

# Contents

Preface	v
<b>Part 1. Mathematical Background</b>	<b>1</b>
Chapter 1. Modular Arithmetic, Groups, Finite Fields and Probability	3
1.1. Modular Arithmetic	3
1.2. Finite Fields	8
1.3. Basic Algorithms	11
1.4. Probability	21
1.5. Big Numbers	24
Chapter 2. Primality Testing and Factoring	27
2.1. Prime Numbers	27
2.2. The Factoring and Factoring-Related Problems	32
2.3. Basic Factoring Algorithms	38
2.4. Modern Factoring Algorithms	42
2.5. Number Field Sieve	44
Chapter 3. Discrete Logarithms	51
3.1. The DLP, DHP and DDH Problems	51
3.2. Pohlig–Hellman	54
3.3. Baby-Step/Giant-Step Method	57
3.4. Pollard-Type Methods	59
3.5. Sub-exponential Methods for Finite Fields	64
Chapter 4. Elliptic Curves	67
4.1. Introduction	67
4.2. The Group Law	69
4.3. Elliptic Curves over Finite Fields	72
4.4. Projective Coordinates	74
4.5. Point Compression	75
4.6. Choosing an Elliptic Curve	77
Chapter 5. Lattices	79
5.1. Lattices and Lattice Reduction	79
5.2. “Hard” Lattice Problems	85
5.3. $q$ -ary Lattices	89
5.4. Coppersmith’s Theorem	90
Chapter 6. Implementation Issues	95
6.1. Introduction	95
6.2. Exponentiation Algorithms	95
6.3. Special Exponentiation Methods	99

6.4. Multi-precision Arithmetic	101
6.5. Finite Field Arithmetic	107
<b>Part 2. Historical Ciphers</b>	<b>117</b>
Chapter 7. Historical Ciphers	119
7.1. Introduction	119
7.2. Shift Cipher	120
7.3. Substitution Cipher	123
7.4. Vigenère Cipher	126
7.5. A Permutation Cipher	131
Chapter 8. The Enigma Machine	133
8.1. Introduction	133
8.2. An Equation for the Enigma	136
8.3. Determining the Plugboard Given the Rotor Settings	137
8.4. Double Encryption of Message Keys	140
8.5. Determining the Internal Rotor Wirings	141
8.6. Determining the Day Settings	147
8.7. The Germans Make It Harder	148
8.8. Known Plaintext Attack and the Bombes	150
8.9. Ciphertext Only Attack	158
Chapter 9. Information-Theoretic Security	163
9.1. Introduction	163
9.2. Probability and Ciphers	164
9.3. Entropy	169
9.4. Spurious Keys and Unicity Distance	173
Chapter 10. Historical Stream Ciphers	179
10.1. Introduction to Symmetric Ciphers	179
10.2. Stream Cipher Basics	181
10.3. The Lorenz Cipher	182
10.4. Breaking the Lorenz Cipher's Wheels	188
10.5. Breaking a Lorenz Cipher Message	192
<b>Part 3. Modern Cryptography Basics</b>	<b>195</b>
Chapter 11. Defining Security	197
11.1. Introduction	197
11.2. Pseudo-random Functions and Permutations	197
11.3. One-Way Functions and Trapdoor One-Way Functions	201
11.4. Public Key Cryptography	202
11.5. Security of Encryption	203
11.6. Other Notions of Security	209
11.7. Authentication: Security of Signatures and MACs	215
11.8. Bit Security	219
11.9. Computational Models: The Random Oracle Model	221
Chapter 12. Modern Stream Ciphers	225
12.1. Stream Ciphers from Pseudo-random Functions	225
12.2. Linear Feedback Shift Registers	227

12.3.	Combining LFSRs	233
12.4.	RC4	238
Chapter 13.	Block Ciphers and Modes of Operation	241
13.1.	Introduction to Block Ciphers	241
13.2.	Feistel Ciphers and DES	244
13.3.	AES	250
13.4.	Modes of Operation	254
13.5.	Obtaining Chosen Ciphertext Security	266
Chapter 14.	Hash Functions, Message Authentication Codes and Key Derivation Functions	271
14.1.	Collision Resistance	271
14.2.	Padding	275
14.3.	The Merkle–Damgård Construction	276
14.4.	The MD-4 Family	278
14.5.	HMAC	282
14.6.	Merkle–Damgård-Based Key Derivation Function	284
14.7.	MACs and KDFs Based on Block Ciphers	285
14.8.	The Sponge Construction and SHA-3	288
Chapter 15.	The “Naive” RSA Algorithm	295
15.1.	“Naive” RSA Encryption	295
15.2.	“Naive” RSA Signatures	299
15.3.	The Security of RSA	301
15.4.	Some Lattice-Based Attacks on RSA	305
15.5.	Partial Key Exposure Attacks on RSA	309
15.6.	Fault Analysis	310
Chapter 16.	Public Key Encryption and Signature Algorithms	313
16.1.	Passively Secure Public Key Encryption Schemes	313
16.2.	Random Oracle Model, OAEP and the Fujisaki–Okamoto Transform	319
16.3.	Hybrid Ciphers	324
16.4.	Constructing KEMs	329
16.5.	Secure Digital Signatures	333
16.6.	Schemes Avoiding Random Oracles	342
Chapter 17.	Cryptography Based on Really Hard Problems	349
17.1.	Cryptography and Complexity Theory	349
17.2.	Knapsack-Based Cryptosystems	353
17.3.	Worst-Case to Average-Case Reductions	356
17.4.	Learning With Errors (LWE)	360
Chapter 18.	Certificates, Key Transport and Key Agreement	369
18.1.	Introduction	369
18.2.	Certificates and Certificate Authorities	371
18.3.	Fresh Ephemeral Symmetric Keys from Static Symmetric Keys	375
18.4.	Fresh Ephemeral Symmetric Keys from Static Public Keys	382
18.5.	The Symbolic Method of Protocol Analysis	388
18.6.	The Game-Based Method of Protocol Analysis	392
<b>Part 4.</b>	<b>Advanced Protocols</b>	<b>401</b>
Chapter 19.	Secret Sharing Schemes	403

19.1.	Access Structures	403
19.2.	General Secret Sharing	405
19.3.	Reed–Solomon Codes	407
19.4.	Shamir Secret Sharing	412
19.5.	Application: Shared RSA Signature Generation	414
Chapter 20.	Commitments and Oblivious Transfer	417
20.1.	Introduction	417
20.2.	Commitment Schemes	417
20.3.	Oblivious Transfer	421
Chapter 21.	Zero-Knowledge Proofs	425
21.1.	Showing a Graph Isomorphism in Zero-Knowledge	425
21.2.	Zero-Knowledge and $\mathcal{NP}$	428
21.3.	Sigma Protocols	429
21.4.	An Electronic Voting System	436
Chapter 22.	Secure Multi-party Computation	439
22.1.	Introduction	439
22.2.	The Two-Party Case	441
22.3.	The Multi-party Case: Honest-but-Curious Adversaries	445
22.4.	The Multi-party Case: Malicious Adversaries	448
<b>Appendix</b>		451
Basic Mathematical Terminology		453
A.1.	Sets	453
A.2.	Relations	453
A.3.	Functions	455
A.4.	Permutations	456
A.5.	Operations	459
A.6.	Groups	461
A.7.	Rings	468
A.8.	Fields	469
A.9.	Vector Spaces	470
Index		475



<http://www.springer.com/978-3-319-21935-6>

Cryptography Made Simple

Smart, N.P.

2016, XII, 481 p., Hardcover

ISBN: 978-3-319-21935-6