

CONTENTS

Notation 10

Preface 12

About the Author 19

PART ONE: BACKGROUND 21

Chapter 1 Information and Network Security Concepts 21

- 1.1** Cybersecurity, Information Security, and Network Security 23
- 1.2** The OSI Security Architecture 26
- 1.3** Security Attacks 27
- 1.4** Security Services 30
- 1.5** Security Mechanisms 33
- 1.6** Cryptography 33
- 1.7** Network Security 36
- 1.8** Trust and Trustworthiness 37
- 1.9** Standards 41
- 1.10** Key Terms, Review Questions, and Problems 42

Chapter 2 Introduction to Number Theory 44

- 2.1** Divisibility and the Division Algorithm 45
 - 2.2** The Euclidean Algorithm 47
 - 2.3** Modular Arithmetic 51
 - 2.4** Prime Numbers 59
 - 2.5** Fermat's and Euler's Theorems 62
 - 2.6** Testing for Primality 66
 - 2.7** The Chinese Remainder Theorem 69
 - 2.8** Discrete Logarithms 71
 - 2.9** Key Terms, Review Questions, and Problems 76
- Appendix 2A The Meaning of Mod 80

PART TWO: SYMMETRIC CIPHERS 83

Chapter 3 Classical Encryption Techniques 83

- 3.1** Symmetric Cipher Model 84
- 3.2** Substitution Techniques 90
- 3.3** Transposition Techniques 105
- 3.4** Key Terms, Review Questions, and Problems 106

Chapter 4 Block Ciphers and the Data Encryption Standard 112

- 4.1** Traditional Block Cipher Structure 113
- 4.2** The Data Encryption Standard 123
- 4.3** A DES Example 125
- 4.4** The Strength of DES 128

6 CONTENTS

4.5	Block Cipher Design Principles	129
4.6	Key Terms, Review Questions, and Problems	131
Chapter 5	Finite Fields	135
5.1	Groups	137
5.2	Rings	139
5.3	Fields	140
5.4	Finite Fields of the Form $GF(p)$	141
5.5	Polynomial Arithmetic	145
5.6	Finite Fields of the Form $GF(2^n)$	151
5.7	Key Terms, Review Questions, and Problems	163
Chapter 6	Advanced Encryption Standard	165
6.1	Finite Field Arithmetic	167
6.2	AES Structure	168
6.3	AES Transformation Functions	174
6.4	AES Key Expansion	184
6.5	An AES Example	187
6.6	AES Implementation	191
6.7	Key Terms, Review Questions, and Problems	196
	Appendix 6A Polynomials with Coefficients in $GF(2^8)$	197
Chapter 7	Block Cipher Operation	201
7.1	Multiple Encryption and Triple DES	202
7.2	Electronic CodeBook	207
7.3	Cipher Block Chaining Mode	210
7.4	Cipher Feedback Mode	212
7.5	Output Feedback Mode	214
7.6	Counter Mode	216
7.7	XTS-AES Mode for Block-Oriented Storage Devices	218
7.8	Format-Preserving Encryption	225
7.9	Key Terms, Review Questions, and Problems	239
Chapter 8	Random Bit Generation and Stream Ciphers	244
8.1	Principles of Pseudorandom Number Generation	246
8.2	Pseudorandom Number Generators	252
8.3	Pseudorandom Number Generation Using a Block Cipher	255
8.4	Stream Ciphers	260
8.5	RC4	262
8.6	Stream Ciphers Using Feedback Shift Registers	264
8.7	True Random Number Generators	272
8.8	Key Terms, Review Questions, and Problems	281
PART THREE: ASYMMETRIC CIPHERS 285		
Chapter 9	Public-Key Cryptography and RSA	285
9.1	Principles of Public-Key Cryptosystems	287
9.2	The RSA Algorithm	296
9.3	Key Terms, Review Questions, and Problems	309

Chapter 10 Other Public-Key Cryptosystems 314

- 10.1 Diffie–Hellman Key Exchange 315
- 10.2 Elgamal Cryptographic System 319
- 10.3 Elliptic Curve Arithmetic 322
- 10.4 Elliptic Curve Cryptography 331
- 10.5 Key Terms, Review Questions, and Problems 335

PART FOUR: CRYPTOGRAPHIC DATA INTEGRITY ALGORITHMS 337**Chapter 11 Cryptographic Hash Functions 337**

- 11.1 Applications of Cryptographic Hash Functions 339
- 11.2 Two Simple Hash Functions 344
- 11.3 Requirements and Security 346
- 11.4 Secure Hash Algorithm (SHA) 352
- 11.5 SHA-3 362
- 11.6 Key Terms, Review Questions, and Problems 374

Chapter 12 Message Authentication Codes 378

- 12.1 Message Authentication Requirements 379
- 12.2 Message Authentication Functions 380
- 12.3 Requirements for Message Authentication Codes 388
- 12.4 Security of MACs 390
- 12.5 MACs Based on Hash Functions: HMAC 391
- 12.6 MACs Based on Block Ciphers: DAA and CMAC 396
- 12.7 Authenticated Encryption: CCM and GCM 399
- 12.8 Key Wrapping 405
- 12.9 Pseudorandom Number Generation Using Hash Functions and MACs 410
- 12.10 Key Terms, Review Questions, and Problems 413

Chapter 13 Digital Signatures 416

- 13.1 Digital Signatures 418
- 13.2 ElGamal Digital Signature Scheme 421
- 13.3 Schnorr Digital Signature Scheme 422
- 13.4 NIST Digital Signature Algorithm 423
- 13.5 Elliptic Curve Digital Signature Algorithm 427
- 13.6 RSA-PSS Digital Signature Algorithm 430
- 13.7 Key Terms, Review Questions, and Problems 435

Chapter 14 Lightweight Cryptography and Post-Quantum Cryptography 438

- 14.1 Lightweight Cryptography Concepts 439
- 14.2 Lightweight Cryptographic Algorithms 448
- 14.3 Post-Quantum Cryptography Concepts 456
- 14.4 Post-Quantum Cryptographic Algorithms 462
- 14.5 Key Terms and Review Questions 472

PART FIVE: MUTUAL TRUST 473**Chapter 15 Cryptographic Key Management and Distribution 473**

- 15.1 Symmetric Key Distribution Using Symmetric Encryption 474
- 15.2 Symmetric Key Distribution Using Asymmetric Encryption 478

8 CONTENTS

15.3	Distribution of Public Keys	481
15.4	X.509 Certificates	485
15.5	Public-Key Infrastructure	494
15.6	Key Terms, Review Questions, and Problems	496
Chapter 16 User Authentication 500		
16.1	Remote User-Authentication Principles	501
16.2	Remote User-Authentication Using Symmetric Encryption	507
16.3	Kerberos	510
16.4	Remote User-Authentication Using Asymmetric Encryption	524
16.5	Federated Identity Management	526
16.6	Key Terms, Review Questions, and Problems	530
PART SIX: NETWORK AND INTERNET SECURITY 533		
Chapter 17 Transport-Level Security 533		
17.1	Web Security Considerations	534
17.2	Transport Layer Security	536
17.3	HTTPS	551
17.4	Secure Shell (SSH)	553
17.5	Review Questions and Problems	564
Chapter 18 Wireless Network Security 566		
18.1	Wireless Security	567
18.2	Mobile Device Security	570
18.3	IEEE 802.11 Wireless Lan Overview	574
18.4	IEEE 802.11i Wireless Lan Security	580
18.5	Key Terms, Review Questions, and Problems	595
Chapter 19 Electronic Mail Security 597		
19.1	Internet Mail Architecture	599
19.2	Email Formats	601
19.3	Email Threats and Comprehensive Email Security	607
19.4	S/MIME	609
19.5	DNSSEC	619
19.6	DNS-Based Authentication of Named Entities	622
19.7	Sender Policy Framework	625
19.8	DomainKeys Identified Mail	628
19.9	Domain-Based Message Authentication, Reporting, and Conformance	634
19.10	Key Terms, Review Questions, and Problems	639
Chapter 20 IP Security 640		
20.1	IP Security Overview	641
20.2	IP Security Policy	643
20.3	Encapsulating Security Payload	648
20.4	Combining Security Associations	656
20.5	Internet Key Exchange	659
20.6	Key Terms, Review Questions, and Problems	667
Chapter 21 Network Endpoint Security 669		
21.1	Firewalls	670
21.2	Intrusion Detection Systems	680

21.3	Malicious Software	685
21.4	Distributed Denial of Service Attacks	688
21.5	Key Terms, Review Questions, and Problems	693
Chapter 22 Cloud Security 698		
22.1	Cloud Computing	699
22.2	Cloud Security Concepts	709
22.3	Cloud Security Risks and Countermeasures	711
22.4	Cloud Security as a Service	719
22.5	An Open-Source Cloud Security Module	722
22.6	Key Terms and Review Questions	723
Chapter 23 Internet of Things (IoT) Security 725		
23.1	The Internet of Things	726
23.2	IoT Security Concepts and Objectives	731
23.3	An Open-Source IoT Security Module	737
23.4	Key Terms and Review Questions	742
Appendix A Basic Concepts from Linear Algebra 744		
A.1	Operations on Vectors and Matrices	745
A.2	Linear Algebra Operations over Z_n	748
Appendix B Measures of Secrecy and Security 751		
B.1	Conditional Probability	752
B.2	Perfect Secrecy	752
B.3	Information and Entropy	756
B.4	Entropy and Secrecy	762
B.5	Min-Entropy	763
Appendix C Data Encryption Standard 766		
Appendix D Simplified AES 774		
D.1	Overview	775
D.2	S-AES Encryption and Decryption	777
D.3	Key Expansion	780
D.4	The S-Box	781
D.5	S-AES Structure	781
ANNEX D.1	Arithmetic in $GF(2^4)$	783
ANNEX D.2	The Mix Column Function	784
Appendix E Mathematical Basis of the Birthday Attack 786		
E.1	Related Problem	787
E.2	The Birthday Paradox	787
E.3	Useful Inequality	789
E.4	The General Case of Duplications	790
E.5	Overlap Between Two Sets	791
Glossary 793		
References 804		
Index 815		
Acronyms 832		