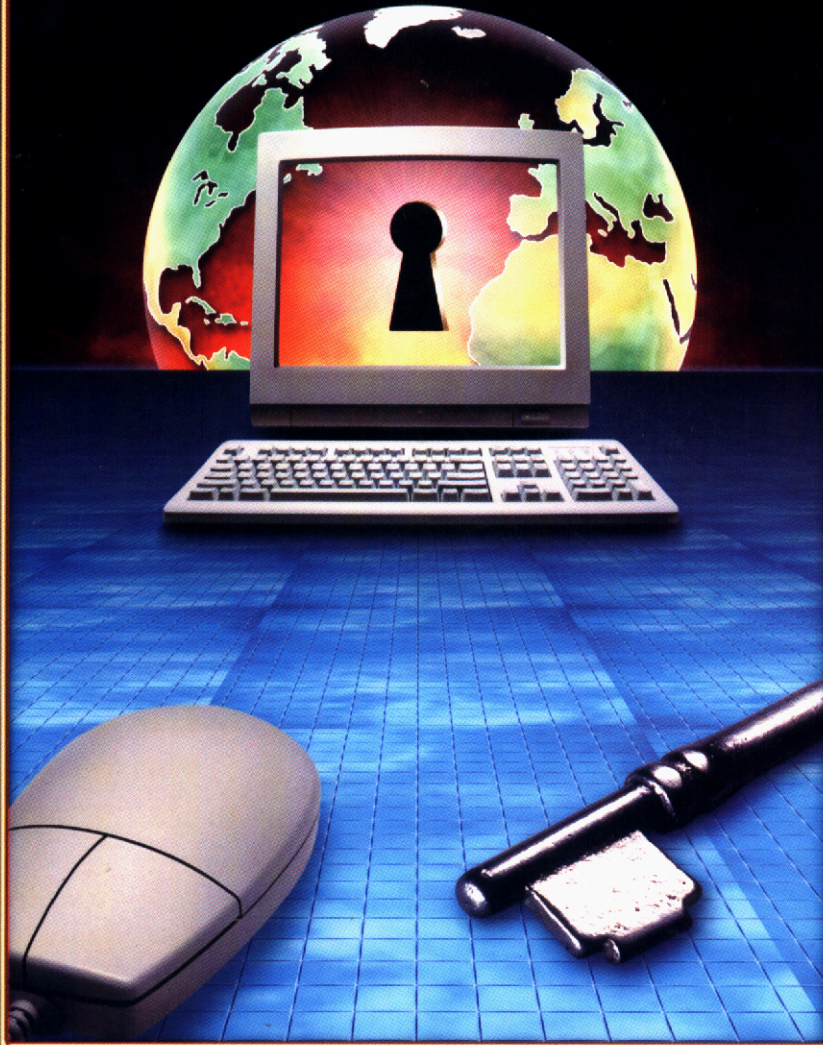


INTERNATIONAL EDITION

THIRD EDITION

Cryptography and Network Security

PRINCIPLES AND PRACTICES



William Stallings

THE WILLIAM STALLINGS BOOKS ON COMPUTER

DATA AND COMPUTER COMMUNICATIONS, SIXTH EDITION

A comprehensive survey that has become the standard in the field, covering (1) data communications, including transmission, media, signal encoding, link control, and multiplexing; (2) communication networks, including circuit- and packet-switched, frame relay, ATM, and LANs; (3) the TCP/IP protocol suite, including IPv6, TCP, MIME, and HTTP, as well as a detailed treatment of network security. **Received the 2000 Text and Academic Authors Association (TAA) award for long-term excellence in a Computer Science Textbook.** ISBN 0-13-084370-9

COMPUTER ORGANIZATION AND ARCHITECTURE, SIXTH EDITION

A unified view of this broad field. Covers fundamentals such as CPU, control unit, microprogramming, instruction set, I/O, and memory. Also covers advanced topics such as RISC, superscalar, and parallel organization. **Fourth and fifth editions received the TAA award for the best Computer Science and Engineering Textbook of the year.** ISBN 0-13-035119-9

OPERATING SYSTEMS, FOURTH EDITION

A state-of-the art survey of operating system principles. Covers fundamental technology as well as contemporary design issues, such as threads, microkernels, SMPs, real-time systems, multiprocessor scheduling, distributed systems, clusters, security, and object-oriented design. **Third edition received the TAA award for the best Computer Science and Engineering Textbook of 1998.** ISBN 0-13-031999-6

HIGH-SPEED NETWORKS AND INTERNETS, SECOND EDITION

A state-of-the art survey of high-speed networks. Topics covered include TCP congestion control, ATM traffic management, internet traffic management, differentiated and integrated services, internet routing protocols and multicast routing protocols, resource reservation and RSVP, and lossless and lossy compression. Examines important topic of self-similar data traffic. ISBN 0-13-03221-0

AND DATA COMMUNICATIONS TECHNOLOGY

WIRELESS COMMUNICATIONS AND NETWORKS

A comprehensive, state-of-the art survey. Covers fundamental wireless communications topics, including antennas and propagation, signal encoding techniques, spread spectrum, and error correction techniques. Examines satellite, cellular, wireless local loop networks and wireless LANs, including Bluetooth and 802.11. Covers Mobile IP and WAP.
ISBN 0-13-040864-6

LOCAL AND METROPOLITAN AREA NETWORKS, SIXTH EDITION

An in-depth presentation of the technology and architecture of local and metropolitan area networks. Covers topology, transmission media, medium access control, standards, internetworking, and network management. Provides an up-to-date coverage of LAN/MAN systems, including Fast Ethernet, Fibre Channel, and wireless LANs, plus LAN QoS.
Received the 2001 TAA award for long-term excellence in a Computer Science Textbook.
ISBN 0-13-012939-9

ISDN AND BROADBAND ISDN, WITH FRAME RELAY AND ATM: FOURTH EDITION

An in-depth presentation of the technology and architecture of integrated services digital networks (ISDN). Covers the integrated digital network (IDN), xDSL, ISDN services and architecture, signaling system no. 7 (SS7) and provides detailed coverage of the ITU-T protocol standards. Also provides detailed coverage of protocols and congestion control strategies for both frame relay and ATM. ISBN 0-13-973744-8

BUSINESS DATA COMMUNICATIONS, FOURTH EDITION

A comprehensive presentation of data communications and telecommunications from a business perspective. Covers voice, data, image, and video communications and applications technology and includes a number of case studies. ISBN 0-13-088263-1

NETWORK SECURITY ESSENTIALS

A tutorial and survey on network security technology. The book covers important network security tools and applications, including S/MIME, IP Security, Kerberos, SSL/TLS, SET, and X509v3. In addition, methods for countering hackers and viruses are explored.
ISBN 0-13-016093-8

Prentice Hall

www.prenhall.com/stallings

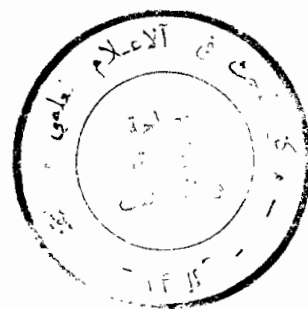
telephone: 800-526-0485

BIBLIOTHEQUE DU CERIST

CRYPTOGRAPHY AND NETWORK SECURITY

Principles and Practice

THIRD EDITION



William Stallings



Pearson Education International

This edition may be sold only in those countries to which it is consigned by Pearson Education International. It is not to be re-exported, and it is not for sale in the U.S.A., Mexico, or Canada.

Vice President and Editorial Director, ECS: *Marcia J. Horton*
 Publisher: *Alan R. Apt*
 Project Manager: *Jake Warde*
 Associate Editor: *Toni D. Holm*
 Editorial Assistant: *Patrick Lindner*
 Vice President and Director of Production and Manufacturing, ESM: *David W. Riccardi*
 Executive Managing Editor: *Vince O'Brien*
 Assistant Managing Editor: *Camille Trentacoste*
 Production Editor: *Rose Kernan*
 Director of Creative Services: *Paul Belfanti*
 Creative Director: *Carole Anson*
 Art Director: *Jon Boylan*
 Art Editor: *Greg Dulles*
 Cover Designer: *Laura Ierardi*
 Manufacturing Manager: *Trudy Piscioti*
 Manufacturing Buyer: *Lisa McDowell*
 Senior Marketing Manager: *Pamela Shaffer*



© 2003 by Pearson Education, Inc.
 Upper Saddle River, New Jersey 07458

All right reserved. No part of this book may be reproduced, in any form or by any means, without permission in writing from the publisher.

The author and publisher of this book have used their best efforts in preparing this book. These efforts include the development, research, and testing of the theories and programs to determine their effectiveness. The author and publisher make no warranty of any kind, expressed or implied, with regard to these programs or the documentation contained in this book. The author and publisher shall not be liable in any event for incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of these programs.

Printed in the United States of America

10 9 8 7 6 5

ISBN 0-13-111502-2

Pearson Education Ltd.
 Pearson Education Australia Pty. Limited
 Pearson Education Singapore, Pte. Ltd.
 Pearson Education North Asia Ltd.
 Pearson Education Canada, Ltd.
 Pearson Educación de México, S.A. de C.V.
 Pearson Education—Japan
 Pearson Education Malaysia, Pte. Ltd.
 Pearson Education, Upper Saddle River, New Jersey

*To my wife ATS,
The most compassionate,
kindest person in the world*

BIBLIOTHEQUE DU CERIST

CONTENTS

CHAPTER 1 OVERVIEW 1

- 1.1 Services, Mechanisms, and Attacks 4
- 1.2 The OSI Security Architecture 7
- 1.3 A Model for Network Security 14
- 1.4 Outline of This Book 17
- 1.5 Recommended Reading 17
- 1.6 Internet and Web Resources 18

PART ONE SYMMETRIC CIPHERS 21

CHAPTER 2 CLASSICAL ENCRYPTION TECHNIQUES 23

- 2.1 Symmetric Cipher Model 24
- 2.2 Substitution Techniques 30
- 2.3 Transposition Techniques 44
- 2.4 Rotor Machines 46
- 2.5 Steganography 47
- 2.6 Recommended Reading and Web Sites 49
- 2.7 Key Terms, Review Questions, and Problems 50

CHAPTER 3 BLOCK CIPHERS AND THE DATA ENCRYPTION STANDARD 55

- 3.1 Simplified DES 56
- 3.2 Block Cipher Principles 63
- 3.3 The Data Encryption Standard 72
- 3.4 The Strength of DES 82
- 3.5 Differential and Linear Cryptanalysis 83
- 3.6 Block Cipher Design Principles 86
- 3.7 Block Cipher Modes of Operation 90
- 3.8 Recommended Reading 98
- 3.9 Key Terms, Review Questions, and Problems 99

CHAPTER 4 INTRODUCTION TO FINITE FIELDS 103

- 4.1 Groups, Rings, and Fields 104
- 4.2 Modular Arithmetic 107
- 4.3 Euclid's Algorithm 115
- 4.4 Finite Fields of the Form $GF(p)$ 117
- 4.5 Polynomial Arithmetic 121
- 4.6 Finite Fields of the Form $GF(2^n)$ 126
- 4.7 Recommended Reading and Web Sites 134
- 4.8 Key Terms, Review Questions, and Problems 134

CHAPTER 5 ADVANCED ENCRYPTION STANDARD 139

- 5.1 Evaluation Criteria for AES 140
- 5.2 The AES Cipher 143
- 5.3 Recommended Reading and Web Sites 167
- 5.4 Key Terms, Review Questions, and Problems 167
- Appendix 5A Polynomials with Coefficients in $GF(2^8)$ 169

CHAPTER 6 CONTEMPORARY SYMMETRIC CIPHERS 173

- 6.1 Triple DES 174
- 6.2 Blowfish 179
- 6.3 RC5 185
- 6.4 Characteristics of Advanced Symmetric Block Ciphers 190
- 6.5 RC4 Stream Cipher 192
- 6.6 Recommended Reading and Web Sites 197
- 6.7 Key Terms, Review Questions, and Problems 197

CHAPTER 7 CONFIDENTIALITY USING SYMMETRIC ENCRYPTION 201

- 7.1 Placement of Encryption Function 202
- 7.2 Traffic Confidentiality 210
- 7.3 Key Distribution 211
- 7.4 Random Number Generation 220
- 7.5 Recommended Reading and Web Site 227
- 7.6 Key Terms, Review Questions, and Problems 228

PART TWO PUBLIC-KEY ENCRYPTION AND HASH FUNCTIONS 233

CHAPTER 8 INTRODUCTION TO NUMBER THEORY 235

- 8.1 Prime Numbers 236
- 8.2 Fermat's and Euler's Theorems 239

- 8.3 Testing for Primality 243
- 8.4 The Chinese Remainder Theorem 245
- 8.5 Discrete Logarithms 248
- 8.6 Recommended Reading and Web Site 252
- 8.7 Key Terms, Review Questions, and Problems 253

CHAPTER 9 PUBLIC-KEY CRYPTOGRAPHY AND RSA 257

- 9.1 Principles of Public-Key Cryptosystems 259
- 9.2 The RSA Algorithm 268
- 9.3 Recommended Reading and Web Site 278
- 9.4 Key Terms, Review Questions, and Problems 279
- Appendix 9A The Complexity of Algorithms 282

CHAPTER 10 KEY MANAGEMENT; OTHER PUBLIC-KEY CRYPTOSYSTEMS 285

- 10.1 Key Management 286
- 10.2 Diffie-Hellman Key Exchange 293
- 10.3 Elliptic Curve Arithmetic 297
- 10.4 Elliptic Curve Cryptography 304
- 10.5 Recommended Reading and Web Site 308
- 10.6 Key Terms, Review Questions, and Problems 308

CHAPTER 11 MESSAGE AUTHENTICATION AND HASH FUNCTIONS 311

- 11.1 Authentication Requirements 312
- 11.2 Authentication Functions 313
- 11.3 Message Authentication Codes 324
- 11.4 Hash Functions 328
- 11.5 Security of Hash Functions and MACs 335
- 11.6 Recommended Reading 338
- 11.7 Key Terms, Review Questions, and Problems 339
- Appendix 11A Mathematical Basis of the Birthday Attack 340

CHAPTER 12 HASH ALGORITHMS 347

- 12.1 MD5 Message Digest Algorithm 348
- 12.2 Secure Hash Algorithm 357
- 12.3 RIPEMD-160 365
- 12.4 HMAC 372
- 12.5 Recommended Reading and Web Sites 377
- 12.6 Key Terms, Review Questions, and Problems 377

**CHAPTER 13 DIGITAL SIGNATURES AND AUTHENTICATION
PROTOCOLS 379**

- 13.1 Digital Signatures 380
- 13.2 Authentication Protocols 384
- 13.3 Digital Signature Standard 392
- 13.4 Recommended Reading 395
- 13.5 Key Terms, Review Questions, and Problems 395

PART THREE NETWORK SECURITY PRACTICE 399

CHAPTER 14 AUTHENTICATION APPLICATIONS 401

- 14.1 Kerberos 402
- 14.2 X.509 Authentication Service 419
- 14.3 Recommended Reading and Web Sites 428
- 14.4 Key Terms, Review Questions, and Problems 429
- Appendix 14A Kerberos Encryption Techniques 431

CHAPTER 15 ELECTRONIC MAIL SECURITY 435

- 15.1 Pretty Good Privacy 436
- 15.2 S/MIME 455
- 15.3 Recommended Web Sites 472
- 15.4 Key Terms, Review Questions, and Problems 472
- Appendix 15A Data Compression Using ZIP 473
- Appendix 15B Radix-64 Conversion 476
- Appendix 15C PGP Random Number Generation 478

CHAPTER 16 IP SECURITY 481

- 16.1 IP Security Overview 482
- 16.2 IP Security Architecture 485
- 16.3 Authentication Header 491
- 16.4 Encapsulating Security Payload 496
- 16.5 Combining Security Associations 501
- 16.6 Key Management 504
- 16.7 Recommended Reading and Web Sites 515
- 16.8 Key Terms, Review Questions, and Problems 516
- Appendix 16A Internetworking and Internet Protocols 517

CHAPTER 17 WEB SECURITY 527

- 17.1 Web Security Considerations 528
- 17.2 Secure Sockets Layer and Transport Layer Security 531
- 17.3 Secure Electronic Transaction 548
- 17.4 Recommended Reading and Web Sites 560
- 17.5 Key Terms, Review Questions, and Problems 560

PART FOUR SYSTEM SECURITY 563**CHAPTER 18 INTRUDERS 565**

- 18.1 Intruders 566
- 18.2 Intrusion Detection 569
- 18.3 Password Management 581
- 18.4 Recommended Reading and Web Sites 591
- 18.5 Key Terms, Review Questions, and Problems 592
- Appendix 18A The Base-Rate Fallacy 594

CHAPTER 19 MALICIOUS SOFTWARE 597

- 19.1 Viruses and Related Threats 598
- 19.2 Virus Countermeasures 609
- 19.3 Recommended Reading and Web Site 613
- 19.4 Key Terms, Review Questions, and Problems 614

CHAPTER 20 FIREWALLS 615

- 20.1 Firewall Design Principles 616
- 20.2 Trusted Systems 628
- 20.3 Recommended Reading and Web Site 634
- 20.4 Key Terms, Review Questions, and Problems 634

APPENDICES**APPENDIX A STANDARDS AND STANDARDS-SETTING ORGANIZATIONS 637**

- A.1 The Importance of Standards 638
- A.2 Standards and Regulation 639
- A.3 Internet Standards and the Internet Society 640
- A.4 National Institute of Standards and Technology 634
- A.5 Standards and Specifications Cited in this Book 644

**APPENDIX B PROJECTS FOR TEACHING CRYPTOGRAPHY
AND NETWORK SECURITY 647**

- B.1 Research Projects 648
- B.2 Programming Projects 649
- B.3 Reading/Report Assignments 649

GLOSSARY 651

REFERENCES 657

INDEX 670