

**CRYPTOGRAPHY AND
NETWORK SECURITY**
PRINCIPLES AND PRACTICE
SEVENTH EDITION
GLOBAL EDITION

William Stallings

PEARSON

Boston Columbus Indianapolis New York San Francisco Hoboken
Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montréal Toronto
Delhi Mexico City São Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

CONTENTS

Notation 10

Preface 12

About the Author 18

PART ONE: BACKGROUND 19

Chapter 1 Computer and Network Security Concepts 19

- 1.1 Computer Security Concepts 21
- 1.2 The OSI Security Architecture 26
- 1.3 Security Attacks 27
- 1.4 Security Services 29
- 1.5 Security Mechanisms 32
- 1.6 Fundamental Security Design Principles 34
- 1.7 Attack Surfaces and Attack Trees 37
- 1.8 A Model for Network Security 41
- 1.9 Standards 43
- 1.10 Key Terms, Review Questions, and Problems 44

Chapter 2 Introduction to Number Theory 46

- 2.1 Divisibility and the Division Algorithm 47
- 2.2 The Euclidean Algorithm 49
- 2.3 Modular Arithmetic 53
- 2.4 Prime Numbers 61
- 2.5 Fermat's and Euler's Theorems 64
- 2.6 Testing for Primality 68
- 2.7 The Chinese Remainder Theorem 71
- 2.8 Discrete Logarithms 73
- 2.9 Key Terms, Review Questions, and Problems 78
- Appendix 2A The Meaning of Mod 82

PART TWO: SYMMETRIC CIPHERS 85

Chapter 3 Classical Encryption Techniques 85

- 3.1 Symmetric Cipher Model 86
- 3.2 Substitution Techniques 92
- 3.3 Transposition Techniques 107
- 3.4 Rotor Machines 108
- 3.5 Steganography 110
- 3.6 Key Terms, Review Questions, and Problems 112

Chapter 4 Block Ciphers and the Data Encryption Standard 118

- 4.1 Traditional Block Cipher Structure 119
- 4.2 The Data Encryption Standard 129
- 4.3 A DES Example 131
- 4.4 The Strength of DES 134

4 CONTENTS

| | | |
|---|--|------------|
| 4.5 | Block Cipher Design Principles | 135 |
| 4.6 | Key Terms, Review Questions, and Problems | 137 |
| Chapter 5 | Finite Fields | 141 |
| 5.1 | Groups | 143 |
| 5.2 | Rings | 145 |
| 5.3 | Fields | 146 |
| 5.4 | Finite Fields of the Form $GF(p)$ | 147 |
| 5.5 | Polynomial Arithmetic | 151 |
| 5.6 | Finite Fields of the Form $GF(2^n)$ | 157 |
| 5.7 | Key Terms, Review Questions, and Problems | 169 |
| Chapter 6 | Advanced Encryption Standard | 171 |
| 6.1 | Finite Field Arithmetic | 172 |
| 6.2 | AES Structure | 174 |
| 6.3 | AES Transformation Functions | 179 |
| 6.4 | AES Key Expansion | 190 |
| 6.5 | An AES Example | 193 |
| 6.6 | AES Implementation | 197 |
| 6.7 | Key Terms, Review Questions, and Problems | 202 |
| | Appendix 6A Polynomials with Coefficients in $GF(2^8)$ | 203 |
| Chapter 7 | Block Cipher Operation | 207 |
| 7.1 | Multiple Encryption and Triple DES | 208 |
| 7.2 | Electronic Codebook | 213 |
| 7.3 | Cipher Block Chaining Mode | 216 |
| 7.4 | Cipher Feedback Mode | 218 |
| 7.5 | Output Feedback Mode | 220 |
| 7.6 | Counter Mode | 222 |
| 7.7 | XTS-AES Mode for Block-Oriented Storage Devices | 224 |
| 7.8 | Format-Preserving Encryption | 231 |
| 7.9 | Key Terms, Review Questions, and Problems | 245 |
| Chapter 8 | Random Bit Generation and Stream Ciphers | 250 |
| 8.1 | Principles of Pseudorandom Number Generation | 252 |
| 8.2 | Pseudorandom Number Generators | 258 |
| 8.3 | Pseudorandom Number Generation Using a Block Cipher | 261 |
| 8.4 | Stream Ciphers | 267 |
| 8.5 | RC4 | 269 |
| 8.6 | True Random Number Generators | 271 |
| 8.7 | Key Terms, Review Questions, and Problems | 280 |
| PART THREE: ASYMMETRIC CIPHERS 283 | | |
| Chapter 9 | Public-Key Cryptography and RSA | 283 |
| 9.1 | Principles of Public-Key Cryptosystems | 285 |
| 9.2 | The RSA Algorithm | 294 |
| 9.3 | Key Terms, Review Questions, and Problems | 308 |

Chapter 10 Other Public-Key Cryptosystems 313

- 10.1** Diffie–Hellman Key Exchange 314
- 10.2** Elgamal Cryptographic System 318
- 10.3** Elliptic Curve Arithmetic 321
- 10.4** Elliptic Curve Cryptography 330
- 10.5** Pseudorandom Number Generation Based on an Asymmetric Cipher 334
- 10.6** Key Terms, Review Questions, and Problems 336

PART FOUR: CRYPTOGRAPHIC DATA INTEGRITY ALGORITHMS 339**Chapter 11 Cryptographic Hash Functions 339**

- 11.1** Applications of Cryptographic Hash Functions 341
- 11.2** Two Simple Hash Functions 346
- 11.3** Requirements and Security 348
- 11.4** Hash Functions Based on Cipher Block Chaining 354
- 11.5** Secure Hash Algorithm (SHA) 355
- 11.6** SHA-3 365
- 11.7** Key Terms, Review Questions, and Problems 377

Chapter 12 Message Authentication Codes 381

- 12.1** Message Authentication Requirements 382
- 12.2** Message Authentication Functions 383
- 12.3** Requirements for Message Authentication Codes 391
- 12.4** Security of MACs 393
- 12.5** MACs Based on Hash Functions: HMAC 394
- 12.6** MACs Based on Block Ciphers: DAA and CMAC 399
- 12.7** Authenticated Encryption: CCM and GCM 402
- 12.8** Key Wrapping 408
- 12.9** Pseudorandom Number Generation Using Hash Functions and MACs 413
- 12.10** Key Terms, Review Questions, and Problems 416

Chapter 13 Digital Signatures 419

- 13.1** Digital Signatures 421
- 13.2** Elgamal Digital Signature Scheme 424
- 13.3** Schnorr Digital Signature Scheme 425
- 13.4** NIST Digital Signature Algorithm 426
- 13.5** Elliptic Curve Digital Signature Algorithm 430
- 13.6** RSA-PSS Digital Signature Algorithm 433
- 13.7** Key Terms, Review Questions, and Problems 438

PART FIVE: MUTUAL TRUST 441**Chapter 14 Key Management and Distribution 441**

- 14.1** Symmetric Key Distribution Using Symmetric Encryption 442
- 14.2** Symmetric Key Distribution Using Asymmetric Encryption 451
- 14.3** Distribution of Public Keys 454
- 14.4** X.509 Certificates 459

6 CONTENTS

- 14.5 Public-Key Infrastructure 467
- 14.6 Key Terms, Review Questions, and Problems 469

Chapter 15 User Authentication 473

- 15.1 Remote User-Authentication Principles 474
- 15.2 Remote User-Authentication Using Symmetric Encryption 478
- 15.3 Kerberos 482
- 15.4 Remote User-Authentication Using Asymmetric Encryption 500
- 15.5 Federated Identity Management 502
- 15.6 Personal Identity Verification 508
- 15.7 Key Terms, Review Questions, and Problems 515

PART SIX: NETWORK AND INTERNET SECURITY 519

Chapter 16 Network Access Control and Cloud Security 519

- 16.1 Network Access Control 520
- 16.2 Extensible Authentication Protocol 523
- 16.3 IEEE 802.1X Port-Based Network Access Control 527
- 16.4 Cloud Computing 529
- 16.5 Cloud Security Risks and Countermeasures 535
- 16.6 Data Protection in the Cloud 537
- 16.7 Cloud Security as a Service 541
- 16.8 Addressing Cloud Computing Security Concerns 544
- 16.9 Key Terms, Review Questions, and Problems 545

Chapter 17 Transport-Level Security 546

- 17.1 Web Security Considerations 547
- 17.2 Transport Layer Security 549
- 17.3 HTTPS 566
- 17.4 Secure Shell (SSH) 567
- 17.5 Key Terms, Review Questions, and Problems 579

Chapter 18 Wireless Network Security 581

- 18.1 Wireless Security 582
- 18.2 Mobile Device Security 585
- 18.3 IEEE 802.11 Wireless LAN Overview 589
- 18.4 IEEE 802.11i Wireless LAN Security 595
- 18.5 Key Terms, Review Questions, and Problems 610

Chapter 19 Electronic Mail Security 612

- 19.1 Internet Mail Architecture 613
- 19.2 Email Formats 617
- 19.3 Email Threats and Comprehensive Email Security 625
- 19.4 S/MIME 627
- 19.5 Pretty Good Privacy 638
- 19.6 DNSSEC 639
- 19.7 DNS-Based Authentication of Named Entities 643
- 19.8 Sender Policy Framework 645
- 19.9 DomainKeys Identified Mail 648

| | | |
|---|---|-----|
| 19.10 | Domain-Based Message Authentication, Reporting, and Conformance | 654 |
| 19.11 | Key Terms, Review Questions, and Problems | 659 |
| Chapter 20 IP Security 661 | | |
| 20.1 | IP Security Overview | 662 |
| 20.2 | IP Security Policy | 668 |
| 20.3 | Encapsulating Security Payload | 673 |
| 20.4 | Combining Security Associations | 681 |
| 20.5 | Internet Key Exchange | 684 |
| 20.6 | Cryptographic Suites | 692 |
| 20.7 | Key Terms, Review Questions, and Problems | 694 |
| APPENDICES 696 | | |
| Appendix A Projects for Teaching Cryptography and Network Security 696 | | |
| A.1 | Sage Computer Algebra Projects | 697 |
| A.2 | Hacking Project | 698 |
| A.3 | Block Cipher Projects | 699 |
| A.4 | Laboratory Exercises | 699 |
| A.5 | Research Projects | 699 |
| A.6 | Programming Projects | 700 |
| A.7 | Practical Security Assessments | 700 |
| A.8 | Firewall Projects | 701 |
| A.9 | Case Studies | 701 |
| A.10 | Writing Assignments | 701 |
| A.11 | Reading/Report Assignments | 702 |
| A.12 | Discussion Topics | 702 |
| Appendix B Sage Examples 703 | | |
| B.1 | Linear Algebra and Matrix Functionality | 704 |
| B.2 | Chapter 2: Number Theory | 705 |
| B.3 | Chapter 3: Classical Encryption | 710 |
| B.4 | Chapter 4: Block Ciphers and the Data Encryption Standard | 713 |
| B.5 | Chapter 5: Basic Concepts in Number Theory and Finite Fields | 717 |
| B.6 | Chapter 6: Advanced Encryption Standard | 724 |
| B.7 | Chapter 8: Pseudorandom Number Generation and Stream Ciphers | 729 |
| B.8 | Chapter 9: Public-Key Cryptography and RSA | 731 |
| B.9 | Chapter 10: Other Public-Key Cryptosystems | 734 |
| B.10 | Chapter 11: Cryptographic Hash Functions | 739 |
| B.11 | Chapter 13: Digital Signatures | 741 |
| References 744 | | |
| Credits 753 | | |
| Index 754 | | |