

Table of Contents

1	Introduction	1
1.1	Preamble	1
1.2	Terminology	3
1.3	Historical Perspective	6
1.4	Modern Cryptography	8
2	Background Theory	11
2.1	Elements of Number Theory	11
2.1.1	Divisibility and the Euclid Algorithm	11
2.1.2	Primes and the Sieve of Eratosthenes	15
2.1.3	Congruences	16
2.1.4	Computing Inverses in Congruences	19
2.1.5	Legendre and Jacobi Symbols	25
2.1.6	Chinese Remainder Theorem	26
2.2	Algebraic Structures in Computing	28
2.2.1	Sets and Operations	28
2.2.2	Polynomial Arithmetic	32
2.2.3	Computing in Galois Fields	36
2.3	Complexity of Computing	38
2.3.1	Asymptotic Behavior of Functions	38
2.3.2	Hierarchy of Functions	39
2.3.3	Problems and Algorithms	41
2.3.4	Classes P and NP	42
2.3.5	NP Completeness	44
2.3.6	Complementary Problems in NP	46
2.3.7	NP -Hard and #P -Complete Problems	48
2.3.8	Problems Used in Cryptography	49
2.3.9	Probabilistic Computations	51

2.3.10	Quantum Computing	52
2.4	Elements of Information Theory	52
2.4.1	Entropy	53
2.4.2	Huffman Codes	55
2.4.3	Redundancy of the Language	57
2.4.4	Key Equivocation and Unicity Distance	60
2.4.5	Equivocation of a Simple Cryptographic System	62
2.5	Problems and Exercises	66
3	Private-Key Cryptosystems	69
3.1	Classical Ciphers	69
3.1.1	Caesar Ciphers	70
3.1.2	Affine Ciphers	72
3.1.3	Monoalphabetic Substitution Ciphers	74
3.1.4	Transposition Ciphers	76
3.1.5	Homophonic Substitution Ciphers	79
3.1.6	Polyalphabetic Substitution Ciphers	81
3.1.7	Cryptanalysis of Polyalphabetic Substitution Ciphers	83
3.2	DES Family	89
3.2.1	Product Ciphers	90
3.2.2	Lucifer Algorithm	93
3.2.3	DES Algorithm	94
3.2.4	DES Modes of Operation	102
3.2.5	Triple DES	104
3.3	Modern Private-Key Cryptographic Algorithms	106
3.3.1	Fast Encryption Algorithm (FEAL)	106
3.3.2	IDEA	106
3.3.3	RC6	110
3.3.4	Rijndael	112
3.3.5	Serpent	117
3.3.6	Other Ciphers	121
3.4	Differential Cryptanalysis	122
3.4.1	XOR Profiles	123
3.4.2	DES Round Characteristics	127
3.4.3	Cryptanalysis of 4-Round DES	129
3.4.4	Cryptanalysis of 6-Round DES	131

3.4.5	Analysis of Other Feistel-Type Cryptosystems	134
3.5	Linear Cryptanalysis	135
3.5.1	Linear Approximation	136
3.5.2	Analysis of 3-Round DES	140
3.5.3	Linear Characteristics	141
3.6	S-box Theory	144
3.6.1	Boolean Functions	145
3.6.2	S-box Design Criteria	149
3.6.3	Bent Functions	156
3.6.4	Propagation and Nonlinearity	158
3.6.5	Constructions of Balanced Functions	161
3.6.6	S-box Design	165
3.7	Problems and Exercises	167
4	Public-Key Cryptosystems	171
4.1	Concept of Public-Key Cryptography	171
4.2	RSA Cryptosystem	174
4.2.1	Variants of RSA	176
4.2.2	Primality Testing	178
4.2.3	Factorization	180
4.2.4	Security of RSA	186
4.3	Merkle-Hellman Cryptosystem	189
4.3.1	Security of Merkle-Hellman Cryptosystem	192
4.4	McEliece Cryptosystem	192
4.4.1	Security of McEliece Cryptosystem	194
4.5	ElGamal Cryptosystem	195
4.5.1	Security of ElGamal Cryptosystem	196
4.6	Elliptic Cryptosystems	196
4.6.1	Elliptic Curves	197
4.6.2	Addition of Points	199
4.6.3	Elliptic Curve Variant of RSA	201
4.6.4	Elliptic Curve Variant of ElGamal	205
4.7	Probabilistic Encryption	206
4.7.1	GM Probabilistic Encryption	207
4.7.2	BG Probabilistic Encryption	208
4.8	Public-Key Encryption Practice	209

4.8.1	Taxonomy of Public-Key Encryption Security	209
4.8.2	Generic OAEP Public-Key Cryptosystem	211
4.8.3	RSA Encryption Standard	213
4.8.4	Extended ElGamal Cryptosystem	214
4.9	Problems and Exercises	216
5	Pseudorandomness	219
5.1	Number Generators	219
5.2	Polynomial Indistinguishability	221
5.3	Pseudorandom Bit Generators	224
5.3.1	RSA Pseudorandom Bit Generator	225
5.3.2	BBS Pseudorandom Bit Generator	227
5.4	Next Bit Test	232
5.5	Pseudorandom Function Generators	233
5.6	Pseudorandom Permutation Generators	238
5.7	Super Pseudorandom Permutation Generators	241
5.8	Problems and Exercises	242
6	Hashing	243
6.1	Properties of Hashing	243
6.2	Birthday Paradox	244
6.3	Serial and Parallel Hashing	249
6.4	Theoretic Constructions	250
6.5	Hashing Based on Cryptosystems	254
6.6	MD (Message Digest) Family	256
6.6.1	MD5	257
6.6.2	SHA-1	262
6.6.3	RIPEMD-160	264
6.6.4	HAVAL	268
6.6.5	Hashing Based on Intractable Problems	273
6.7	Keyed Hashing	275
6.7.1	Early MACs	276
6.7.2	MACs from Keyless Hashing	278
6.8	Problems and Exercises	280

7	Digital Signatures	283
7.1	Properties of Digital Signatures	283
7.2	Generic Signature Schemes	285
7.2.1	Rabin Signatures	285
7.2.2	Lamport Signatures	286
7.2.3	Matyas-Meyer Signatures	287
7.3	RSA Signatures	288
7.4	ElGamal Signatures	290
7.5	Blind Signatures	294
7.6	Undeniable Signatures	295
7.7	Fail-Stop Signatures	299
7.8	Timestamping	302
7.9	Problems and Exercises	304
8	Authentication	307
8.1	Active Opponents	307
8.2	Model of Authentication Systems	309
8.2.1	Elements of the Theory of Games	310
8.2.2	Impersonation Game	311
8.2.3	Substitution Game	314
8.2.4	Spoofing Game	316
8.3	Information Theoretic Bounds	317
8.4	Constructions of A-codes	319
8.4.1	A-codes in Projective Spaces	319
8.4.2	A-codes and Orthogonal Arrays	321
8.4.3	A-codes Based on Error Correcting Codes	322
8.5	General A-codes	323
8.6	Problems and Exercises	324
9	Secret Sharing	327
9.1	Threshold Secret Sharing	327
9.1.1	(t, t) Threshold Schemes	328
9.1.2	Shamir Scheme	329
9.1.3	Blakley Scheme	331
9.1.4	Modular Scheme	331
9.2	General Secret Sharing	332

9.2.1	Cumulative Array Construction	334
9.2.2	Benaloh-Leichter Construction	337
9.3	Perfectness	338
9.4	Information Rate	340
9.4.1	Upper Bounds	341
9.4.2	Ideal Schemes	344
9.4.3	Non-ideal Optimal Secret Sharing	347
9.5	Extended Capabilities	348
9.6	Problems and Exercises	350
10	Group-Oriented Cryptography	353
10.1	Conditionally Secure Shamir Scheme	353
10.1.1	Description of the Scheme	354
10.1.2	Renewal of the Scheme	355
10.1.3	Noninteractive Verification of Shares	356
10.1.4	Proactive Secret Sharing	358
10.2	Threshold Decryption	361
10.2.1	ElGamal Threshold Decryption	361
10.2.2	RSA Threshold Decryption	363
10.2.3	RSA Decryption Without Dealer	366
10.3	Threshold Signatures	368
10.3.1	RSA Threshold Signatures	369
10.3.2	ElGamal Threshold Signatures	371
10.3.3	Threshold DSS Signatures	373
10.4	Problems and Exercises	376
11	Key Establishment Protocols	379
11.1	Classical Key Transport Protocols	381
11.2	Diffie-Hellman Key Agreement Protocol	383
11.2.1	DH Problem	385
11.3	Modern Key Distribution Protocols	385
11.3.1	Kerberos	387
11.3.2	SPX	390
11.3.3	Other Authentication Services	392
11.4	Key Agreement Protocols	393
11.4.1	MTI Protocols	394

11.4.2	Station-to-Station Protocol	394
11.4.3	Protocols with Self-certified Public Keys	395
11.4.4	Identity-Based Protocols	397
11.5	Conference-Key Establishment Protocols	398
11.6	BAN Logic of Authentication	401
11.6.1	BAN Logical Postulates	401
11.6.2	Analysis of the Needham-Schroeder Protocol	403
11.7	Problems and Exercises	407
12	Zero-Knowledge Proof Systems	409
12.1	Interactive Proof Systems	409
12.2	Perfect Zero-Knowledge Proofs	413
12.3	Computational Zero-Knowledge Proofs	421
12.4	Bit Commitment Schemes	424
12.4.1	Blobs with Unconditional Secrecy	425
12.4.2	Blobs with Unconditional Binding	427
12.4.3	Multivalued Blobs	428
12.5	Problems and Exercises	430
13	Identification	433
13.1	Basic Identification Techniques	433
13.2	User Identification	434
13.3	Passwords	436
13.3.1	Attacks on Passwords	437
13.3.2	Weaknesses of Passwords	439
13.4	Challenge-Response Identification	440
13.4.1	Authentication of Shared Keys	440
13.4.2	Authentication of Public Keys	441
13.5	Identification Protocols	443
13.5.1	Fiat-Shamir Identification Protocol	443
13.5.2	Feige-Fiat-Shamir Identification Protocol	445
13.5.3	Guillou-Quisquater Identification Protocol	447
13.6	Identification Schemes	450
13.6.1	Schnorr Identification Scheme	450
13.6.2	Okamoto Identification Scheme	452
13.6.3	Signatures from Identification Schemes	454

13.7	Problems and Exercises	456
14	Intrusion Detection	459
14.1	Introduction	459
14.2	Anomaly Intrusion Detection	461
14.2.1	Statistical IDS	462
14.2.2	Predictive Patterns	463
14.2.3	Neural Networks	465
14.3	Misuse Intrusion Detection	466
14.4	Uncertainty in Intrusion Detection	467
14.4.1	Probabilistic Model	467
14.4.2	Dempster-Shafer Theory	471
14.5	Generic Intrusion Detection Model	473
14.6	Host Intrusion Detection Systems	476
14.6.1	IDES	476
14.6.2	Haystack	478
14.6.3	MIDAS	479
14.7	Network Intrusion Detection Systems	480
14.7.1	NSM	481
14.7.2	DIDS	483
14.7.3	NADIR	485
14.7.4	Cooperating Security Manager (CSM)	485
14.8	Limitations of Current Intrusion Detection Systems	487
14.8.1	General Limitations	487
14.8.2	Network-IDS Shortcomings	488
14.9	The Common Intrusion Detection Framework (CIDF)	490
14.10	Partial List of ID Systems	492
14.11	Problems and Exercises	497
15	Electronic Elections and Digital Money	499
15.1	Electronic Elections	499
15.1.1	A Simple Electronic Election Protocol	501
15.1.2	Chaum Protocol	503
15.1.3	Boyd Protocol	505
15.1.4	Fujioka-Okamoto-Ohta Protocol	506
15.1.5	Other Protocols	508

15.2	Digital Cash	509
15.2.1	Untraceable Digital Coins	510
15.2.2	Divisible Electronic Cash	513
15.2.3	Brands Electronic Cash Protocol	517
15.2.4	Other E-Cash Protocols	519
15.2.5	Micropayments	520
15.3	Payment Protocols	522
16	Database Protection and Security	525
16.1	Database Access Control	525
16.2	Security Filters	527
16.3	Encryption Methods	529
16.3.1	Privacy Homomorphisms	538
16.4	Database Machines and Architectures	539
16.4.1	Experimental Back-end Database Systems	541
16.5	Database Views	544
16.5.1	Advantages and Disadvantages of Views	546
16.5.2	Completeness and Consistency of Views	548
16.5.3	Design and Implementations of Views	549
16.6	Security in Distributed Databases	551
16.7	Security in Object-Oriented Database Systems	554
16.8	Security in Knowledge-Based Systems	557
16.9	Oracle8 Security	558
16.9.1	User Authentication	558
16.9.2	Access Control	560
16.9.3	Oracle Security Server	563
17	Access Control	565
17.1	Mandatory Access Control	567
17.1.1	Lattice Model	567
17.1.2	Bell-LaPadula Model	569
17.2	Discretionary Access Control	571
17.2.1	Access Matrix Model	571
17.2.2	Harrison-Ruzzo-Ullman Model	574
17.3	Role-Based Access Control Model	576
17.4	Implementations of Access Control	578

17.4.1	Security Kernel	578
17.4.2	Multics	581
17.4.3	UNIX	582
17.4.4	Capabilities	584
17.4.5	Access Control Lists	587
18	Network Security	591
18.1	Internet Protocol Security (IPsec)	591
18.1.1	Security Associations	594
18.1.2	Authentication Header Protocol	594
18.1.3	Encapsulating Security Payload Protocol	596
18.1.4	Internet Key Exchange	597
18.1.5	Virtual Private Networks	601
18.2	Secure Sockets Layer	602
18.2.1	States of SSL	602
18.2.2	SSL Record Protocol	604
18.2.3	Handshake Protocol	606
18.2.4	Change Cipher Spec and Alert Protocols	609
18.2.5	Cryptographic Computations	610
18.2.6	Transport-Layer Security	611
18.3	Computer Viruses	611
18.3.1	What Is a Computer Virus?	611
18.3.2	Worms and Trojan Horses	612
18.3.3	Taxonomy of Viruses	613
18.3.4	IBM-PC Viruses	615
18.3.5	Macintosh Operating System	619
18.3.6	Macintosh Viruses	623
18.3.7	Macro Viruses	625
18.3.8	Protection Against Viruses	627
	References	631
	Index	665