

Contents

<i>Preface to the Second Edition</i>	<i>xi</i>
<i>Preface to the First Edition</i>	<i>xv</i>
<i>Important Terms and Abbreviations</i>	<i>xvii</i>
1. Attacks on Computers and Computer Security	1
1.1 Introduction	1
1.2 The Need for Security	1
1.3 Security Approaches	4
1.4 Principles of Security	7
1.5 Types of Attacks	12
<i>Summary</i>	33
<i>Multiple-choice Questions</i>	34
<i>Exercises</i>	36
<i>Design/Programming Exercises</i>	37
2. Cryptography: Concepts and Techniques	38
2.1 Introduction	38
2.2 Plain Text and Cipher Text	40
2.3 Substitution Techniques	41
2.4 Transposition Techniques	54
2.5 Encryption and Decryption	59
2.6 Symmetric and Asymmetric Key Cryptography	62
2.7 Steganography	73
2.8 Key Range and Key Size	74
2.9 Possible Types of Attacks	77
<i>Summary</i>	81
<i>Multiple-choice Questions</i>	83
<i>Exercises</i>	85
<i>Design/Programming Exercises</i>	85
3. Symmetric Key Algorithms and AES	87
3.1 Introduction	87

3.2	Algorithm Types and Modes	87
3.3	An Overview of Symmetric Key Cryptography	98
3.4	Data Encryption Standard (DES)	100
3.5	International Data Encryption Algorithm (IDEA)	115
3.6	RC4	123
3.7	RC5	125
3.8	Blowfish	131
3.9	Advanced Encryption Standard (AES)	137
	<i>Summary</i>	148
	<i>Multiple-choice Questions</i>	150
	<i>Exercises</i>	152
	<i>Design/Programming Exercises</i>	152
4.	Asymmetric Key Algorithms, Digital Signatures and RSA	153
4.1	Introduction	153
4.2	Brief History of Asymmetric Key Cryptography	153
4.3	An Overview of Asymmetric Key Cryptography	154
4.4	The RSA Algorithm	156
4.5	Symmetric and Asymmetric Key Cryptography Together	160
4.6	Digital Signatures	165
4.7	Knapsack Algorithm	197
4.8	Some Other Algorithms	198
	<i>Summary</i>	201
	<i>Multiple-choice Questions</i>	201
	<i>Exercises</i>	203
	<i>Design/Programming Exercises</i>	203
5.	Digital Certificates and Public Key Infrastructure (PKI)	205
5.1	Introduction	205
5.2	Digital Certificates	206
5.3	Private Key Management	237
5.4	The PKIX Model	239
5.5	Public Key Cryptography Standards (PKCS)	241
5.6	XML, PKI and Security	247
5.7	Creating Digital Certificates Using Java	252
	<i>Summary</i>	260
	<i>Multiple-choice Questions</i>	262
	<i>Exercises</i>	263
	<i>Design/Programming Exercises</i>	263
6.	Internet Security Protocols	265
6.1	Introduction	265

6.2 Basic Concepts	265
6.3 Secure Socket Layer (SSL)	272
6.4 Transport Layer Security (TLS)	284
6.5 Secure Hyper Text Transfer Protocol (SHTTP)	284
6.6 Time Stamping Protocol (TSP)	285
6.7 Secure Electronic Transaction (SET)	286
6.8 SSL Versus SET	298
6.9 3-D Secure Protocol	299
6.10 Electronic Money	302
6.11 Email Security	307
6.12 Wireless Application Protocol (WAP) Security	327
6.13 Security in GSM	330
6.14 Security in 3G	332
<i>Summary</i>	335
<i>Multiple-choice Questions</i>	337
<i>Exercises</i>	338
<i>Design/Programming Exercises</i>	339
7. User Authentication and Kerberos	340
7.1 Introduction	340
7.2 Authentication Basics	340
7.3 Passwords	341
7.4 Authentication Tokens	354
7.5 Certificate-based Authentication	365
7.6 Biometric Authentication	371
7.7 Kerberos	372
7.8 Key Distribution Center (KDC)	378
7.9 Security Handshake Pitfalls	379
7.10 Single Sign On (SSO) Approaches	387
<i>Summary</i>	388
<i>Multiple-choice Questions</i>	390
<i>Exercises</i>	391
<i>Design/Programming Exercises</i>	391
8. Cryptography in Java, .NET and Operating Systems	393
8.1 Introduction	393
8.2 Cryptographic Solutions Using Java	393
8.3 Cryptographic Solutions Using Microsoft .NET Framework	400
8.4 Cryptographic Toolkits	403
8.5 Security and Operating Systems	404
8.6 Database Security	409

<i>Summary</i>	426	
<i>Multiple-choice Questions</i>	427	
<i>Exercises</i>	428	
<i>Design/Programming Exercises</i>	428	
9. Network Security, Firewalls and Virtual Private Networks (VPN)		430
9.1 Introduction	430	
9.2 Brief Introduction to TCP/IP	430	
9.3 Firewalls	435	
9.4 IP Security	452	
9.5 Virtual Private Networks (VPN)	469	
9.6 Intrusion	472	
<i>Summary</i>	476	
<i>Multiple-choice Questions</i>	478	
<i>Exercises</i>	479	
<i>Design/Programming Exercises</i>	480	
10. Case Studies on Cryptography and Security		481
10.1 Introduction	481	
10.2 Cryptographic Solutions—A Case Study	481	
10.3 Single Sign On (SSO)	488	
10.4 Secure Inter-branch Payment Transactions	491	
10.5 Denial Of Service (DOS) Attacks	496	
10.6 IP Spoofing Attacks	498	
10.7 Cross Site Scripting Vulnerability (CSSV)	499	
10.8 Contract Signing	501	
10.9 Secret Splitting	501	
10.10 Virtual Elections	502	
10.11 Secure Multiparty Calculation	504	
10.12 Creating a VPN	505	
10.13 Cookies and Privacy	506	
<i>Appendix A: Mathematical Background</i>		507
<i>Appendix B: Number Systems</i>		516
<i>Appendix C: Information Theory</i>		521
<i>Appendix D: Real-life Tools</i>		523
<i>Appendix E: Web Resources</i>		524
<i>Appendix F: A Brief Introduction to ASN, BER, DER</i>		527
<i>Index</i>		533