

# Contents

<b>1</b>	<b>Classical Ciphers and Their Cryptanalysis</b>	<b>1</b>
1.1	The Caesar Cipher	1
1.2	Substitution Ciphers	7
1.3	The Vigenère Cipher.	12
1.3.1	The Vigenère Cipher in Maple.	14
1.3.2	Cryptanalysis of the Vigenère Cipher	16
1.4	The Hill Cipher	25
1.4.1	The Hill Cipher in Maple	27
1.4.2	Cryptanalysis of the Hill Cipher.	29
1.5	Some Conclusions	32
<b>2</b>	<b>Basic Concepts from Probability, Complexity, Algebra and Number Theory</b>	<b>35</b>
2.1	Basic Probability Theory	35
2.2	Integers and Divisibility	39
2.2.1	Representation of Integers	40
2.3	Basic Computational Complexity	42
2.3.1	Asymptotic Notation.	43
2.3.2	Efficient Computation and $\mathcal{P}$ Versus $\mathcal{NP}$	45
2.3.3	Running Times of Some Simple Algorithms	51
2.3.4	Probabilistic Algorithms	58
2.3.5	Final Remarks on Complexity	60
2.4	The Euclidean Algorithm	61
2.5	Groups, Rings and Fields.	68
2.5.1	Basic Concepts.	68
2.5.2	Congruences and the Residue Class Ring	73
2.6	The Chinese Remainder Theorem.	76
2.6.1	The Chinese Remainder Theorem and the Residue Class Ring.	78

2.7	Euler's Theorem and Modular Exponentiation . . . . .	80
2.7.1	Euler's Theorem. . . . .	80
2.7.2	Modular Exponentiation . . . . .	83
2.7.3	Finding Generators in $\mathbb{Z}_p^*$ . . . . .	89
2.8	Finite Fields. . . . .	95
2.8.1	A Field of 4 Elements. . . . .	95
2.8.2	The Polynomial Ring . . . . .	99
2.8.3	The Field of $p^n$ Elements . . . . .	104
2.8.4	The Field of 256 Elements . . . . .	111
2.8.5	The Multiplicative Group of a Finite Field . . . . .	113
2.9	Quadratic Residues and Modular Square Roots . . . . .	115
2.9.1	Quadratic Residues and the Legendre and Jacobi Symbols . . . . .	115
2.9.2	Computing Modular Square Roots . . . . .	123
<b>3</b>	<b>Private-Key Encryption . . . . .</b>	<b>131</b>
3.1	Perfect Secrecy . . . . .	131
3.2	The One-Time Pad . . . . .	135
3.3	From Unconditional Security to Computational Security: Pseudo-Random Generators and One-way Functions. . . . .	139
3.3.1	Pseudo-Random Generators . . . . .	139
3.3.2	One-Way Functions . . . . .	144
3.3.3	From One-Way Functions to Pseudo-Random Generators: The Blum–Blum–Shub PRG. . . . .	148
3.4	PRGs and Related Constructions in Maple . . . . .	155
3.4.1	The Blum–Blum–Shub PRG in Maple . . . . .	156
3.4.2	An Approximation to the One-Time Pad in Maple . . . . .	158
3.4.3	Practical Security Aspects . . . . .	162
3.5	Private-Key Encryption Schemes and Their Security . . . . .	167
3.5.1	Private-Key Encryption Schemes . . . . .	168
3.5.2	Security Definitions for Private-Key Encryption Schemes . . . . .	169
3.5.3	CPA Security and CCA Security . . . . .	174
3.5.4	Concluding Remarks. . . . .	178
<b>4</b>	<b>Block Ciphers and Modes of Operation. . . . .</b>	<b>181</b>
4.1	Block Ciphers and Pseudo-Random Functions . . . . .	181
4.2	The Advanced Encryption Standard . . . . .	186
4.2.1	The Data Encryption Standard . . . . .	187
4.2.2	Introducing AES. . . . .	189
4.2.3	AES Decryption . . . . .	198
4.2.4	Remarks on AES Design and AES Security. . . . .	200
4.3	Modes of Operation . . . . .	202
4.3.1	Confidentiality Modes. . . . .	202
4.3.2	A CPA Secure Encryption Scheme. . . . .	211

4.4	AES in Maple . . . . .	216
4.4.1	AES Operations in Maple . . . . .	216
4.4.2	AES Encryption and Decryption. . . . .	219
4.5	Some Modes of Operation in Maple . . . . .	222
4.5.1	OFB and CTR in Maple . . . . .	222
4.5.2	Encryption and Decryption with OFB and CTR. . . . .	226
<b>5</b>	<b>Message Authentication . . . . .</b>	<b>231</b>
5.1	Confidentiality Versus Authenticity . . . . .	231
5.2	Message Authentication Codes. . . . .	233
5.2.1	Defining MACs . . . . .	233
5.2.2	Security for MACs . . . . .	234
5.3	Constructing MACs . . . . .	236
5.3.1	MACs from Pseudo-Random Functions. . . . .	236
5.3.2	CBC-MAC . . . . .	238
5.3.3	CMAC and Its Maple Implementation. . . . .	240
5.4	CCA Security and Authenticated Encryption . . . . .	244
5.4.1	A CCA Secure Encryption Scheme. . . . .	244
5.4.2	Obtaining Authenticated Encryption . . . . .	246
5.5	MACs Based on Universal Hashing . . . . .	250
5.5.1	GCM . . . . .	251
5.5.2	GMAC . . . . .	256
5.6	Collision Resistant Hash Functions. . . . .	258
5.6.1	A Couple of Applications . . . . .	260
5.6.2	The Merkle–Damgård Construction . . . . .	261
5.6.3	SHA-256. . . . .	263
5.6.4	SHA-256 in Maple . . . . .	264
5.6.5	MACs with Hash Functions: HMAC. . . . .	268
5.7	The Birthday Attack on Hash Functions . . . . .	271
5.7.1	The Birthday Paradox . . . . .	271
5.7.2	The Birthday Attack . . . . .	274
<b>6</b>	<b>Algorithmic Number Theory for Cryptography and Cryptanalysis: Primality, Factoring and Discrete Logarithms. . . .</b>	<b>283</b>
6.1	Large Primes and How to Find Them . . . . .	283
6.1.1	Searching for Large Random Primes. . . . .	284
6.1.2	The Distribution of Prime Numbers . . . . .	286
6.2	Primality Testing . . . . .	292
6.2.1	The Fermat Test and Pseudoprimes . . . . .	292
6.2.2	The Strong Probable Prime Test. . . . .	299
6.2.3	The Miller–Rabin Test . . . . .	304
6.2.4	Other Primality Tests . . . . .	311
6.3	Generating Random Primes . . . . .	314
6.3.1	Generating Safe Primes. . . . .	317
6.3.2	Generating Pseudo-Random Primes with Maple. . . . .	319

6.4	The Integer Factorization Problem . . . . .	320
6.4.1	Trial Division as a Factoring Algorithm . . . . .	321
6.4.2	Pollard's Rho Method and Its Maple Implementation . . . . .	323
6.4.3	Fermat's Factorization Method. . . . .	326
6.4.4	Fermat's Factorization Method in Maple. . . . .	329
6.4.5	Factor Bases . . . . .	334
6.4.6	The Factor Base Method in Maple . . . . .	340
6.4.7	The Quadratic Sieve . . . . .	353
6.4.8	The Basic QS Algorithm in Maple . . . . .	358
6.4.9	Some Improvements on the Basic QS . . . . .	364
6.4.10	The Current Status of Factorization . . . . .	366
6.5	The Discrete Logarithm Problem . . . . .	371
6.5.1	The Baby-Step Giant-Step Algorithm and Its Maple Implementation . . . . .	372
6.5.2	Pollard's Rho Method for Discrete Logarithms . . . . .	376
6.5.3	The Rho Method for Discrete Logarithms in Maple . . . . .	379
6.5.4	The Pohlig–Hellman Algorithm and Its Maple Implementation . . . . .	382
6.5.5	The Index Calculus Method for Discrete Logarithms . . . . .	385
6.5.6	The Index Calculus Method in Maple. . . . .	389
6.5.7	Extensions of the Index Calculus Method . . . . .	395
6.5.8	Final Remarks on the Discrete Logarithm Problem. . . . .	397
<b>7</b>	<b>Introduction to Public-Key Cryptography:</b>	
	<b>The Diffie–Hellman Protocol . . . . .</b>	<b>399</b>
7.1	From Private-Key to Public-Key Cryptography . . . . .	399
7.2	The Diffie–Hellman Key Agreement. . . . .	403
7.2.1	The DH Protocol and the DH Problems . . . . .	403
7.2.2	Man-in-the-Middle Attacks . . . . .	407
7.2.3	Groups for the DH Protocol. . . . .	408
7.2.4	Attacking the Diffie–Hellman Protocol with Maple . . . . .	412
7.2.5	Concluding Remarks on the Diffie–Hellman Protocol . . . . .	416
<b>8</b>	<b>Public-Key Encryption . . . . .</b>	<b>419</b>
8.1	Public-Key Encryption Schemes. . . . .	419
8.2	Security for Public-Key Encryption . . . . .	422
8.2.1	Definitions of Security . . . . .	423
8.2.2	Hybrid Encryption and Its Security. . . . .	427

8.3	RSA . . . . .	429
8.3.1	The RSA Assumption . . . . .	429
8.3.2	Plain RSA . . . . .	434
8.3.3	Plain RSA in Maple . . . . .	440
8.3.4	Security of RSA . . . . .	447
8.3.5	RSA with Probabilistic Encryption . . . . .	458
8.3.6	RSA-OAEP . . . . .	461
8.3.7	RSAs-OAEP in Maple . . . . .	469
8.4	Rabin Encryption . . . . .	475
8.4.1	Plain Rabin Encryption . . . . .	475
8.4.2	Plain Rabin Encryption in Maple . . . . .	480
8.4.3	CCA Secure Rabin Encryption . . . . .	483
8.4.4	Rabin-SAsEP <sup>+</sup> in Maple . . . . .	489
8.5	The Elgamal Encryption Scheme . . . . .	495
8.5.1	Security of Elgamal . . . . .	497
8.5.2	Elgamal on the Group of Quadratic Residues Modulo a Safe Prime . . . . .	501
8.6	The Cramer–Shoup Encryption Scheme . . . . .	505
8.6.1	Cramer–Shoup Encryption and Its Security . . . . .	505
8.6.2	A Variant of the Cramer–Shoup Encryption Scheme in Maple . . . . .	513
8.7	A Speed Comparison Among Implementations of CCA Secure Schemes . . . . .	520
8.8	Homomorphic Encryption . . . . .	523
8.8.1	The Goldwasser–Micali Encryption Scheme . . . . .	523
8.8.2	The Paillier Encryption Scheme . . . . .	526
8.8.3	The Paillier Encryption Scheme in Maple . . . . .	532
8.9	Final Remarks on Public-Key Encryption . . . . .	533
8.9.1	Fully Homomorphic Encryption . . . . .	534
8.9.2	Lattice-Based Cryptography . . . . .	535
<b>9</b>	<b>Digital Signatures . . . . .</b>	<b>537</b>
9.1	Digital Signature Schemes . . . . .	538
9.1.1	Definition of Signature Schemes . . . . .	538
9.1.2	Security of Signature Schemes . . . . .	539
9.2	Some Early Signature Schemes . . . . .	541
9.2.1	Plain RSA Signatures . . . . .	541
9.2.2	Elgamal Signatures . . . . .	543
9.3	The “Hash-then-Decrypt” Paradigm . . . . .	544
9.3.1	Hashed RSA Signatures . . . . .	545
9.3.2	Hashed Elgamal Signatures . . . . .	546
9.4	The Digital Signature Algorithm . . . . .	548
9.4.1	The DSA Signature Scheme . . . . .	549
9.4.2	DSA Security . . . . .	551
9.4.3	DSA in Maple . . . . .	553

9.5	CMA Secure Signature Schemes . . . . .	560
9.5.1	FDH Signatures . . . . .	560
9.5.2	PSS Signatures . . . . .	564
9.5.3	RSASSA-PSS from PKCS #1 v2.1 . . . . .	567
9.5.4	RSASSA-PSS in Maple . . . . .	570
9.5.5	Cramer–Shoup Signatures . . . . .	576
9.6	Signatures with Added Functionality . . . . .	578
9.6.1	Blind Signatures . . . . .	578
9.6.2	Other Signatures with Added Functionality . . . . .	580
9.7	Public-Key Infrastructures . . . . .	581
9.7.1	Certificates . . . . .	581
9.7.2	Multiple Certification Authorities . . . . .	583
<b>10</b>	<b>Identity-Based Cryptography . . . . .</b>	<b>587</b>
10.1	Introducing Identity-Based Cryptography . . . . .	587
10.2	Identity-Based Signatures . . . . .	590
10.2.1	IBS Schemes . . . . .	590
10.2.2	From Signature Schemes to IBS Schemes . . . . .	591
10.3	Identity-Based Encryption . . . . .	593
10.3.1	IBE Definition . . . . .	593
10.3.2	Applications of IBE . . . . .	594
10.3.3	The Cocks IBE Scheme . . . . .	595
10.3.4	The Cocks IBE Scheme in Maple . . . . .	599
10.4	The Boneh–Franklin IBE Scheme . . . . .	605
10.4.1	Pairings . . . . .	605
10.4.2	The Boneh–Franklin Scheme . . . . .	607
10.5	Final Remarks on Identity-Based Cryptography . . . . .	610
<b>11</b>	<b>An Introduction to Elliptic Curve Cryptography . . . . .</b>	<b>611</b>
11.1	Elliptic Curves and Their Group Structure . . . . .	613
11.1.1	Definition of Elliptic Curve . . . . .	613
11.1.2	The Group Structure on an Elliptic Curve . . . . .	616
11.2	Elliptic Curves Over Finite Fields . . . . .	624
11.2.1	Some Small Examples . . . . .	624
11.2.2	Elliptic Curve Elementary Computations . . . . .	626
11.2.3	The Orders of Elliptic Curve Groups . . . . .	632
11.2.4	Elliptic Curve Groups Over Prime Fields in Maple . . . . .	639
11.3	The Elliptic Curve Discrete Logarithm Problem . . . . .	648
11.3.1	The Rho Method and Pohlig–Hellman for the ECDLP in Maple . . . . .	649
11.3.2	The Current State of the ECDLP . . . . .	653
11.3.3	Reduction Attacks Against the ECDLP . . . . .	655
11.3.4	Final Remarks on the ECDLP . . . . .	660

11.4	Elliptic Curve Schemes . . . . .	662
11.4.1	ECC Schemes and Their Domain Parameters. . . . .	662
11.4.2	The Elliptic Curve Digital Signature Algorithm (ECDSA) . . . . .	665
11.4.3	ECDSA in Maple . . . . .	668
11.4.4	Elliptic Curve Encryption . . . . .	673
11.5	Final Remarks on Elliptic Curve Cryptography . . . . .	676
<b>Appendix A: Some Maple Conversion Functions . . . . .</b>		<b>677</b>
<b>References . . . . .</b>		<b>685</b>
<b>Index . . . . .</b>		<b>695</b>



<http://www.springer.com/978-3-642-32166-5>

Introduction to Cryptography with Maple

Gómez Pardo, J.L.

2013, XXX, 706 p.,

ISBN: 978-3-642-32166-5