

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	14
2.2.1 DES	15
2.2.2 Modes of Operation	18
3. Public-Key Cryptography	23
3.1 The Concept of Public-Key Cryptography	23
3.2 Modular Arithmetic	25
3.2.1 The Integers	25
3.2.2 The Integers Modulo n	27
3.3 RSA	31
3.3.1 Key Generation and Encryption	31
3.3.2 Digital Signatures	35
3.3.3 Attacks Against RSA	36
3.3.4 The Secure Application of RSA Encryption	37
3.4 Hash Functions	39
3.4.1 Merkle's Meta Method	40
3.4.2 Construction of Hash Functions	41
3.4.3 Probabilistic Signatures	43
3.5 The Discrete Logarithm	46
3.5.1 ElGamal's Encryption	47
3.5.2 ElGamal's Signature Scheme	48
3.5.3 Digital Signature Algorithm	49
3.6 Modular Squaring	52
3.6.1 Rabin's Encryption	52
3.6.2 Rabin's Signature Scheme	54

4. Cryptographic Protocols	57
4.1 Key Exchange and Entity Authentication	57
4.1.1 Kerberos	58
4.1.2 Diffie-Hellman Key Agreement	61
4.1.3 Key Exchange and Mutual Authentication	62
4.1.4 Station-to-Station Protocol	64
4.1.5 Public-Key Management Techniques	65
4.2 Identification Schemes	67
4.2.1 Interactive Proof Systems	67
4.2.2 Simplified Fiat-Shamir Identification Scheme	69
4.2.3 Zero-Knowledge	71
4.2.4 Fiat-Shamir Identification Scheme	73
4.2.5 Fiat-Shamir Signature Scheme	75
4.3 Commitment Schemes	76
4.3.1 A Commitment Scheme Based on Quadratic Residues	77
4.3.2 A Commitment Scheme Based on Discrete Logarithms	78
4.3.3 Homomorphic Commitments	79
4.4 Electronic Elections	80
4.4.1 Secret Sharing	81
4.4.2 A Multi-Authority Election Scheme	83
4.4.3 Proofs of Knowledge	86
4.4.4 Non-Interactive Proofs of Knowledge	88
4.4.5 Extension to Multi-Way Elections	88
4.4.6 Eliminating the Trusted Center	89
4.5 Digital Cash	91
4.5.1 Blindly Issued Proofs	93
4.5.2 A Fair Electronic Cash System	99
4.5.3 Underlying Problems	104
5. Probabilistic Algorithms	111
5.1 Coin-Tossing Algorithms	111
5.2 Monte Carlo and Las Vegas Algorithms	116
6. One-Way Functions and the Basic Assumptions	123
6.1 A Notation for Probabilities	124
6.2 Discrete Exponential Function	125
6.3 Uniform Sampling Algorithms	131
6.4 Modular Powers	134
6.5 Modular Squaring	137
6.6 Quadratic Residuosity Property	138
6.7 Formal Definition of One-Way Functions	139
6.8 Hard-Core Predicates	143

7. Bit Security of One-Way Functions	151
7.1 Bit Security of the Exp Family	151
7.2 Bit Security of the RSA Family	158
7.3 Bit Security of the Square Family	166
8. One-Way Functions and Pseudorandomness	175
8.1 Computationally Perfect Pseudorandom Bit Generators	175
8.2 Yao's Theorem	183
9. Provably Secure Encryption	191
9.1 Classical Information-Theoretic Security	191
9.2 Perfect Secrecy and Probabilistic Attacks	196
9.3 Public-Key One-Time Pads	199
9.4 Computationally Secret Encryption Schemes	202
9.5 Unconditional Security of Cryptosystems	208
9.5.1 The Bounded Storage Model	209
9.5.2 The Noisy Channel Model	217
10. Provably Secure Digital Signatures	221
10.1 Attacks and Levels of Security	221
10.2 Claw-Free Pairs and Collision-Resistant Hash Functions	224
10.3 Authentication-Tree-Based Signatures	227
10.4 A State-Free Signature Scheme	229
A. Algebra and Number Theory	245
A.1 The Integers	245
A.2 Residues	251
A.3 The Chinese Remainder Theorem	255
A.4 Primitive Roots and the Discrete Logarithm	257
A.5 Quadratic Residues	259
A.6 Modular Square Roots	264
A.7 Primes and Primality Tests	268
B. Probabilities and Information Theory	273
B.1 Finite Probability Spaces and Random Variables	273
B.2 The Weak Law of Large Numbers	281
B.3 Distance Measures	284
B.4 Basic Concepts of Information Theory	288
References	297
Index	305