



International
Edition

Cryptography and Network Security

PRINCIPLES AND PRACTICE

Fifth Edition

William Stallings

PEARSON

CONTENTS

Notation 13

Preface 15

About the Author 23

Chapter 0 Reader's Guide 25

- 0.1 Outline of This Book 26
- 0.2 A Roadmap for Readers and Instructors 26
- 0.3 Internet and Web Resources 28
- 0.4 Standards 29

Chapter 1 Overview 31

- 1.1 Computer Security Concepts 33
- 1.2 The OSI Security Architecture 38
- 1.3 Security Attacks 39
- 1.4 Security Services 43
- 1.5 Security Mechanisms 47
- 1.6 A Model for Network Security 49
- 1.7 Recommended Reading and Web Sites 51
- 1.8 Key Terms, Review Questions, and Problems 53

PART ONE SYMMETRIC CIPHERS 55

Chapter 2 Classical Encryption Techniques 55

- 2.1 Symmetric Cipher Model 57
- 2.2 Substitution Techniques 62
- 2.3 Transposition Techniques 77
- 2.4 Rotor Machines 79
- 2.5 Steganography 81
- 2.6 Recommended Reading and Web Sites 83
- 2.7 Key Terms, Review Questions, and Problems 84

Chapter 3 Block Ciphers and the Data Encryption Standard 90

- 3.1 Block Cipher Principles 92
- 3.2 The Data Encryption Standard (DES) 101
- 3.3 A DES Example 109
- 3.4 The Strength of DES 112
- 3.5 Differential and Linear Cryptanalysis 113
- 3.6 Block Cipher Design Principles 116
- 3.7 Recommended Reading and Web Site 120
- 3.8 Key Terms, Review Questions, and Problems 121

Chapter 4 Basic Concepts in Number Theory and Finite Fields 125

- 4.1 Divisibility and the Division Algorithm 127
- 4.2 The Euclidean Algorithm 129

- 4.3 Modular Arithmetic 132
- 4.4 Groups, Rings, and Fields 140
- 4.5 Finite Fields of the Form $GF(p)$ 144
- 4.6 Polynomial Arithmetic 146
- 4.7 Finite Fields of the Form $GF(2^n)$ 153
- 4.8 Recommended Reading and Web Sites 165
- 4.9 Key Terms, Review Questions, and Problems 165
- Appendix 4A The Meaning of mod 168

Chapter 5 Advanced Encryption Standard 171

- 5.1 Finite Field Arithmetic 172
- 5.2 AES Structure 174
- 5.3 AES Transformation Functions 179
- 5.4 AES Key Expansion 190
- 5.5 An AES Example 193
- 5.6 AES Implementation 198
- 5.7 Recommended Reading and Web Sites 202
- 5.8 Key Terms, Review Questions, and Problems 203
- Appendix 5A Polynomials with Coefficients in $GF(2^8)$ 204
- Appendix 5B Simplified AES 207

Chapter 6 Block Cipher Operation 216

- 6.1 Multiple Encryption and Triple DES 217
- 6.2 Electronic Code Book 222
- 6.3 Cipher Block Chaining Mode 225
- 6.4 Cipher Feedback Mode 227
- 6.5 Output Feedback Mode 229
- 6.6 Counter Mode 230
- 6.7 XTS-AES Mode for Block-Oriented Storage Devices 234
- 6.8 Recommended Web Site 238
- 6.9 Key Terms, Review Questions, and Problems 238

Chapter 7 Pseudorandom Number Generation and Stream Ciphers 242

- 7.1 Principles of Pseudorandom Number Generation 243
- 7.2 Pseudorandom Number Generators 250
- 7.3 Pseudorandom Number Generation Using a Block Cipher 253
- 7.4 Stream Ciphers 256
- 7.5 RC4 258
- 7.6 True Random Number Generators 261
- 7.7 Recommended Reading and Web Sites 262
- 7.8 Key Terms, Review Questions, and Problems 263

PART TWO ASYMMETRIC CIPHERS 267

Chapter 8 Introduction to Number Theory 267

- 8.1 Prime Numbers 269
- 8.2 Fermat's and Euler's Theorems 272
- 8.3 Testing for Primality 275
- 8.4 The Chinese Remainder Theorem 278

- 8.5 Discrete Logarithms 281
- 8.6 Recommended Reading and Web Sites 286
- 8.7 Key Terms, Review Questions, and Problems 287

Chapter 9 Public-Key Cryptography and RSA 290

- 9.1 Principles of Public-Key Cryptosystems 293
- 9.2 The RSA Algorithm 301
- 9.3 Recommended Reading and Web Site 315
- 9.4 Key Terms, Review Questions, and Problems 315
- Appendix 9A Proof of the RSA Algorithm 320
- Appendix 9B The Complexity of Algorithms 321

Chapter 10 Other Public-Key Cryptosystems 324

- 10.1 Diffie-Hellman Key Exchange 325
- 10.2 ElGamal Cryptographic system 329
- 10.3 Elliptic Curve Arithmetic 332
- 10.4 Elliptic Curve Cryptography 341
- 10.5 Pseudorandom Number Generation Based on an Asymmetric Cipher 345
- 10.6 Recommended Reading and Web Site 347
- 10.7 Key Terms, Review Questions, and Problems 348

PART THREE CRYPTOGRAPHIC DATA INTEGRITY ALGORITHMS 351

Chapter 11 Cryptographic Hash Functions 351

- 11.1 Applications of Cryptographic Hash Functions 353
- 11.2 Two Simple Hash Functions 357
- 11.3 Requirements and Security 359
- 11.4 Hash Functions Based on Cipher Block Chaining 365
- 11.5 Secure Hash Algorithm (SHA) 366
- 11.6 SHA-3 376
- 11.7 Recommended Reading and Web Sites 377
- 11.8 Key Terms, Review Questions, and Problems 377
- Appendix 11A Mathematical Basis of the Birthday Attack 380

Chapter 12 Message Authentication Codes 386

- 12.1 Message Authentication Requirements 388
- 12.2 Message Authentication Functions 389
- 12.3 Requirements for Message Authentication Codes 396
- 12.4 Security of MACs 398
- 12.5 MACs Based on Hash Functions: HMAC 399
- 12.6 MACs Based on Block Ciphers: DAA and CMAC 404
- 12.7 Authenticated Encryption: CCM and GCM 407
- 12.8 Pseudorandom Number Generation Using Hash Functions and MACs 413
- 12.9 Recommended Reading and Web Site 416
- 12.10 Key Terms, Review Questions, and Problems 417

Chapter 13 Digital Signatures 419

- 13.1 Digital Signatures 420
- 13.2 ElGamal Digital Signature Scheme 424

- 13.3 Schnorr Digital Signature Scheme 426
- 13.4 Digital Signature Standard 427
- 13.5 Recommended Reading and Web Site 430
- 13.6 Key Terms, Review Questions, and Problems 431

PART FOUR MUTUAL TRUST 435

Chapter 14 Key Management and Distribution 435

- 14.1 Symmetric Key Distribution Using Symmetric Encryption 437
- 14.2 Symmetric Key Distribution Using Asymmetric Encryption 446
- 14.3 Distribution of Public Keys 448
- 14.4 X.509 Certificates 453
- 14.5 Public-Key Infrastructure 461
- 14.6 Recommended Reading and Web Sites 463
- 14.7 Key Terms, Review Questions, and Problems 464

Chapter 15 User Authentication 468

- 15.1 Remote User-Authentication Principles 469
- 15.2 Remote User-Authentication Using Symmetric Encryption 472
- 15.3 Kerberos 476
- 15.4 Remote User Authentication Using Asymmetric Encryption 494
- 15.5 Federated Identity Management 496
- 15.6 Recommended Reading and Web Sites 502
- 15.7 Key Terms, Review Questions, and Problems 503
- Appendix 15A Kerberos Encryption Techniques 505

PART FIVE NETWORK AND INTERNET SECURITY 509

Chapter 16 Transport-Level Security 509

- 16.1 Web Security Considerations 510
- 16.2 Secure Socket Layer and Transport Layer Security 513
- 16.3 Transport Layer Security 526
- 16.4 HTTPS 530
- 16.5 Secure Shell (SSH) 532
- 16.6 Recommended Reading and Web Sites 543
- 16.7 Key Terms, Review Questions, and Problems 543

Chapter 17 Wireless Network Security 545

- 17.1 IEEE 802.11 Wireless LAN Overview 547
- 17.2 IEEE 802.11i Wireless LAN Security 553
- 17.3 Wireless Application Protocol Overview 567
- 17.4 Wireless Transport Layer Security 574
- 17.5 WAP End-to-End Security 584
- 17.6 Recommended Reading and Web Sites 587
- 17.7 Key Terms, Review Questions, and Problems 588

Chapter 18 Electronic Mail Security 591

- 18.1 Pretty Good Privacy 592
- 18.2 S/MIME 611

- 18.3 DomainKeys Identified Mail 627
- 18.4 Recommended Reading and Web Sites 634
- 18.5 Key Terms, Review Questions, and Problems 635
- Appendix 18A Radix-64 Conversion 636

Chapter 19 IP Security 639

- 19.1 IP Security Overview 640
- 19.2 IP Security Policy 646
- 19.3 Encapsulating Security Payload 651
- 19.4 Combining Security Associations 658
- 19.5 Internet Key Exchange 662
- 19.6 Cryptographic Suites 671
- 19.7 Recommended Reading and Web Sites 672
- 19.8 Key Terms, Review Questions, and Problems 673

APPENDICES 675

Appendix A Projects for Teaching Cryptography and Network Security 675

- A.1 Sage Computer Algebra Projects 676
- A.2 Hacking Project 677
- A.3 Block Cipher Projects 677
- A.4 Laboratory Exercises 678
- A.5 Research Projects 678
- A.6 Programming Projects 679
- A.7 Practical Security Assessments 679
- A.8 Writing Assignments 679
- A.9 Reading/Report Assignments 680

Appendix B Sage Examples 681

- B.1 Linear Algebra and Matrix Functionality 682
- B.2 Chapter 2: Classical Encryption 683
- B.3 Chapter 3: Block Ciphers and the Data Encryption Standard 686
- B.4 Chapter 4: Basic Concepts in Number Theory and Finite Fields 690
- B.5 Chapter 5: Advanced Encryption Standard 697
- B.6 Chapter 6: Pseudorandom Number Generation and Stream Ciphers 702
- B.7 Chapter 8: Number Theory 704
- B.8 Chapter 9: Public-Key Cryptography and RSA 709
- B.9 Chapter 10: Other Public-Key Cryptosystems 712
- B.10 Chapter 11: Cryptographic Hash Functions 717
- B.11 Chapter 13: Digital Signatures 719

References 723

Index 735

ONLINE CHAPTERS

PART SIX SYSTEM SECURITY

Chapter 20 Intruders

- 20.1 Intruders
- 20.2 Intrusion Detection