Contents

Preface VII

1 Introduction to Cryptocomplexity 1

2 Foundations of Computer Science and Mathematics 9
2.1 Algorithmics 9
2.2 Formal Languages and Recursive Function Theory 16
2.3 Logic 29
2.3.1 Propositional Logic 29
2.3.2 Predicate Logic 34
2.4 Algebra, Number Theory, and Graph Theory 37
2.4.1 Algebra and Number Theory 37
2.4.2 Permutation Groups 41
2.4.3 Graph Theory 43
2.5 Probability Theory 46
2.6 Exercises and Problems 47
2.7 Summary and Bibliographic Remarks 51

3 Foundations of Complexity Theory 53
3.1 Tasks and Aims of Complexity Theory 53
3.2 Complexity Measures and Classes 56
3.3 Speed-Up, Compression, and Hierarchy Theorems 63
3.4 Between Logarithmic and Polynomial Space 72
3.5 Reducibilities and Completeness 77
3.5.1 Many-One Reducibilities, Hardness, and Completeness 77
3.5.2 NL-Completeness 81
3.5.3 NP-Completeness 88
3.6 Inside NP 106
3.6.1 P versus NP and the Graph Isomorphism Problem 106
3.6.2 The Berman–Hartmanis Isomorphism Conjecture and One-Way Functions 108

3.7 Exercises and Problems 114
3.8 Summary and Bibliographic Remarks 118

4 Foundations of Cryptology 127
4.1 Tasks and Aims of Cryptology 127
4.2 Some Classical Cryptosystems and Their Cryptanalysis 130
4.2.1 Substitution and Permutation Ciphers 130
4.2.2 Affine Linear Block Ciphers 135
4.2.3 Block and Stream Ciphers 145
4.3 Perfect Secrecy 151
4.3.1 Shannon's Theorem and Vernam's One-Time Pad 151
4.3.2 Entropy and Key Equivocation 155
4.4 Exercises and Problems 161
4.5 Summary and Bibliographic Remarks 168

5 Hierarchies Based on NP 171
5.1 Boolean Hierarchy over NP 172
5.2 Polynomial Hierarchy 190
5.3 Parallel Access to NP 201
5.3.1 A Brief Digression to Social Choice Theory 206
5.3.2 Determining Young Winners Is Complete for Parallel Access to NP 208
5.4 Query Hierarchies over NP 212
5.5 The Boolean Hierarchy Collapsing the Polynomial Hierarchy 217
5.6 Alternating Turing Machines 221
5.7 The Low and the High Hierarchy within NP 232
5.8 Exercises and Problems 241
5.9 Summary and Bibliographic Remarks 248

6 Randomized Algorithms and Complexity Classes 261
6.1 The Satisfiability Problem of Propositional Logic 262
6.1.1 Deterministic Time Complexity 263
6.1.2 Probabilistic Time Complexity 265
6.2 Probabilistic Polynomial-Time Classes 268
6.2.1 PP, RP, and ZPP: Monte Carlo and Las Vegas Algorithms . . 268
6.2.2 BPP: Bounded-Error Probabilistic Polynomial Time 275
6.3 Quantifiers and Arthur-Merlin Games 279
6.3.1 Quantifiers and BPP 279
6.3.2 Arthur-Merlin Hierarchy 286
6.4 Counting Classes 290
6.5 Graph Isomorphism and Lowness 294
6.5.1 Graph Isomorphism Is in the Low Hierarchy 294
6.5.2 Graph Isomorphism Is in SPP 298
6.6 Exercises and Problems 302
6.7 Summary and Bibliographic Remarks 306

7 RSA Cryptosystem, Primality, and Factoring 311

7.1 RSA 312

7.1.1 RSA Public-Key Cryptosystem 312

7.1.2 RSA Digital Signature Scheme 316

7.2 Primality Tests 317

7.2.1 Fermat Test 319

7.2.2 Miller–Rabin Test 323

7.2.3 Solovay–Strassen Test 329

7.2.4 Primality Is in P 335

7.3 Factoring 335

7.3.1 Trial Division 336

7.3.2 Pollard's Algorithm 337

7.3.3 Quadratic Sieve 338

7.3.4 Other Factoring Methods 343

7.4 Security of RSA: Possible Attacks and Countermeasures 345

7.5 Exercises and Problems 353

7.6 Summary and Bibliographic Remarks 357

8 Other Public-Key Cryptosystems and Protocols 361

8.1 Diffie–Hellman and the Discrete Logarithm Problem 362

8.1.1 Diffie and Hellman's Secret-Key Agreement Protocol 362

8.1.2 Discrete Logarithm and the Diffie–Hellman Problem 366

8.2 ElGamal's Protocols 369

8.2.1 ElGamal's Public-Key Cryptosystem 369

8.2.2 ElGamal's Digital Signature Scheme 371

8.2.3 Security of ElGamal's Protocols 373

8.3 Rabin's Public-Key Cryptosystem 380

8.3.1 Rabin's Cryptosystem 381

8.3.2 Security of Rabin's System 383

8.4 Arthur-Merlin Games and Zero-Knowledge 386

8.5 Merkle and Hellman's Public-Key Cryptosystem 393

8.6 Rabi, Rivest, and Sherman's Protocols 396

8.7 Exercises and Problems 402

8.8 Summary and Bibliographic Remarks 408

List of Figures 413

List of Tables 415

References 417

Index 444