

# CONTENTS

---

Notation xiii

Preface xv

About the Author xxiii

## **Chapter 0 Reader's Guide 1**

- 0.1 Outline of This Book 2
- 0.2 A Roadmap for Readers and Instructors 2
- 0.3 Internet and Web Resources 4
- 0.4 Standards 5

## **Chapter 1 Overview 7**

- 1.1 Computer Security Concepts 9
- 1.2 The OSI Security Architecture 14
- 1.3 Security Attacks 15
- 1.4 Security Services 19
- 1.5 Security Mechanisms 23
- 1.6 A Model for Network Security 25
- 1.7 Recommended Reading and Web Sites 27
- 1.8 Key Terms, Review Questions, and Problems 29

## **PART ONE SYMMETRIC CIPHERS 31**

### **Chapter 2 Classical Encryption Techniques 31**

- 2.1 Symmetric Cipher Model 33
- 2.2 Substitution Techniques 38
- 2.3 Transposition Techniques 53
- 2.4 Rotor Machines 55
- 2.5 Steganography 57
- 2.6 Recommended Reading and Web Sites 59
- 2.7 Key Terms, Review Questions, and Problems 60

### **Chapter 3 Block Ciphers and the Data Encryption Standard 66**

- 3.1 Block Cipher Principles 68
- 3.2 The Data Encryption Standard (DES) 77
- 3.3 A DES Example 85
- 3.4 The Strength of DES 88
- 3.5 Differential and Linear Cryptanalysis 89
- 3.6 Block Cipher Design Principles 92
- 3.7 Recommended Reading and Web Site 96
- 3.8 Key Terms, Review Questions, and Problems 97

### **Chapter 4 Basic Concepts in Number Theory and Finite Fields 101**

- 4.1 Divisibility and the Division Algorithm 103
- 4.2 The Euclidean Algorithm 105

- 4.3 Modular Arithmetic 108
- 4.4 Groups, Rings, and Fields 116
- 4.5 Finite Fields of the Form  $GF(p)$  120
- 4.6 Polynomial Arithmetic 122
- 4.7 Finite Fields of the Form  $GF(2^n)$  129
- 4.8 Recommended Reading and Web Sites 141
- 4.9 Key Terms, Review Questions, and Problems 141
- Appendix 4A The Meaning of mod 144

## **Chapter 5 Advanced Encryption Standard 47**

- 5.1 The Origins AES 148
- 5.2 AES Structure 150
- 5.3 AES Round Functions 155
- 5.4 AES Key Expansion 166
- 5.5 An AES Example 169
- 5.6 AES Implementation 174
- 5.7 Recommended Reading and Web Sites 178
- 5.8 Key Terms, Review Questions, and Problems 179
- Appendix 5A Polynomials with Coefficients in  $GF(2^8)$  180
- Appendix 5B Simplified AES 183

## **Chapter 6 Block Cipher Operation 192**

- 6.1 Multiple Encryption and Triple DES 193
- 6.2 Electronic Codebook Mode 198
- 6.3 Cipher Block Chaining Mode 201
- 6.4 Cipher Feedback Mode 203
- 6.5 Output Feedback Mode 205
- 6.6 Counter Mode 206
- 6.7 XTS Mode for Block-Oriented Storage Devices 210
- 6.8 Recommended Web Site 214
- 6.9 Key Terms, Review Questions, and Problems 214

## **Chapter 7 Pseudorandom Number Generation and Stream Ciphers 218**

- 7.1 Principles of Pseudorandom Number Generation 219
- 7.2 Pseudorandom Number Generators 226
- 7.3 Pseudorandom Number Generation Using a Block Cipher 229
- 7.4 Stream Ciphers 232
- 7.5 RC4 234
- 7.6 True Random Numbers 237
- 7.7 Recommended Reading 238
- 7.8 Key Terms, Review Questions, and Problems 239

## **PART TWO ASYMMETRIC CIPHERS 243**

### **Chapter 8 More Number Theory 243**

- 8.1 Prime Numbers 245
- 8.2 Fermat's and Euler's Theorems 248
- 8.3 Testing for Primality 251
- 8.4 The Chinese Remainder Theorem 254

- 8.5 Discrete Logarithms 257
- 8.6 Recommended Reading and Web Sites 262
- 8.7 Key Terms, Review Questions, and Problems 263

## **Chapter 9 Public-Key Cryptography and RSA 266**

- 9.1 Principles of Public-Key Cryptosystems 269
- 9.2 The RSA Algorithm 277
- 9.3 Recommended Reading and Web Sites 291
- 9.4 Key Terms, Review Questions, and Problems 291
- Appendix 9A Proof of the RSA Algorithm 296
- Appendix 9B The Complexity of Algorithms 297

## **Chapter 10 Other Public-Key Cryptosystems 300**

- 10.1 Diffie-Hellman Key Exchange 301
- 10.2 ElGamal Cryptosystem 305
- 10.3 Elliptic Curve Arithmetic 308
- 10.4 Elliptic Curve Cryptography 317
- 10.5 Pseudorandom Number Generation Based on an Asymmetric Cipher 321
- 10.6 Recommended Reading and Web Sites 323
- 10.7 Key Terms, Review Questions, and Problems 324

## **PART THREE CRYPTOGRAPHIC DATA INTEGRITY ALGORITHMS 327**

### **Chapter 11 Cryptographic Hash Functions 327**

- 11.1 Applications of Cryptographic Hash Functions 329
- 11.2 Two Simple Hash Functions 333
- 11.3 Requirements and Security 335
- 11.4 Hash Functions Based on Cipher Block Chaining 341
- 11.5 Secure Hash Algorithm (SHA) 342
- 11.6 SHA-3 352
- 11.7 Recommended Reading and Web Sites 353
- 11.8 Key Terms, Review Questions, and Problems 353
- Appendix 11A Mathematical Basis of Birthday Attack 356

### **Chapter 12 Message Authentication Codes 362**

- 12.1 Message Authentication Requirements 364
- 12.2 Message Authentication Functions 365
- 12.3 Message Authentication Codes 372
- 12.4 Security of MACs 374
- 12.5 MACs Based on Hash Functions: HMAC 375
- 12.6 MACs Based on Block Ciphers: DAA and CMAC 380
- 12.7 Authenticated Encryption: CCM and GCM 383
- 12.8 Pseudorandom Number Generation Using Hash Functions and MACs 389
- 12.9 Recommended Reading 392
- 12.10 Key Terms, Review Questions, and Problems 393

### **Chapter 13 Digital Signatures 395**

- 13.1 Digital Signatures 396
- 13.2 ElGamal Digital Signature Scheme 400

- 13.3 Schnorr Digital Signature Scheme 402
- 13.4 Digital Signature Standard (DSS) 403
- 13.5 Recommended Reading and Web Sites 406
- 13.6 Key Terms, Review Questions, and Problems 407

## **PART FOUR MUTUAL TRUST 410**

### **Chapter 14 Key Management and Distribution 410**

- 14.1 Symmetric Key Distribution Using Symmetric Encryption 412
- 14.2 Symmetric Key Distribution Using Asymmetric Encryption 421
- 14.3 Distribution of Public Keys 423
- 14.4 X.509 Certificates 428
- 14.5 Public Key Infrastructure 436
- 14.6 Recommended Reading and Web Sites 438
- 14.7 Key Terms, Review Questions, and Problems 439

### **Chapter 15 User Authentication Protocols 444**

- 15.1 Remote User Authentication Principles 445
  - 15.2 Remote User Authentication Using Symmetric Encryption 448
  - 15.3 Kerberos 452
  - 15.4 Remote User Authentication Using Asymmetric Encryption 470
  - 15.5 Federated Identity Management 472
  - 15.6 Recommended Reading and Web Sites 478
  - 15.7 Key Terms, Review Questions, and Problems 479
- Appendix 15A Kerberos Encryption Techniques 481

## **PART FIVE NETWORK AND INTERNET SECURITY 485**

### **Chapter 16 Transport-Level Security 485**

- 16.1 Web Security Issues 486
- 16.2 Secure Sockets Layer (SSL) 489
- 16.3 Transport Layer Security (TLS) 502
- 16.4 HTTPS 506
- 16.5 Secure Shell (SSH) 508
- 16.6 Recommended Reading and Web Sites 519
- 16.7 Key Terms, Review Questions, and Problems 519

### **Chapter 17 Wireless Network Security 521**

- 17.1 IEEE 802.11 Wireless LAN Overview 523
- 17.2 IEEE 802.11i Wireless LAN Security 529
- 17.3 Wireless Application Protocol Overview 543
- 17.4 Wireless Transport Layer Security 550
- 17.5 WAP End-to-End Security 560
- 17.6 Recommended Reading and Web Sites 563
- 17.7 Key Terms, Review Questions, and Problems 563

### **Chapter 18 Electronic Mail Security 567**

- 18.1 Pretty Good Privacy (PGP) 568
- 18.2 S/MIME 587

- 18.3 DomainKeys Identified Mail (DKIM) 603
- 18.4 Recommended Web Sites 610
- 18.5 Key Terms, Review Questions, and Problems 611
- Appendix 18A Radix-64 Conversion 612

## **Chapter 19 IP Security 615**

- 19.1 IP Security Overview 616
- 19.2 IP Security Policy 622
- 19.3 Encapsulating Security Payload 627
- 19.4 Combining Security Associations 634
- 19.5 Internet Key Exchange 638
- 19.6 Cryptographic Suites 647
- 19.7 Recommended Reading and Web Sites 648
- 19.8 Key Terms, Review Questions, and Problems 649

## **APPENDICES 651**

### **Appendix A Projects for Teaching Cryptography and Network Security 651**

- A.1 Sage Computer Algebra Projects 652
- A.2 Hacking Project 653
- A.3 Block Cipher Projects 653
- A.4 Laboratory Exercises 654
- A.5 Research Projects 654
- A.6 Programming Projects 655
- A.7 Practical Security Assessments 655
- A.8 Writing Assignments 655
- A.9 Reading/Report Assignments 656

### **Appendix B Sage Examples 657**

- B.1 Chapter 2: Classical Encryption Techniques 659
- B.2 Chapter 3: Block Ciphers and the Data Encryption Standard 662
- B.3 Chapter 4: Basic Concepts in Number Theory and Finite Fields 666
- B.4 Chapter 5: Advanced Encryption Standard 673
- B.5 Chapter 6: Pseudorandom Number Generation and Stream Ciphers 678
- B.6 Chapter 8: Number Theory 680
- B.6 Chapter 9: Public-Key Cryptography and RSA 685
- B.7 Chapter 10: Other Public-Key Cryptosystems 688
- B.8 Chapter 11: Cryptographic Hash Functions 693
- B.9 Chapter 13: Digital Signatures 695

### **References 699**

### **Index 711**

## **ONLINE CHAPTERS**

## **PART SIX SYSTEM SECURITY**

### **Chapter 20 Intruders**

- 20.1 Intruders
- 20.2 Intrusion Detection