

Contents

Preface	xi
1 Overview	1
1.1 Secure Communications	2
1.2 Cryptographic Applications	9
2 Classical Cryptosystems	12
2.1 Shift Ciphers	13
2.2 Affine Ciphers	14
2.3 The Vigenère Cipher	16
2.4 Substitution Ciphers	23
2.5 Sherlock Holmes	26
2.6 The Playfair and ADFGX Ciphers	29
2.7 Block Ciphers	33
2.8 Binary Numbers and ASCII	37
2.9 One-Time Pads	38
2.10 Pseudo-random Bit Generation	40
2.11 Linear Feedback Shift Register Sequences	42
2.12 Enigma	49
2.13 Exercises	54
2.14 Computer Problems	56
3 Basic Number Theory	59
3.1 Basic Notions	59
3.2 Solving $ax + by = d$	65
3.3 Congruences	66
3.4 The Chinese Remainder Theorem	72
3.5 Modular Exponentiation	74
3.6 Fermat and Euler	75
3.7 Primitive Roots	79
3.8 Inverting Matrices Mod n	80
3.9 Square Roots Mod n	81

3.10	Finite Fields	83
3.11	Exercises	91
3.12	Computer Problems	95
4	The Data Encryption Standard	97
4.1	Introduction	97
4.2	A Simplified DES-Type Algorithm	98
4.3	Differential Cryptanalysis	102
4.4	DES	107
4.5	Modes of Operation	115
4.6	Breaking DES	118
4.7	Password Security	123
4.8	Exercises	125
5	AES: Rijndael	127
5.1	The Basic Algorithm	128
5.2	The Layers	129
5.3	Decryption	133
5.4	Design Considerations	136
6	The RSA Algorithm	137
6.1	The RSA Algorithm	137
6.2	Attacks on RSA	142
6.3	Primality Testing	145
6.4	Factoring	149
6.5	The RSA Challenge	154
6.6	An Application to Treaty Verification	156
6.7	The Public Key Concept	156
6.8	Exercises	159
6.9	Computer Problems	162
7	Discrete Logarithms	165
7.1	Discrete Logarithms	165
7.2	Computing Discrete Logs	166
7.3	Bit Commitment	173
7.4	The ElGamal Public Key Cryptosystem	173
7.5	Exercises	175
7.6	Computer Problems	176
8	Digital Signatures	177
8.1	RSA Signatures	178
8.2	The ElGamal Signature Scheme	179
8.3	Hash Functions	182

8.4	Birthday Attacks	186
8.5	The Digital Signature Algorithm	190
8.6	Exercises	191
8.7	Computer Problems	194
9	E-Commerce and Digital Cash	196
9.1	Secure Electronic Transaction	197
9.2	Digital Cash	199
9.3	Exercises	206
10	Secret Sharing Schemes	208
10.1	Secret Splitting	208
10.2	Threshold Schemes	209
10.3	Exercises	215
10.4	Computer Problems	217
11	Games	219
11.1	Flipping Coins over the Telephone	219
11.2	Poker over the Telephone	221
11.3	Exercises	226
12	Zero-Knowledge Techniques	228
12.1	The Basic Setup	228
12.2	Feige-Fiat-Shamir Identification Scheme	231
12.3	Exercises	233
13	Key Establishment Protocols	236
13.1	Key Agreement Protocols	237
13.2	Key Pre-distribution	239
13.3	Key Distribution	241
13.4	Public Key Infrastructures (PKI)	246
13.5	Exercises	248
14	Information Theory	250
14.1	Probability Review	251
14.2	Entropy	253
14.3	Huffman Codes	258
14.4	Perfect Secrecy	260
14.5	The Entropy of English	263
14.6	Exercises	268

15 Elliptic Curves	272
15.1 The Addition Law	272
15.2 Elliptic Curves Mod n	276
15.3 Factoring with Elliptic Curves	280
15.4 Elliptic Curves in Characteristic 2	284
15.5 Elliptic Curve Cryptosystems	287
15.6 Exercises	290
15.7 Computer Problems	293
16 Error Correcting Codes	295
16.1 Introduction	295
16.2 Error Correcting Codes	301
16.3 Bounds on General Codes	305
16.4 Linear Codes	311
16.5 Hamming Codes	319
16.6 Golay Codes	320
16.7 Cyclic Codes	329
16.8 BCH Codes	335
16.9 Reed-Solomon Codes	343
16.10 The McEliece Cryptosystem	345
16.11 Other Topics	348
16.12 Exercises	349
16.13 Computer Problems	352
17 Quantum Cryptography	353
17.1 A Quantum Experiment	354
17.2 Quantum Key Distribution	357
17.3 Shor's Algorithm	359
17.4 Exercises	370
A Mathematica	372
A.1 Getting Started with Mathematica	372
A.2 Some Commands	374
A.3 Examples for Chapter 2	375
A.4 Examples for Chapter 3	382
A.5 Examples for Chapter 6	386
A.6 Examples for Chapter 8	394
A.7 Examples for Chapter 10	395
A.8 Examples for Chapter 11	396
A.9 Examples for Chapter 15	397

B Maple Examples	403
B.1 Getting Started with Maple	403
B.2 Some Commands	404
B.3 Examples for Chapter 2	406
B.4 Examples for Chapter 3	414
B.5 Examples for Chapter 6	419
B.6 Examples for Chapter 8	428
B.7 Examples for Chapter 10	428
B.8 Examples for Chapter 11	430
B.9 Examples for Chapter 15	432
 C MATLAB Examples	 437
C.1 Getting Started with MATLAB	438
C.2 Examples for Chapter 2	444
C.3 Examples for Chapter 3	456
C.4 Examples for Chapter 6	460
C.5 Examples for Chapter 8	466
C.6 Examples for Chapter 10	466
C.7 Examples for Chapter 11	467
C.8 Examples for Chapter 15	470
 D Further Reading	 478
 Bibliography	 479
 Index	 485