

Contents

Chapter 1. Classical Two-Way Cryptography	1
1.1 Cryptosystems and Cryptanalysis	1
1.2 Monoalphabetic Systems	10
1.3 Polyalphabetic and Other Systems	22
1.4 Rotors and DES	39
Chapter 2. The Idea of Public Keys	55
2.1 Some Streets Are One-Way	55
2.2 How to Realize the Idea	64
2.3 Obvious Advantages of Public Keys	71
Chapter 3. Knapsack Systems	77
3.1 A Trapdoor is Built	77
3.2 How to Find the Trapdoor	87
3.3 Theory of Reachability	96
3.4 Trying to Hide the Trapdoor Again	108
3.5 Dense Knapsacks	117
Chapter 4. RSA	125
4.1 Legal World	125
4.2 Attack and Defense	134
4.3 Primality	137
4.4 Cryptanalysis and Factoring	143
4.5 Partial Information on RSA	147
4.6 Discrete Logarithms and Key Exchange	154
Chapter 5. Other Bases of Cryptosystems	159
5.1 Exponentiation in Quadratic Fields	159
5.2 Iteration of Morphisms	166
5.3 Automata and Language Theory	174
5.4 Coding Theory	178
Chapter 6. Cryptographic Protocols: Surprising Vistas for Communication	181
6.1 More Than Etiquette	181
6.2 Coin Flipping by Telephone. Poker Revisited	184
6.3 How to Share a Secret	187
6.4 Partial Disclosure of Secrets	190
6.5 Oblivious Transfer	194
6.6 Applications: Banking and Ballots	200

6.7	Convincing Proofs with No Details	202
6.8	Zero-Knowledge Proofs	208
6.9	Zero-Knowledge Proofs of Identity	213
6.10	Secret Balloting Systems Revisited	218
6.11	Cryptographic Protocols Without Computers	234
Appendix A. Tutorial in Complexity Theory		245
Appendix B. Tutorial in Number Theory		249
Problems		255
Historical and Bibliographical Remarks		263
References		265
Index		269