

Contents

1. Introduction	1
1.1 Encryption and Secrecy	1
1.2 The Objectives of Cryptography	2
1.3 Attacks	4
1.4 Cryptographic Protocols	5
1.5 Provable Security	6
2. Symmetric-Key Encryption	11
2.1 Stream Ciphers	12
2.2 Block Ciphers	15
2.2.1 DES	16
2.2.2 AES	19
2.2.3 Modes of Operation	25
3. Public-Key Cryptography	33
3.1 The Concept of Public-Key Cryptography	33
3.2 Modular Arithmetic	35
3.2.1 The Integers	35
3.2.2 The Integers Modulo n	37
3.3 RSA	41
3.3.1 Key Generation and Encryption	41
3.3.2 Digital Signatures	45
3.3.3 Attacks Against RSA	46
3.3.4 Probabilistic RSA Encryption	51
3.4 Cryptographic Hash Functions	54
3.4.1 Security Requirements for Hash Functions	54
3.4.2 Construction of Hash Functions	56
3.4.3 Data Integrity and Message Authentication	62
3.4.4 Hash Functions as Random Functions	64
3.4.5 Signatures with Hash Functions	65
3.5 The Discrete Logarithm	70
3.5.1 ElGamal's Encryption	70
3.5.2 ElGamal's Signature Scheme	72
3.5.3 Digital Signature Algorithm	73

3.6	Modular Squaring	76
3.6.1	Rabin's Encryption	76
3.6.2	Rabin's Signature Scheme	77
4.	Cryptographic Protocols	81
4.1	Key Exchange and Entity Authentication	81
4.1.1	Kerberos	82
4.1.2	Diffie-Hellman Key Agreement	85
4.1.3	Key Exchange and Mutual Authentication	86
4.1.4	Station-to-Station Protocol	88
4.1.5	Public-Key Management Techniques	89
4.2	Identification Schemes	91
4.2.1	Interactive Proof Systems	91
4.2.2	Simplified Fiat-Shamir Identification Scheme	93
4.2.3	Zero-Knowledge	95
4.2.4	Fiat-Shamir Identification Scheme	97
4.2.5	Fiat-Shamir Signature Scheme	99
4.3	Commitment Schemes	100
4.3.1	A Commitment Scheme Based on Quadratic Residues	101
4.3.2	A Commitment Scheme Based on Discrete Logarithms	102
4.3.3	Homomorphic Commitments	103
4.4	Electronic Elections	104
4.4.1	Secret Sharing	105
4.4.2	A Multi-Authority Election Scheme	107
4.4.3	Proofs of Knowledge	110
4.4.4	Non-Interactive Proofs of Knowledge	112
4.4.5	Extension to Multi-Way Elections	112
4.4.6	Eliminating the Trusted Center	113
4.5	Digital Cash	115
4.5.1	Blindly Issued Proofs	117
4.5.2	A Fair Electronic Cash System	123
4.5.3	Underlying Problems	128
5.	Probabilistic Algorithms	135
5.1	Coin-Tossing Algorithms	135
5.2	Monte Carlo and Las Vegas Algorithms	140
6.	One-Way Functions and the Basic Assumptions	147
6.1	A Notation for Probabilities	148
6.2	Discrete Exponential Function	149
6.3	Uniform Sampling Algorithms	155
6.4	Modular Powers	158
6.5	Modular Squaring	161
6.6	Quadratic Residuosity Property	162
6.7	Formal Definition of One-Way Functions	163

6.8	Hard-Core Predicates	167
7.	Bit Security of One-Way Functions	175
7.1	Bit Security of the Exp Family	175
7.2	Bit Security of the RSA Family	182
7.3	Bit Security of the Square Family	190
8.	One-Way Functions and Pseudorandomness	199
8.1	Computationally Perfect Pseudorandom Bit Generators	199
8.2	Yao's Theorem	207
9.	Provably Secure Encryption	215
9.1	Classical Information-Theoretic Security	216
9.2	Perfect Secrecy and Probabilistic Attacks	220
9.3	Public-Key One-Time Pads	224
9.4	Passive Eavesdroppers	226
9.5	Chosen-Ciphertext Attacks	233
9.5.1	A Security Proof in the Random Oracle Model	236
9.5.2	Security Under Standard Assumptions	245
9.6	Unconditional Security of Cryptosystems	250
9.6.1	The Bounded Storage Model	251
9.6.2	The Noisy Channel Model	260
10.	Provably Secure Digital Signatures	265
10.1	Attacks and Levels of Security	265
10.2	Claw-Free Pairs and Collision-Resistant Hash Functions	268
10.3	Authentication-Tree-Based Signatures	271
10.4	A State-Free Signature Scheme	273
A.	Algebra and Number Theory	289
A.1	The Integers	289
A.2	Residues	295
A.3	The Chinese Remainder Theorem	299
A.4	Primitive Roots and the Discrete Logarithm	301
A.5	Polynomials and Finite Fields	304
A.5.1	The Ring of Polynomials	305
A.5.2	Residue Class Rings	307
A.5.3	Finite Fields	309
A.6	Quadratic Residues	310
A.7	Modular Square Roots	315
A.8	Primes and Primality Tests	319

B. Probabilities and Information Theory	325
B.1 Finite Probability Spaces and Random Variables	325
B.2 The Weak Law of Large Numbers	333
B.3 Distance Measures	336
B.4 Basic Concepts of Information Theory	340
References	349
Index	361