

# Contents

<i>Foreword</i>	<i>vii</i>
<i>Note of Appreciation</i>	<i>xi</i>
<i>Preface</i>	<i>xiii</i>
<i>Acknowledgements</i>	<i>xvii</i>
<b>1. Introduction to the Concepts of Security</b>	<b>1</b>
1.1 Introduction	1
1.2 The Need for Security	2
1.3 Security Approaches	3
1.4 Principles of Security	4
1.5 Types of Attacks	8
<i>Outline of the Book</i>	23
<i>Multiple-choice Questions</i>	25
<i>Review Questions</i>	26
<i>Design/Programming Exercises</i>	27
<b>2. Cryptographic Techniques</b>	<b>28</b>
2.1 Introduction	28
2.2 Plain Text and Cipher Text	29
2.3 Substitution Techniques	31
2.4 Transposition Techniques	36
2.5 Encryption and Decryption	40
2.6 Symmetric and Asymmetric Key Cryptography	43
2.7 Steganography	53
2.8 Key Range and Key Size	54
2.9 Possible Types of Attacks	57
<i>Chapter Summary</i>	58
<i>Key Terms and Concepts</i>	59
<i>Multiple-choice Questions</i>	59
<i>Review Questions</i>	60
<i>Design/Programming Exercises</i>	61
<b>3. Computer-based Symmetric Key Cryptographic Algorithms</b>	<b>63</b>
3.1 Introduction	63
3.2 Algorithm Types and Modes	63
3.3 An Overview of Symmetric Key Cryptography	73
3.4 Data Encryption Standard (DES)	75
3.5 International Data Encryption Algorithm (IDEA)	90
3.6 RC5	98
3.7 Blowfish	105
3.8 Advanced Encryption Standard (AES)	107
3.9 Differential and Linear Cryptanalysis	109
<i>Chapter Summary</i>	110
<i>Key Terms and Concepts</i>	110
<i>Multiple-choice Questions</i>	110
<i>Review Questions</i>	111
<i>Design/Programming Exercises</i>	111

<b>4. Computer-based Asymmetric Key Cryptographic Algorithms</b>	<b>112</b>
4.1 Introduction	112
4.2 Brief History of Asymmetric Key Cryptography	112
4.3 An Overview of Asymmetric Key Cryptography	113
4.4 The RSA Algorithm	115
4.5 Symmetric and Asymmetric Key Cryptography Together	119
4.6 Digital Signatures	125
4.7 Knapsack Algorithm	154
4.8 Some other Algorithms	154
<i>Chapter Summary</i>	157
<i>Key Terms and Concepts</i>	158
<i>Multiple-choice Questions</i>	158
<i>Review Questions</i>	159
<i>Design/Programming Exercises</i>	159
<b>5. Public Key Infrastructure (PKI)</b>	<b>161</b>
5.1 Introduction	161
5.2 Digital Certificates	162
5.3 Private Key Management	194
5.4 The PKIX Model	196
5.5 Public Key Cryptography Standards (PKCS)	198
5.6 XML, PKI and Security	204
<i>Chapter Summary</i>	208
<i>Key Terms and Concepts</i>	208
<i>Multiple-choice Questions</i>	209
<i>Review Questions</i>	210
<i>Design/Programming Exercises</i>	210
<b>6. Internet Security Protocols</b>	<b>211</b>
6.1 Basic Concepts	211
6.2 Secure Socket Layer (SSL)	218
6.3 Secure Hyper Text Transfer Protocol (SHTTP)	229
6.4 Time Stamping Protocol (TSP)	230
6.5 Secure Electronic Transaction (SET)	231
6.6 SSL Versus SET	244
6.7 3-D Secure Protocol	244
6.8 Electronic Money	245
6.9 Email Security	250
6.10 Wireless Application Protocol (WAP) Security	263
6.11 Security in GSM	266
<i>Chapter Summary</i>	268
<i>Key Terms and Concepts</i>	269
<i>Multiple-choice Questions</i>	269
<i>Review Questions</i>	270
<i>Design/Programming Exercises</i>	270
<b>7. User Authentication Mechanisms</b>	<b>271</b>
7.1 Introduction	271
7.2 Authentication Basics	271
7.3 Passwords	272
7.4 Authentication Tokens	286
7.5 Certificate-based Authentication	297
7.6 Biometric Authentication	303
7.7 Kerberos	304

7.8 Single Sign On (SSO) Approaches	309
<i>Chapter Summary</i>	310
<i>Key Terms and Concepts</i>	311
<i>Multiple-choice Questions</i>	311
<i>Review Questions</i>	312
<i>Design/Programming Exercises</i>	312
<b>8. Practical Implementations of Cryptography/Security</b>	<b>314</b>
8.1 Cryptographic Solutions Using Java	314
8.2 Cryptographic Solutions Using Microsoft	322
8.3 Cryptographic Toolkits	324
8.4 Security and Operating Systems	325
<i>Chapter Summary</i>	330
<i>Key Terms and Concepts</i>	330
<i>Multiple-choice Questions</i>	330
<i>Review Questions</i>	331
<i>Design/Programming Exercises</i>	331
<b>9. Network Security</b>	<b>332</b>
9.1 Brief Introduction to TCP/IP	332
9.2 Firewalls	338
9.3 IP Security	349
9.4 Virtual Private Networks (VPN)	365
<i>Chapter Summary</i>	368
<i>Key Terms and Concepts</i>	368
<i>Multiple-choice Questions</i>	369
<i>Review Questions</i>	369
<b>10. Case Studies on Cryptography and Security</b>	<b>371</b>
10.1 Introduction	371
10.2 Cryptographic Solutions—A Case Study	371
10.3 Single Sign On (SSO)	379
10.4 Secure Inter-branch Payment Transactions	382
10.5 Denial of Service (DOS) Attacks	385
10.6 IP Spoofing Attacks	388
10.7 Cross Site Scripting Vulnerability (CSSV)	389
10.8 Contract Signing	391
10.9 Secret Splitting	392
10.10 Virtual Elections	394
10.11 Secure Multiparty Calculation	395
<b>Appendix A— Mathematical Background</b>	<b>396</b>
<b>Appendix B— Number Systems</b>	<b>401</b>
<b>Appendix C— Information Theory</b>	<b>406</b>
<b>Appendix D— Real-life Tools</b>	<b>408</b>
<b>Appendix E— Web Resources</b>	<b>409</b>
<b>Appendix F— A Brief Introduction to ASN, BER, DER</b>	<b>411</b>
<b>Appendix G— Modern Security Trends</b>	<b>413</b>
<b>Answers to Multiple-choice Questions</b>	<b>419</b>
<b>Glossary</b>	<b>420</b>
<b>References</b>	<b>426</b>
<b>Index</b>	<b>428</b>