbehalt genannt; im Einzelfall empfiehlt sich stets ein Vergleich mit den Daten des Herstellers. Aus Platzgründen wurde auch weitgehend auf Stromverstärkungstransistoren verzichtet, ein Zusatzsymbol hinter der Typenbezeichnung weist jedoch darauf hin, dass eine Unterteilung in verschiedene Stromverstärkungsbereiche möglich ist. Insgesamt sind etwa 5000 Transistoren mit über 50 000 Daten und 220 Gehäuseformen aufgelistet. *ko.*