
Contents

Preface	xiii
Getting Started with SageMath	1
0.1. Installation	1
0.2. SageMath Command Line	2
0.3. Browser Notebooks	2
0.4. Computations with SageMath	3
Chapter 1. Fundamentals	7
1.1. Sets, Relations and Functions	7
1.2. Combinatorics	14
1.3. Computational Complexity	16
1.4. Discrete Probability	19
1.5. Random Numbers	23
1.6. Summary	27
Exercises	28
Chapter 2. Encryption Schemes and Definitions of Security	31
2.1. Encryption Schemes	32
2.2. Perfect Secrecy	35
2.3. Computational Security	36
2.4. Indistinguishable Encryptions	37
2.5. Eavesdropping Attacks	39

2.6. Chosen Plaintext Attacks	41
2.7. Chosen Ciphertext Attacks	43
2.8. Pseudorandom Generators	45
2.9. Pseudorandom Functions	48
2.10. Block Ciphers and Operation Modes	52
2.11. Summary	58
Exercises	58
Chapter 3. Elementary Number Theory	61
3.1. Integers	61
3.2. Congruences	65
3.3. Modular Exponentiation	67
3.4. Summary	69
Exercises	69
Chapter 4. Algebraic Structures	73
4.1. Groups	73
4.2. Rings and Fields	81
4.3. Finite Fields	82
4.4. Linear and Affine Maps	92
4.5. Summary	97
Exercises	97
Chapter 5. Block Ciphers	101
5.1. Constructions of Block Ciphers	101
5.2. Advanced Encryption Standard	104
5.3. Summary	111
Exercises	111
Chapter 6. Stream Ciphers	115
6.1. Definition of Stream Ciphers	115
6.2. Linear Feedback Shift Registers	119
6.3. RC4	128
6.4. Salsa20 and ChaCha20	130
6.5. Summary	135
Exercises	135

Chapter 7. Hash Functions	137
7.1. Definitions and Security Requirements	137
7.2. Applications of Hash Functions	139
7.3. Merkle-Damgård Construction	140
7.4. SHA-1	142
7.5. SHA-2	145
7.6. SHA-3	146
7.7. Summary	149
Exercises	149
Chapter 8. Message Authentication Codes	151
8.1. Definitions and Security Requirements	151
8.2. CBC MAC	154
8.3. HMAC	156
8.4. Authenticated Encryption	157
8.5. Summary	161
Exercises	161
Chapter 9. Public-Key Encryption and the RSA Cryptosystem	163
9.1. Public-Key Cryptosystems	163
9.2. Plain RSA	166
9.3. RSA Security	168
9.4. Generation of Primes	170
9.5. Efficiency of RSA	173
9.6. Padded RSA	175
9.7. Factoring	177
9.8. Summary	182
Exercises	182
Chapter 10. Key Establishment	185
10.1. Key Distribution	186
10.2. Key Exchange Protocols	186
10.3. Diffie-Hellman Key Exchange	188
10.4. Diffie-Hellman using Subgroups of \mathbb{Z}_p^*	190
10.5. Discrete Logarithm	192
10.6. Key Encapsulation	194
10.7. Hybrid Encryption	197

10.8. Summary	200
Exercises	200
Chapter 11. Digital Signatures	203
11.1. Definitions and Security Requirements	203
11.2. Plain RSA Signature	205
11.3. Probabilistic Signature Scheme	206
11.4. Summary	210
Exercises	210
Chapter 12. Elliptic Curve Cryptography	213
12.1. Weierstrass Equations and Elliptic Curves	213
12.2. Elliptic Curve Diffie-Hellman	222
12.3. Efficiency and Security of Elliptic Curve Cryptography	223
12.4. Elliptic Curve Factoring Method	224
12.5. Summary	227
Exercises	227
Chapter 13. Quantum Computing	229
13.1. Quantum Bits	230
13.2. Multiple Qubit Systems	234
13.3. Quantum Algorithms	235
13.4. Quantum Fourier Transform	241
13.5. Shor's Factoring Algorithm	242
13.6. Quantum Key Distribution	248
13.7. Summary	251
Exercises	251
Chapter 14. Lattice-based Cryptography	253
14.1. Lattices	254
14.2. Lattice Algorithms	260
14.3. GGH Cryptosystem	269
14.4. NTRU	271
14.5. Learning with Errors	276
14.6. Summary	282
Exercises	282

Chapter 15. Code-based Cryptography	285
15.1. Linear Codes	286
15.2. Bounds on Codes	290
15.3. Goppa Codes	295
15.4. McEliece Cryptosystem	303
15.5. Summary	309
Exercises	310
Bibliography	313
Index	319