

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 Cryptography	11
2.1 Symmetric-Key Encryption	11
2.1.1 Stream Ciphers	12
2.1.2 Block Ciphers	15
2.1.3 DES	16
2.1.4 AES	19
2.1.5 Modes of Operation	25
2.2 Cryptographic Hash Functions	30
2.2.1 Security Requirements for Hash Functions	30
2.2.2 Construction of Hash Functions	32
2.2.3 Data Integrity and Message Authentication	42
2.2.4 Hash Functions as Random Functions	44
3. Public-Key Cryptography	49
3.1 The Concept of Public-Key Cryptography	49
3.2 Modular Arithmetic	51
3.2.1 The Integers	51
3.2.2 The Integers Modulo n	53
3.3 RSA	58
3.3.1 Key Generation and Encryption	58
3.3.2 Attacks Against RSA Encryption	62
3.3.3 Probabilistic RSA Encryption	67
3.3.4 Digital Signatures — The Basic Scheme	70
3.3.5 Signatures with Hash Functions	71
3.4 The Discrete Logarithm	77
3.4.1 ElGamal Encryption	77
3.4.2 ElGamal Signatures	78

3.4.3	Digital Signature Algorithm	80
3.4.4	ElGamal Encryption in a Prime-Order Subgroup	82
3.5	Modular Squaring	85
3.5.1	Rabin's Encryption	85
3.5.2	Rabin's Signature Scheme	86
3.6	Homomorphic Encryption Algorithms	87
3.6.1	ElGamal Encryption	87
3.6.2	Paillier Encryption	88
3.6.3	Re-encryption of Ciphertexts	89
3.7	Elliptic Curve Cryptography	90
3.7.1	Selecting the Curve and the Base Point	93
3.7.2	Diffie–Hellman Key Exchange	98
3.7.3	ElGamal Encryption	100
3.7.4	Elliptic Curve Digital Signature Algorithm	102
4.	Cryptographic Protocols	107
4.1	Key Exchange and Entity Authentication	107
4.1.1	Kerberos	108
4.1.2	Diffie–Hellman Key Agreement	111
4.1.3	Key Exchange and Mutual Authentication	112
4.1.4	Station-to-Station Protocol	114
4.1.5	Public-Key Management Techniques	115
4.2	Identification Schemes	117
4.2.1	Interactive Proof Systems	117
4.2.2	Simplified Fiat–Shamir Identification Scheme	119
4.2.3	Zero-Knowledge	121
4.2.4	Fiat–Shamir Identification Scheme	123
4.2.5	Fiat–Shamir Signature Scheme	125
4.3	Commitment Schemes	126
4.3.1	A Commitment Scheme Based on Quadratic Residues	127
4.3.2	A Commitment Scheme Based on Discrete Logarithms	128
4.3.3	Homomorphic Commitments	129
4.4	Secret Sharing	130
4.5	Verifiable Electronic Elections	133
4.5.1	A Multi-authority Election Scheme	135
4.5.2	Proofs of Knowledge	138
4.5.3	Non-interactive Proofs of Knowledge	142
4.5.4	Extension to Multi-way Elections	143
4.5.5	Eliminating the Trusted Center	144
4.6	Mix Nets and Shuffles	146
4.6.1	Decryption Mix Nets	147
4.6.2	Re-encryption Mix Nets	150
4.6.3	Proving Knowledge of the Plaintext	153
4.6.4	Zero-Knowledge Proofs of Shuffles	154
4.7	Receipt-Free and Coercion-Resistant Elections	168

4.7.1	Receipt-Freeness by Randomized Re-encryption	169
4.7.2	A Coercion-Resistant Protocol	176
4.8	Digital Cash	184
4.8.1	Blindly Issued Proofs	186
4.8.2	A Fair Electronic Cash System	192
4.8.3	Underlying Problems	197
5.	Probabilistic Algorithms	203
5.1	Coin-Tossing Algorithms	203
5.2	Monte Carlo and Las Vegas Algorithms	208
6.	One-Way Functions and the Basic Assumptions	215
6.1	A Notation for Probabilities	216
6.2	Discrete Exponential Function	217
6.3	Uniform Sampling Algorithms	223
6.4	Modular Powers	226
6.5	Modular Squaring	229
6.6	Quadratic Residuosity Property	230
6.7	Formal Definition of One-Way Functions	231
6.8	Hard-Core Predicates	235
7.	Bit Security of One-Way Functions	243
7.1	Bit Security of the Exp Family	243
7.2	Bit Security of the RSA Family	250
7.3	Bit Security of the Square Family	258
8.	One-Way Functions and Pseudorandomness	267
8.1	Computationally Perfect Pseudorandom Bit Generators	267
8.2	Yao's Theorem	275
9.	Provably Secure Encryption	283
9.1	Classical Information-Theoretic Security	284
9.2	Perfect Secrecy and Probabilistic Attacks	288
9.3	Public-Key One-Time Pads	292
9.4	Passive Eavesdroppers	294
9.5	Chosen-Ciphertext Attacks	301
9.5.1	A Security Proof in the Random Oracle Model	304
9.5.2	Security Under Standard Assumptions	313
10.	Unconditional Security of Cryptosystems	321
10.1	The Bounded Storage Model	322
10.2	The Noisy Channel Model	332
10.3	Unconditionally Secure Message Authentication	333
10.3.1	Almost Universal Classes of Hash Functions	333
10.3.2	Message Authentication with Universal Hash Families	335

10.3.3	Authenticating Multiple Messages	336
10.4	Collision Entropy and Privacy Amplification	337
10.4.1	Rényi Entropy	338
10.4.2	Privacy Amplification	340
10.4.3	Extraction of a Secret Key	341
10.5	Quantum Key Distribution	343
10.5.1	Quantum Bits and Quantum Measurements	344
10.5.2	The BB84 Protocol	350
10.5.3	Estimation of the Error Rate	353
10.5.4	Intercept-and-Resend Attacks	354
10.5.5	Information Reconciliation	362
10.5.6	Exchanging a Secure Key – An Example	367
10.5.7	General Attacks and Security Proofs	368
11.	Provably Secure Digital Signatures	373
11.1	Attacks and Levels of Security	373
11.2	Claw-Free Pairs and Collision-Resistant Hash Functions	376
11.3	Authentication-Tree-Based Signatures	379
11.4	A State-Free Signature Scheme	381
A.	Algebra and Number Theory	397
A.1	The Integers	397
A.2	Residues	403
A.3	The Chinese Remainder Theorem	407
A.4	Primitive Roots and the Discrete Logarithm	409
A.5	Polynomials and Finite Fields	413
A.5.1	The Ring of Polynomials	413
A.5.2	Residue Class Rings	415
A.5.3	Finite Fields	417
A.6	Solving Quadratic Equations in Binary Fields	419
A.7	Quadratic Residues	421
A.8	Modular Square Roots	426
A.9	The Group $\mathbb{Z}_{n^2}^*$	430
A.10	Primes and Primality Tests	432
A.11	Elliptic Curves	437
A.11.1	Plane Curves	438
A.11.2	Normal Forms of Elliptic Curves	446
A.11.3	Point Addition on Elliptic Curves	449
A.11.4	Group Order and Group Structure of Elliptic Curves	455
B.	Probabilities and Information Theory	458
B.1	Finite Probability Spaces and Random Variables	458
B.2	Some Useful and Important Inequalities	466
B.3	The Weak Law of Large Numbers	469
B.4	Distance Measures	471

B.5 Basic Concepts of Information Theory	475
References	483
Index	501