CONTENTS

Notation 11

Preface 13

Chapter 0 Guide for Readers and Instructors 21

0.1 Outline of This Book 22
0.2 A Roadmap for Readers and Instructors 23
0.3 Internet and Web Resources 24
0.4 Standards 25

Chapter 1 Overview 27

1.1 Computer Security Concepts 29
1.2 The OSI Security Architecture 34
1.3 Security Attacks 35
1.4 Security Services 37
1.5 Security Mechanisms 40
1.6 A Model for Network Security 42
1.7 Recommended Reading 44
1.8 Key Terms, Review Questions, and Problems 45

PART ONE SYMMETRIC CIPHERS 47

Chapter 2 Classical Encryption Techniques 47

2.1 Symmetric Cipher Model 48
2.2 Substitution Techniques 54
2.3 Transposition Techniques 69
2.4 Rotor Machines 70
2.5 Steganography 72
2.6 Recommended Reading 74
2.7 Key Terms, Review Questions, and Problems 75

Chapter 3 Block Ciphers and the Data Encryption Standard 81

3.1 Traditional Block Cipher Structure 83
3.2 The Data Encryption Standard 92
3.3 A DES Example 94
3.4 The Strength of DES 97
3.5 Block Cipher Design Principles 98
3.6 Recommended Reading 100
3.7 Key Terms, Review Questions, and Problems 101

Chapter 4 Basic Concepts in Number Theory and Finite Fields 105

4.1 Divisibility and the Division Algorithm 107
4.2 The Euclidean Algorithm 108

4.3 Modular Arithmetic 111
4.4 Groups, Rings, and Fields 119
4.5 Finite Fields of the Form GF(p) 122
4.6 Polynomial Arithmetic 126
4.7 Finite Fields of the Form GF(2^n) 132
4.8 Recommended Reading 144
4.9 Key Terms, Review Questions, and Problems 144
Appendix 4A The Meaning of mod 147

Chapter 5 Advanced Encryption Standard 149

5.1 Finite Field Arithmetic 150
5.2 AES Structure 152
5.3 AES Transformation Functions 157
5.4 AES Key Expansion 168
5.5 An AES Example 171
5.6 AES Implementation 175
5.7 Recommended Reading 179
5.8 Key Terms, Review Questions, and Problems 180
Appendix 5A Polynomials with Coefficients in GF(2^8) 182
Appendix 5B Simplified AES 184

Chapter 6 Block Cipher Operation 194

6.1 Multiple Encryption and Triple DES 195
6.2 Electronic Code book 200
6.3 Cipher Block Chaining Mode 203
6.4 Cipher Feedback Mode 205
6.5 Output Feedback Mode 207
6.6 Counter Mode 209
6.7 XTS-AES Mode for Block-Oriented Storage Devices 211
6.8 Recommended Reading 218
6.9 Key Terms, Review Questions, and Problems 218

Chapter 7 Pseudorandom Number Generation and Stream Ciphers 222

7.1 Principles of Pseudorandom Number Generation 223
7.2 Pseudorandom Number Generators 230
7.3 Pseudorandom Number Generation Using a Block Cipher 233
7.4 Stream Ciphers 239
7.5 RC4 241
7.6 True Random Number Generators 243
7.7 Recommended Reading 247
7.8 Key Terms, Review Questions, and Problems 248

PART TWO ASYMMETRIC CIPHERS 251

Chapter 8 More Number Theory 251

8.1 Prime Numbers 252
8.2 Fermat's and Euler's Theorems 256
8.3 Testing for Primality 259
8.4 The Chinese Remainder Theorem 262

8.5 Discrete Logarithms 264
8.6 Recommended Reading 269
8.7 Key Terms, Review Questions, and Problems 270

Chapter 9 Public-Key Cryptography and RSA 273
9.1 Principles of Public-Key Cryptosystems 276
9.2 The RSA Algorithm 284
9.3 Recommended Reading 298
9.4 Key Terms, Review Questions, and Problems 299
Appendix 9A The Complexity of Algorithms 303

Chapter 10 Other Public-Key Cryptosystems 306
10.1 Diffie-Hellman Key Exchange 307
10.2 Elgamal Cryptographic System 312
10.3 Elliptic Curve Arithmetic 315
10.4 Elliptic Curve Cryptography 323
10.5 Pseudorandom Number Generation Based on an Asymmetric Cipher 326
10.6 Recommended Reading 329
10.7 Key Terms, Review Questions, and Problems 329

PART THREE CRYPTOGRAPHIC DATA INTEGRITY ALGORITHMS 333

Chapter 11 Cryptographic Hash Functions 333
11.1 Applications of Cryptographic Hash Functions 335
11.2 Two Simple Hash Functions 340
11.3 Requirements and Security 342
11.4 Hash Functions Based on Cipher Block Chaining 348
11.5 Secure Hash Algorithm (SHA) 349
11.6 SHA-3 359
11.7 Recommended Reading 371
11.8 Key Terms, Review Questions, and Problems 371

Chapter 12 Message Authentication Codes 375
12.1 Message Authentication Requirements 377
12.2 Message Authentication Functions 377
12.3 Requirements for Message Authentication Codes 385
12.4 Security of MACs 387
12.5 MACs Based on Hash Functions: HMAC 388
12.6 MACs Based on Block Ciphers: DAA and CMAC 393
12.7 Authenticated Encryption: CCM and GCM 396
12.8 Key Wrapping 402
12.9 Pseudorandom Number Generation using Hash Functions and MACs 407
12.10 Recommended Reading 410
12.11 Key Terms, Review Questions, and Problems 410

Chapter 13 Digital Signatures 413
13.1 Digital Signatures 415
13.2 Elgamal Digital Signature Scheme 418
13.3 Schnorr Digital Signature Scheme 420

13.4 NIST Digital Signature Algorithm 421
13.5 Elliptic Curve Digital Signature Algorithm 424
13.6 RSA-PSS Digital Signature Algorithm 427
13.7 Recommended Reading 432
13.8 Key Terms, Review Questions, and Problems 432

PART FOUR MUTUAL TRUST 437

Chapter 14 Key Management and Distribution 437

14.1 Symmetric Key Distribution Using Symmetric Encryption 438
14.2 Symmetric Key Distribution Using Asymmetric Encryption 447
14.3 Distribution of Public Keys 450
14.4 X.509 Certificates 455
14.5 Public-Key Infrastructure 463
14.6 Recommended Reading 465
14.7 Key Terms, Review Questions, and Problems 466

Chapter 15 User Authentication 470

15.1 Remote User-Authentication Principles 471
15.2 Remote User-Authentication Using Symmetric Encryption 474
15.3 Kerberos 478
15.4 Remote User Authentication Using Asymmetric Encryption 496
15.5 Federated Identity Management 498
15.6 Personal Identity Verification 504
15.7 Recommended Reading 511
15.8 Key Terms, Review Questions, and Problems 511

PART FIVE NETWORK AND INTERNET SECURITY 515

Chapter 16 Network Access Control and Cloud Security 515

16.1 Network Access Control 516
16.2 Extensible Authentication Protocol 519
16.3 IEEE 802.1X Port-Based Network Access Control 523
16.4 Cloud Computing 525
16.5 Cloud Security Risks and Countermeasures 532
16.6 Data Protection in the Cloud 534
16.7 Cloud Security as a Service 537
16.8 Recommended Reading 540
16.9 Key Terms, Review Questions, and Problems 541

Chapter 17 Transport-Level Security 542

17.1 Web Security Considerations 543
17.2 Secure Sockets Layer 545
17.3 Transport Layer Security 559
17.4 HTTPS 563
17.5 Secure Shell (SSH) 564
17.6 Recommended Reading 575
17.7 Key Terms, Review Questions, and Problems 576

Chapter 18 Wireless Network Security 578

18.1 Wireless Security 579
18.2 Mobile Device Security 582
18.3 IEEE 802.11 Wireless LAN Overview 586
18.4 IEEE 802.11i Wireless LAN Security 592
18.5 Recommended Reading 606
18.6 Key Terms, Review Questions, and Problems 607

Chapter 19 Electronic Mail Security 610

19.1 Pretty Good Privacy 611
19.2 S/MIME 619
19.3 DomainKeys Identified Mail 635
19.4 Recommended Reading 642
19.5 Key Terms, Review Questions, and Problems 642
Appendix 19A Radix-64 Conversion 643

Chapter 20 IP Security 646

20.1 IP Security Overview 648
20.2 IP Security Policy 652
20.3 Encapsulating Security Payload 658
20.4 Combining Security Associations 665
20.5 Internet Key Exchange 669
20.6 Cryptographic Suites 677
20.7 Recommended Reading 679
20.8 Key Terms, Review Questions, and Problems 679

APPENDICES 681

Appendix A Projects for Teaching Cryptography and Network Security 681

A.1 Sage Computer Algebra Projects 682
A.2 Hacking Project 683
A.3 Block Cipher Projects 684
A.4 Laboratory Exercises 684
A.5 Research Projects 684
A.6 Programming Projects 685
A.7 Practical Security Assessments 685
A.8 Firewall Projects 686
A.9 Case Studies 686
A.10 Writing Assignments 686
A.11 Reading/Report Assignments 687
A.12 Discussion Topics 687

Appendix B Sage Examples 688

B.1 Linear Algebra and Matrix Functionality 689
B.2 Chapter 2: Classical Encryption 680
B.3 Chapter 3: Block Ciphers and the Data Encryption Standard 693
B.4 Chapter 4: Basic Concepts in Number Theory and Finite Fields 697
B.5 Chapter 5: Advanced Encryption Standard 704

B.6 Chapter 6: Pseudorandom Number Generation and Stream Ciphers 709
B.7 Chapter 8: Number Theory 701
B.8 Chapter 9: Public-Key Cryptography and RSA 716
B.9 Chapter 10: Other Public-Key Cryptosystems 719
B.10 Chapter 11: Cryptographic Hash Functions 724
B.11 Chapter 13: Digital Signatures 726

References 730

Credits 740

Index 743

ONLINE CHAPTERS AND APPENDICES[1]

PART SIX SYSTEM SECURITY

Chapter 21 Malicious Software

21.1 Types of Malicious Software
21.2 Propagation – Infected Content - Viruses
21.3 Propagation – Vulnerability Exploit - Worms
21.4 Propagation – Social Engineering – SPAM, Trojans
21.5 Payload – System Corruption
21.6 Payload – Attack Agent – Zombie, Bots
21.7 Payload – Information Theft – Keyloggers, Phishing, Spyware
21.8 Payload – Stealthing – Backdoors, Rootkits
21.9 Countermeasures
21.10 Distributed Denial of Service Attacks
21.11 Recommended Reading
21.12 Key Terms, Review Questions, and Problems

Chapter 22 Intruders

22.1 Intruders
22.2 Intrusion Detection
22.3 Password Management
22.4 Recommended Reading
22.5 Key Terms, Review Questions, and Problems
Appendix 22A The Base-Rate Fallacy

Chapter 23 Firewalls

23.1 The Need for Firewalls
23.2 Firewall Characteristics
23.3 Types of Firewalls
23.4 Firewall Basing
23.5 Firewall Location and Configurations
23.6 Recommended Reading
23.7 Key Terms, Review Questions, and Problems

[1] Online chapters, appendices, and other documents are Premium Content, available via the access card at the front of this book.

PART SEVEN LEGAL AND ETHICAL ISSUES

Chapter 24 Legal and Ethical Issues

24.1 Cybercrime and Computer Crime
24.2 Intellectual Property
24.3 Privacy
24.4 Ethical Issues
24.5 Recommended Reading
24.6 Key Terms, Review Questions, and Problems

Appendix C Sage Exercises

Appendix D Standards and Standards-Setting Organizations

Appendix E Basic Concepts from Linear Algebra

Appendix F Measures of Security and Secrecy

Appendix G Simplified DES

Appendix H Evaluation Criteria for AES

Appendix I More on Simplified AES

Appendix J Knapsack Public-Key Algorithm

Appendix K Proof of the Digital Signature Algorithm

Appendix L TCP/IP and OSI

Appendix M Java Cryptographic APIs

Appendix N MD5 and Whirlpool Hash Functions

Appendix O Data Compression Using ZIP

Appendix P More on PGP

Appendix Q The International Reference Alphabet

Appendix R Proof of the RSA Algorithm

Appendix S Data Encryption Standard (DES)

Appendix T Kerberos Encryption Techniques

Appendix U Mathematical Basis of the Birthday Attack

Appendix V Evaluation Criteria for SHA-3

Glossary