- 1 Classical Cryptography p. 1
- 1.1 Introduction: Some Simple Cryptosystems p. 1
- 1.1.1 The Shift Cipher p. 3
- 1.1.2 The Substitution Cipher p. 7
- 1.1.3 The Affine Cipher p. 8
- 1.1.4 The Vigenere Cipher p. 12
- 1.1.5 The Hill Cipher p. 13
- 1.1.6 The Permutation Cipher p. 18
- 1.1.7 Stream Ciphers p. 20
- 1.2 Cryptanalysis p. 25
- 1.2.1 Cryptanalysis of the Affine Cipher p. 27
- 1.2.2 Cryptanalysis of the Substitution Cipher p. 28
- 1.2.3 Cryptanalysis of the Vigenere Cipher p. 31
- 1.2.4 Cryptanalysis of the Hill Cipher p. 34
- 1.2.5 Cryptanalysis of the LFSR Stream Cipher p. 36
- 1.3 Notes p. 38
- Exercises p. 38
- 2 Shannon's Theory p. 45
- 2.1 Introduction p. 45
- 2.2 Elementary Probability Theory p. 46
- 2.3 Perfect Secrecy p. 48
- 2.4 Entropy p. 54
- 2.4.1 Huffman Encodings p. 56
- 2.5 Properties of Entropy p. 59
- 2.6 Spurious Keys and Unicity Distance p. 62
- 2.7 Product Cryptosystems p. 67
- 2.8 Notes p. 70
- Exercises p. 70
- 3 Block Ciphers and the Advanced Encryption Standard p. 73
- 3.1 Introduction p. 73
- 3.2 Substitution-Permutation Networks p. 74
- 3.3 Linear Cryptanalysis p. 79
- 3.3.1 The Piling-up Lemma p. 80
- 3.3.2 Linear Approximations of S-boxes p. 82
- 3.3.3 A Linear Attack on an SPN p. 85
- 3.4 Differential Cryptanalysis p. 89
- 3.5 The Data Encryption Standard p. 95
- 3.5.1 Description of DES p. 95
- 3.5.2 Analysis of DES p. 100
- 3.6 The Advanced Encryption Standard p. 102
- 3.6.1 Description of AES p. 103
- 3.6.2 Analysis of AES p. 108
- 3.7 Modes of Operation p. 109
- 3.8 Notes and References p. 112
- Exercises p. 113
- 4 Cryptographic Hash Functions p. 117

- 4.1 Hash Functions and Data Integrity p. 117
- 4.2 Security of Hash Functions p. 119
- 4.2.1 The Random Oracle Model p. 120
- 4.2.2 Algorithms in the Random Oracle Model p. 121
- 4.2.3 Comparison of Security Criteria p. 125
- 4.3 Interated Hash Functions p. 127
- 4.3.1 The Merkle-Damgard Construction p. 128
- 4.3.2 The Secure Hash Algorithm p. 133
- 4.4 Message Authentication Codes p. 136
- 4.4.1 Nested MACs and HMAC p. 138
- 4.4.2 CBC-MAC p. 140
- 4.5 Unconditionally Secure MACs p. 141
- 4.5.1 Strongly Universal Hash Families p. 144
- 4.5.2 Optimality of Deception Probabilities p. 146
- 4.6 Notes and References p. 149
- Exercises p. 150
- 5 The RSA Cryptosystem and Factoring Integers p. 155
- 5.1 Introduction to Public-key Cryptography p. 155
- 5.2 More Number Theory p. 157
- 5.2.1 The Euclidean Algorithm p. 157
- 5.2.2 The Chinese Remainder Theorem p. 162
- 5.2.3 Other Useful Facts p. 164
- 5.3 The RSA Cryptosystem p. 167
- 5.3.1 Implementing RSA p. 168
- 5.4 Primality Testing p. 171
- 5.5 Square Roots Modulo n p. 181
- 5.6 Factoring Algorithms p. 182
- 5.6.1 The Pollard p--1 Algorithm p. 182
- 5.6.2 The Pollard Rho Algorithm p. 184
- 5.6.3 Dixon's Random Squares Algorithm p. 187
- 5.6.4 Factoring Algorithms in Practice p. 192
- 5.7 Other Attacks on RSA p. 194
- 5.7.1 Computing [phi](n) p. 194
- 5.7.2 The Decryption Exponent p. 195
- 5.7.3 Wiener's Low Decryption Exponent Attack p. 200
- 5.8 The Rabin Cryptosystem p. 204
- 5.8.1 Security of the Rabin Cryptosystem p. 206
- 5.9 Semantic Security of RSA p. 208
- 5.9.1 Partial Information Concerning Plaintext Bits p. 209
- 5.9.2 Optimal Asymmetric Encryption Padding p. 212
- 5.10 Notes and References p. 218
- Exercises p. 219
- 6 Public-key Cryptosystems Based on the Discrete Logarithm Problem p. 226
- 6.1 The ElGamal Cryptosystem p. 226
- 6.2 Algorithms for the Discrete Logarithm Problem p. 228
- 6.2.1 Shank's Algorithm p. 229

- 6.2.2 The Pollard Rho Discrete Logarithm Algorithm p. 231
- 6.2.3 The Pohlig-Hellman Algorithm p. 234
- 6.2.4 The Index Calculus Method p. 237
- 6.3 Lower Bounds on the Complexity of Generic Algorithms p. 239
- 6.4 Finite Fields p. 243
- 6.5 Elliptic Curves p. 247
- 6.5.1 Elliptic Curves over the Reals p. 247
- 6.5.2 Elliptic Curves Modulo a Prime p. 250
- 6.5.3 Properties of Elliptic Curves p. 254
- 6.5.4 Point Compression and the ECIES p. 255
- 6.5.5 Computing Point Multiples on Elliptic Curves p. 257
- 6.6 Discrete Logarithm Algorithms in Practice p. 259
- 6.7 Security of ElGamal Systems p. 261
- 6.7.1 Bit Security of Discrete Logarithms p. 261
- 6.7.2 Semantic Security of ElGamal Systems p. 264
- 6.7.3 The Diffie-Hellman Problems p. 265
- 6.8 Notes and References p. 267
- Exercises p. 268
- 7 Signature Schemes p. 274
- 7.1 Introduction p. 274
- 7.2 Security Requirements for Signature Schemes p. 277
- 7.2.1 Signatures and Hash Functions p. 279
- 7.3 The ElGamal Signature Scheme p. 280
- 7.3.1 Security of the ElGamal Signature Scheme p. 282
- 7.4 Variants of the ElGamal Signature Scheme p. 286
- 7.4.1 The Schnorr Signature Scheme p. 286
- 7.4.2 The Digital Signature Algorithm p. 288
- 7.4.3 The Elliptic Curve DSA p. 291
- 7.5 Provably Secure Signature Schemes p. 292
- 7.5.1 One-time Signatures p. 292
- 7.5.2 Full Domain Hash p. 297
- 7.6 Undeniable Signatures p. 300
- 7.7 Fail-stop Signatures p. 305
- 7.8 Notes and References p. 310
- Exercises p. 311
- Further Reading p. 315
- Bibliography p. 317
- Cryptosystem Index p. 331
- Algorithm Index p. 333
- Problem Index p. 334
- Subject Index p. 335