

# Contents

<b>1</b>	<b>Classical Cryptography</b>	<b>1</b>
1.1	Introduction: Some Simple Cryptosystems	1
1.1.1	The Shift Cipher	3
1.1.2	The Substitution Cipher	7
1.1.3	The Affine Cipher	8
1.1.4	The Vigenère Cipher	12
1.1.5	The Hill Cipher	13
1.1.6	The Permutation Cipher	19
1.1.7	Stream Ciphers	21
1.2	Cryptanalysis	26
1.2.1	Cryptanalysis of the Affine Cipher	27
1.2.2	Cryptanalysis of the Substitution Cipher	29
1.2.3	Cryptanalysis of the Vigenère Cipher	32
1.2.4	Cryptanalysis of the Hill Cipher	36
1.2.5	Cryptanalysis of the LFSR Stream Cipher	37
1.3	Notes	39
	Exercises	39
<b>2</b>	<b>Shannon's Theory</b>	<b>45</b>
2.1	Introduction	45
2.2	Elementary Probability Theory	46
2.3	Perfect Secrecy	48
2.4	Entropy	54
2.4.1	Huffman Encodings	56
2.5	Properties of Entropy	59
2.6	Spurious Keys and Unicity Distance	62
2.7	Product Cryptosystems	67
2.8	Notes	70
	Exercises	70

<b>3</b>	<b>Block Ciphers and the Advanced Encryption Standard</b>	<b>73</b>
3.1	Introduction . . . . .	73
3.2	Substitution-Permutation Networks . . . . .	74
3.3	Linear Cryptanalysis . . . . .	79
3.3.1	The Piling-up Lemma . . . . .	80
3.3.2	Linear Approximations of S-boxes . . . . .	82
3.3.3	A Linear Attack on an SPN . . . . .	84
3.4	Differential Cryptanalysis . . . . .	89
3.5	The Data Encryption Standard . . . . .	95
3.5.1	Description of DES . . . . .	95
3.5.2	Analysis of DES . . . . .	100
3.6	The Advanced Encryption Standard . . . . .	102
3.6.1	Description of AES . . . . .	103
3.6.2	Analysis of AES . . . . .	108
3.7	Modes of Operation . . . . .	109
3.8	Notes and References . . . . .	113
	Exercises . . . . .	114
<b>4</b>	<b>Cryptographic Hash Functions</b>	<b>119</b>
4.1	Hash Functions and Data Integrity . . . . .	119
4.2	Security of Hash Functions . . . . .	121
4.2.1	The Random Oracle Model . . . . .	122
4.2.2	Algorithms in the Random Oracle Model . . . . .	123
4.2.3	Comparison of Security Criteria . . . . .	127
4.3	Iterated Hash Functions . . . . .	129
4.3.1	The Merkle-Damgård Construction . . . . .	131
4.3.2	The Secure Hash Algorithm . . . . .	137
4.4	Message Authentication Codes . . . . .	140
4.4.1	Nested MACs and HMAC . . . . .	141
4.4.2	CBC-MAC and Authenticated Encryption . . . . .	144
4.5	Unconditionally Secure MACs . . . . .	145
4.5.1	Strongly Universal Hash Families . . . . .	148
4.5.2	Optimality of Deception Probabilities . . . . .	151
4.6	Notes and References . . . . .	153
	Exercises . . . . .	155
<b>5</b>	<b>The RSA Cryptosystem and Factoring Integers</b>	<b>161</b>
5.1	Introduction to Public-key Cryptography . . . . .	161
5.2	More Number Theory . . . . .	163
5.2.1	The Euclidean Algorithm . . . . .	163
5.2.2	The Chinese Remainder Theorem . . . . .	167
5.2.3	Other Useful Facts . . . . .	170
5.3	The RSA Cryptosystem . . . . .	173
5.3.1	Implementing RSA . . . . .	174

5.4	Primality Testing . . . . .	178
5.4.1	Legendre and Jacobi Symbols . . . . .	179
5.4.2	The Solovay-Strassen Algorithm . . . . .	182
5.4.3	The Miller-Rabin Algorithm . . . . .	186
5.5	Square Roots Modulo $n$ . . . . .	187
5.6	Factoring Algorithms . . . . .	189
5.6.1	The Pollard $p - 1$ Algorithm . . . . .	189
5.6.2	The Pollard Rho Algorithm . . . . .	191
5.6.3	Dixon's Random Squares Algorithm . . . . .	194
5.6.4	Factoring Algorithms in Practice . . . . .	199
5.7	Other Attacks on RSA . . . . .	201
5.7.1	Computing $\phi(n)$ . . . . .	201
5.7.2	The Decryption Exponent . . . . .	202
5.7.3	Wiener's Low Decryption Exponent Attack . . . . .	207
5.8	The Rabin Cryptosystem . . . . .	211
5.8.1	Security of the Rabin Cryptosystem . . . . .	213
5.9	Semantic Security of RSA . . . . .	215
5.9.1	Partial Information Concerning Plaintext Bits . . . . .	215
5.9.2	Optimal Asymmetric Encryption Padding . . . . .	218
5.10	Notes and References . . . . .	225
	Exercises . . . . .	226
<b>6</b>	<b>Public-key Cryptography and Discrete Logarithms</b>	<b>233</b>
6.1	The ElGamal Cryptosystem . . . . .	233
6.2	Algorithms for the Discrete Logarithm Problem . . . . .	236
6.2.1	Shanks' Algorithm . . . . .	236
6.2.2	The Pollard Rho Discrete Logarithm Algorithm . . . . .	238
6.2.3	The Pohlig-Hellman Algorithm . . . . .	241
6.2.4	The Index Calculus Method . . . . .	244
6.3	Lower Bounds on the Complexity of Generic Algorithms . . . . .	246
6.4	Finite Fields . . . . .	250
6.5	Elliptic Curves . . . . .	254
6.5.1	Elliptic Curves over the Reals . . . . .	255
6.5.2	Elliptic Curves Modulo a Prime . . . . .	257
6.5.3	Properties of Elliptic Curves . . . . .	261
6.5.4	Point Compression and the ECIES . . . . .	262
6.5.5	Computing Point Multiples on Elliptic Curves . . . . .	265
6.6	Discrete Logarithm Algorithms in Practice . . . . .	267
6.7	Security of ElGamal Systems . . . . .	268
6.7.1	Bit Security of Discrete Logarithms . . . . .	268
6.7.2	Semantic Security of ElGamal Systems . . . . .	272
6.7.3	The Diffie-Hellman Problems . . . . .	273
6.8	Notes and References . . . . .	274
	Exercises . . . . .	275

<b>7</b>	<b>Signature Schemes</b>	<b>281</b>
7.1	Introduction . . . . .	281
7.2	Security Requirements for Signature Schemes . . . . .	284
7.2.1	Signatures and Hash Functions . . . . .	286
7.3	The ElGamal Signature Scheme . . . . .	287
7.3.1	Security of the ElGamal Signature Scheme . . . . .	289
7.4	Variants of the ElGamal Signature Scheme . . . . .	292
7.4.1	The Schnorr Signature Scheme . . . . .	293
7.4.2	The Digital Signature Algorithm . . . . .	294
7.4.3	The Elliptic Curve DSA . . . . .	297
7.5	Provably Secure Signature Schemes . . . . .	299
7.5.1	One-time Signatures . . . . .	299
7.5.2	Full Domain Hash . . . . .	304
7.6	Undeniable Signatures . . . . .	307
7.7	Fail-stop Signatures . . . . .	313
7.8	Notes and References . . . . .	317
	Exercises . . . . .	318
<b>8</b>	<b>Pseudo-random Number Generation</b>	<b>323</b>
8.1	Introduction and Examples . . . . .	323
8.2	Indistinguishability of Probability Distributions . . . . .	327
8.2.1	Next Bit Predictors . . . . .	330
8.3	The Blum-Blum-Shub Generator . . . . .	336
8.3.1	Security of the BBS Generator . . . . .	339
8.4	Probabilistic Encryption . . . . .	344
8.5	Notes and References . . . . .	349
	Exercises . . . . .	350
<b>9</b>	<b>Identification Schemes and Entity Authentication</b>	<b>353</b>
9.1	Introduction . . . . .	353
9.2	Challenge-and-Response in the Secret-key Setting . . . . .	356
9.2.1	Attack Model and Adversarial Goals . . . . .	361
9.2.2	Mutual Authentication . . . . .	363
9.3	Challenge-and-Response in the Public-key Setting . . . . .	367
9.3.1	Certificates . . . . .	367
9.3.2	Public-key Identification Schemes . . . . .	368
9.4	The Schnorr Identification Scheme . . . . .	371
9.4.1	Security of the Schnorr Identification Scheme . . . . .	374
9.5	The Okamoto Identification Scheme . . . . .	378
9.6	The Guillou-Quisquater Identification Scheme . . . . .	383
9.6.1	Identity-based Identification Schemes . . . . .	386
9.7	Notes and References . . . . .	387
	Exercises . . . . .	388

<b>10 Key Distribution</b>	<b>393</b>
10.1 Introduction	393
10.2 Diffie-Hellman Key Predistribution	397
10.3 Unconditionally Secure Key Predistribution	399
10.3.1 The Blom Key Predistribution Scheme	399
10.4 Key Distribution Patterns	406
10.4.1 Fiat-Naor Key Distribution Patterns	409
10.4.2 Mitchell-Piper Key Distribution Patterns	410
10.5 Session Key Distribution Schemes	414
10.5.1 The Needham-Schroeder Scheme	415
10.5.2 The Denning-Sacco Attack on the NS Scheme	416
10.5.3 Kerberos	417
10.5.4 The Bellare-Rogaway Scheme	421
10.6 Notes and References	424
Exercises	424
<b>11 Key Agreement Schemes</b>	<b>429</b>
11.1 Introduction	429
11.2 Diffie-Hellman Key Agreement	429
11.2.1 The Station-to-station Key Agreement Scheme	431
11.2.2 Security of STS	432
11.2.3 Known Session Key Attacks	436
11.3 MTI Key Agreement Schemes	438
11.3.1 Known Session Key Attacks on MTI/A0	441
11.4 Key Agreement Using Self-certifying Keys	444
11.5 Encrypted Key Exchange	448
11.6 Conference Key Agreement Schemes	450
11.7 Notes and References	453
Exercises	455
<b>12 Public-key Infrastructure</b>	<b>457</b>
12.1 Introduction: What is a PKI?	457
12.1.1 A Practical Protocol: Secure Socket Layer	459
12.2 Certificates	461
12.2.1 Certificate Life-cycle Management	463
12.3 Trust Models	464
12.3.1 Strict Hierarchy Model	464
12.3.2 Networked PKIs	466
12.3.3 The Web Browser Model	467
12.3.4 Pretty Good Privacy	468
12.4 The Future of PKI?	471
12.4.1 Alternatives to PKI	471
12.5 Identity-based Cryptography	472
12.5.1 The Cocks Identity-based Encryption Scheme	473

12.6	Notes and References . . . . .	479
	Exercises . . . . .	480
<b>13</b>	<b>Secret Sharing Schemes</b>	<b>481</b>
13.1	Introduction: The Shamir Threshold Scheme . . . . .	481
13.1.1	A Simplified $(t, t)$ -threshold Scheme . . . . .	485
13.2	Access Structures and General Secret Sharing . . . . .	486
13.2.1	The Monotone Circuit Construction . . . . .	488
13.2.2	Formal Definitions . . . . .	493
13.3	Information Rate and Construction of Efficient Schemes	496
13.3.1	The Vector Space Construction . . . . .	498
13.3.2	An Upper Bound on the Information Rate . . . . .	505
13.3.3	The Decomposition Construction . . . . .	509
13.4	Notes and References . . . . .	513
	Exercises . . . . .	514
<b>14</b>	<b>Multicast Security and Copyright Protection</b>	<b>517</b>
14.1	Introduction to Multicast Security . . . . .	517
14.2	Broadcast Encryption . . . . .	518
14.2.1	An Improvement using Ramp Schemes . . . . .	528
14.3	Multicast Re-keying . . . . .	531
14.3.1	The Blacklisting Scheme . . . . .	533
14.3.2	The Naor-Pinkas Re-keying Scheme . . . . .	534
14.3.3	Logical Key Hierarchy . . . . .	537
14.4	Copyright Protection . . . . .	539
14.4.1	Fingerprinting . . . . .	540
14.4.2	Identifiable Parent Property . . . . .	542
14.4.3	2-IPP Codes . . . . .	544
14.5	Tracing Illegally Redistributed Keys . . . . .	548
14.6	Notes and References . . . . .	552
	Exercises . . . . .	552
	<b>Further Reading</b>	<b>557</b>
	<b>Bibliography</b>	<b>561</b>
	<b>Index</b>	<b>583</b>