
Table of Contents

List of Tables	xv
List of Figures	xix
Foreword by R.L. Rivest	xxi
Preface	xxiii
1 Overview of Cryptography	1
1.1 Introduction	1
1.2 Information security and cryptography	2
1.3 Background on functions	6
1.3.1 Functions (1-1, one-way, trapdoor one-way)	6
1.3.2 Permutations	10
1.3.3 Involutions	10
1.4 Basic terminology and concepts	11
1.5 Symmetric-key encryption	15
1.5.1 Overview of block ciphers and stream ciphers	15
1.5.2 Substitution ciphers and transposition ciphers	17
1.5.3 Composition of ciphers	19
1.5.4 Stream ciphers	20
1.5.5 The key space	21
1.6 Digital signatures	22
1.7 Authentication and identification	24
1.7.1 Identification	24
1.7.2 Data origin authentication	25
1.8 Public-key cryptography	25
1.8.1 Public-key encryption	25
1.8.2 The necessity of authentication in public-key systems	27
1.8.3 Digital signatures from reversible public-key encryption	28
1.8.4 Symmetric-key vs. public-key cryptography	31
1.9 Hash functions	33
1.10 Protocols and mechanisms	33
1.11 Key establishment, management, and certification	35
1.11.1 Key management through symmetric-key techniques	36
1.11.2 Key management through public-key techniques	37
1.11.3 Trusted third parties and public-key certificates	39
1.12 Pseudorandom numbers and sequences	39
1.13 Classes of attacks and security models	41
1.13.1 Attacks on encryption schemes	41
1.13.2 Attacks on protocols	42
1.13.3 Models for evaluating security	42
1.13.4 Perspective for computational security	44
1.14 Notes and further references	45

2	Mathematical Background	49
2.1	Probability theory	50
2.1.1	Basic definitions	50
2.1.2	Conditional probability	51
2.1.3	Random variables	51
2.1.4	Binomial distribution	52
2.1.5	Birthday attacks	53
2.1.6	Random mappings	54
2.2	Information theory	56
2.2.1	Entropy	56
2.2.2	Mutual information	57
2.3	Complexity theory	57
2.3.1	Basic definitions	57
2.3.2	Asymptotic notation	58
2.3.3	Complexity classes	59
2.3.4	Randomized algorithms	62
2.4	Number theory	63
2.4.1	The integers	63
2.4.2	Algorithms in \mathbb{Z}	66
2.4.3	The integers modulo n	67
2.4.4	Algorithms in \mathbb{Z}_n	71
2.4.5	The Legendre and Jacobi symbols	72
2.4.6	Blum integers	74
2.5	Abstract algebra	75
2.5.1	Groups	75
2.5.2	Rings	76
2.5.3	Fields	77
2.5.4	Polynomial rings	78
2.5.5	Vector spaces	79
2.6	Finite fields	80
2.6.1	Basic properties	80
2.6.2	The Euclidean algorithm for polynomials	81
2.6.3	Arithmetic of polynomials	83
2.7	Notes and further references	85
3	Number-Theoretic Reference Problems	87
3.1	Introduction and overview	87
3.2	The integer factorization problem	89
3.2.1	Trial division	90
3.2.2	Pollard's rho factoring algorithm	91
3.2.3	Pollard's $p - 1$ factoring algorithm	92
3.2.4	Elliptic curve factoring	94
3.2.5	Random square factoring methods	94
3.2.6	Quadratic sieve factoring	95
3.2.7	Number field sieve factoring	98
3.3	The RSA problem	98
3.4	The quadratic residuosity problem	99
3.5	Computing square roots in \mathbb{Z}_n	99
3.5.1	Case (i): n prime	100
3.5.2	Case (ii): n composite	101

3.6	The discrete logarithm problem	103
3.6.1	Exhaustive search	104
3.6.2	Baby-step giant-step algorithm	104
3.6.3	Pollard's rho algorithm for logarithms	106
3.6.4	Pohlig-Hellman algorithm	107
3.6.5	Index-calculus algorithm	109
3.6.6	Discrete logarithm problem in subgroups of \mathbb{Z}_p^*	113
3.7	The Diffie-Hellman problem	113
3.8	Composite moduli	114
3.9	Computing individual bits	114
3.9.1	The discrete logarithm problem in \mathbb{Z}_p^* — individual bits	116
3.9.2	The RSA problem — individual bits	116
3.9.3	The Rabin problem — individual bits	117
3.10	The subset sum problem	117
3.10.1	The L^3 -lattice basis reduction algorithm	118
3.10.2	Solving subset sum problems of low density	120
3.10.3	Simultaneous diophantine approximation	121
3.11	Factoring polynomials over finite fields	122
3.11.1	Square-free factorization	123
3.11.2	Berlekamp's Q -matrix algorithm	124
3.12	Notes and further references	125
4	Public-Key Parameters	133
4.1	Introduction	133
4.1.1	Generating large prime numbers naively	134
4.1.2	Distribution of prime numbers	134
4.2	Probabilistic primality tests	135
4.2.1	Fermat's test	136
4.2.2	Solovay-Strassen test	137
4.2.3	Miller-Rabin test	138
4.2.4	Comparison: Fermat, Solovay-Strassen, and Miller-Rabin	140
4.3	(True) Primality tests	142
4.3.1	Testing Mersenne numbers	142
4.3.2	Primality testing using the factorization of $n - 1$	143
4.3.3	Jacobi sum test	144
4.3.4	Tests using elliptic curves	145
4.4	Prime number generation	145
4.4.1	Random search for probable primes	145
4.4.2	Strong primes	149
4.4.3	NIST method for generating DSA primes	150
4.4.4	Constructive techniques for provable primes	152
4.5	Irreducible polynomials over \mathbb{Z}_p	154
4.5.1	Irreducible polynomials	154
4.5.2	Irreducible trinomials	157
4.5.3	Primitive polynomials	157
4.6	Generators and elements of high order	160
4.6.1	Selecting a prime p and generator of \mathbb{Z}_p^*	164
4.7	Notes and further references	165

5	Pseudorandom Bits and Sequences	169
5.1	Introduction	169
5.1.1	Background and Classification	170
5.2	Random bit generation	171
5.3	Pseudorandom bit generation	173
5.3.1	ANSI X9.17 generator	173
5.3.2	FIPS 186 generator	174
5.4	Statistical tests	175
5.4.1	The normal and chi-square distributions	176
5.4.2	Hypothesis testing	179
5.4.3	Golomb's randomness postulates	180
5.4.4	Five basic tests	181
5.4.5	Maurer's universal statistical test	183
5.5	Cryptographically secure pseudorandom bit generation	185
5.5.1	RSA pseudorandom bit generator	185
5.5.2	Blum-Blum-Shub pseudorandom bit generator	186
5.6	Notes and further references	187
6	Stream Ciphers	191
6.1	Introduction	191
6.1.1	Classification	192
6.2	Feedback shift registers	195
6.2.1	Linear feedback shift registers	195
6.2.2	Linear complexity	198
6.2.3	Berlekamp-Massey algorithm	200
6.2.4	Nonlinear feedback shift registers	202
6.3	Stream ciphers based on LFSRs	203
6.3.1	Nonlinear combination generators	205
6.3.2	Nonlinear filter generators	208
6.3.3	Clock-controlled generators	209
6.4	Other stream ciphers	212
6.4.1	SEAL	213
6.5	Notes and further references	216
7	Block Ciphers	223
7.1	Introduction and overview	223
7.2	Background and general concepts	224
7.2.1	Introduction to block ciphers	224
7.2.2	Modes of operation	228
7.2.3	Exhaustive key search and multiple encryption	233
7.3	Classical ciphers and historical development	237
7.3.1	Transposition ciphers (background)	238
7.3.2	Substitution ciphers (background)	238
7.3.3	Polyalphabetic substitutions and Vigenère ciphers (historical)	241
7.3.4	Polyalphabetic cipher machines and rotors (historical)	242
7.3.5	Cryptanalysis of classical ciphers (historical)	245
7.4	DES	250
7.4.1	Product ciphers and Feistel ciphers	250
7.4.2	DES algorithm	252
7.4.3	DES properties and strength	256

7.5	FEAL	259
7.6	IDEA	263
7.7	SAFER, RC5, and other block ciphers	266
7.7.1	SAFER	266
7.7.2	RC5	269
7.7.3	Other block ciphers	270
7.8	Notes and further references	271
8	Public-Key Encryption	283
8.1	Introduction	283
8.1.1	Basic principles	284
8.2	RSA public-key encryption	285
8.2.1	Description	286
8.2.2	Security of RSA	287
8.2.3	RSA encryption in practice	290
8.3	Rabin public-key encryption	292
8.4	ElGamal public-key encryption	294
8.4.1	Basic ElGamal encryption	294
8.4.2	Generalized ElGamal encryption	297
8.5	McEliece public-key encryption	298
8.6	Knapsack public-key encryption	300
8.6.1	Merkle-Hellman knapsack encryption	300
8.6.2	Chor-Rivest knapsack encryption	302
8.7	Probabilistic public-key encryption	306
8.7.1	Goldwasser-Micali probabilistic encryption	307
8.7.2	Blum-Goldwasser probabilistic encryption	308
8.7.3	Plaintext-aware encryption	311
8.8	Notes and further references	312
9	Hash Functions and Data Integrity	321
9.1	Introduction	321
9.2	Classification and framework	322
9.2.1	General classification	322
9.2.2	Basic properties and definitions	323
9.2.3	Hash properties required for specific applications	327
9.2.4	One-way functions and compression functions	327
9.2.5	Relationships between properties	329
9.2.6	Other hash function properties and applications	330
9.3	Basic constructions and general results	332
9.3.1	General model for iterated hash functions	332
9.3.2	General constructions and extensions	333
9.3.3	Formatting and initialization details	334
9.3.4	Security objectives and basic attacks	335
9.3.5	Bitsizes required for practical security	337
9.4	Unkeyed hash functions (MDCs)	338
9.4.1	Hash functions based on block ciphers	338
9.4.2	Customized hash functions based on MD4	343
9.4.3	Hash functions based on modular arithmetic	351
9.5	Keyed hash functions (MACs)	352
9.5.1	MACs based on block ciphers	353

9.5.2	Constructing MACs from MDCs	354
9.5.3	Customized MACs	356
9.5.4	MACs for stream ciphers	358
9.6	Data integrity and message authentication	359
9.6.1	Background and definitions	359
9.6.2	Non-malicious vs. malicious threats to data integrity	362
9.6.3	Data integrity using a MAC alone	364
9.6.4	Data integrity using an MDC and an authentic channel	364
9.6.5	Data integrity combined with encryption	364
9.7	Advanced attacks on hash functions	368
9.7.1	Birthday attacks	369
9.7.2	Pseudo-collisions and compression function attacks	371
9.7.3	Chaining attacks	373
9.7.4	Attacks based on properties of underlying cipher	375
9.8	Notes and further references	376
10	Identification and Entity Authentication	385
10.1	Introduction	385
10.1.1	Identification objectives and applications	386
10.1.2	Properties of identification protocols	387
10.2	Passwords (weak authentication)	388
10.2.1	Fixed password schemes: techniques	389
10.2.2	Fixed password schemes: attacks	391
10.2.3	Case study – UNIX passwords	393
10.2.4	PINs and passkeys	394
10.2.5	One-time passwords (towards strong authentication)	395
10.3	Challenge-response identification (strong authentication)	397
10.3.1	Background on time-variant parameters	397
10.3.2	Challenge-response by symmetric-key techniques	400
10.3.3	Challenge-response by public-key techniques	403
10.4	Customized and zero-knowledge identification protocols	405
10.4.1	Overview of zero-knowledge concepts	405
10.4.2	Feige-Fiat-Shamir identification protocol	410
10.4.3	GQ identification protocol	412
10.4.4	Schnorr identification protocol	414
10.4.5	Comparison: Fiat-Shamir, GQ, and Schnorr	416
10.5	Attacks on identification protocols	417
10.6	Notes and further references	420
11	Digital Signatures	425
11.1	Introduction	425
11.2	A framework for digital signature mechanisms	426
11.2.1	Basic definitions	426
11.2.2	Digital signature schemes with appendix	428
11.2.3	Digital signature schemes with message recovery	430
11.2.4	Types of attacks on signature schemes	432
11.3	RSA and related signature schemes	433
11.3.1	The RSA signature scheme	433
11.3.2	Possible attacks on RSA signatures	434
11.3.3	RSA signatures in practice	435

11.3.4	The Rabin public-key signature scheme	438
11.3.5	ISO/IEC 9796 formatting	442
11.3.6	PKCS #1 formatting	445
11.4	Fiat-Shamir signature schemes	447
11.4.1	Feige-Fiat-Shamir signature scheme	447
11.4.2	GQ signature scheme	450
11.5	The DSA and related signature schemes	451
11.5.1	The Digital Signature Algorithm (DSA)	452
11.5.2	The ElGamal signature scheme	454
11.5.3	The Schnorr signature scheme	459
11.5.4	The ElGamal signature scheme with message recovery	460
11.6	One-time digital signatures	462
11.6.1	The Rabin one-time signature scheme	462
11.6.2	The Merkle one-time signature scheme	464
11.6.3	Authentication trees and one-time signatures	466
11.6.4	The GMR one-time signature scheme	468
11.7	Other signature schemes	471
11.7.1	Arbitrated digital signatures	472
11.7.2	ESIGN	473
11.8	Signatures with additional functionality	474
11.8.1	Blind signature schemes	475
11.8.2	Undeniable signature schemes	476
11.8.3	Fail-stop signature schemes	478
11.9	Notes and further references	481
12	Key Establishment Protocols	489
12.1	Introduction	489
12.2	Classification and framework	490
12.2.1	General classification and fundamental concepts	490
12.2.2	Objectives and properties	493
12.2.3	Assumptions and adversaries in key establishment protocols	495
12.3	Key transport based on symmetric encryption	497
12.3.1	Symmetric key transport and derivation without a server	497
12.3.2	Kerberos and related server-based protocols	500
12.4	Key agreement based on symmetric techniques	505
12.5	Key transport based on public-key encryption	506
12.5.1	Key transport using PK encryption without signatures	507
12.5.2	Protocols combining PK encryption and signatures	509
12.5.3	Hybrid key transport protocols using PK encryption	512
12.6	Key agreement based on asymmetric techniques	515
12.6.1	Diffie-Hellman and related key agreement protocols	515
12.6.2	Implicitly-certified public keys	520
12.6.3	Diffie-Hellman protocols using implicitly-certified keys	522
12.7	Secret sharing	524
12.7.1	Simple shared control schemes	524
12.7.2	Threshold schemes	525
12.7.3	Generalized secret sharing	526
12.8	Conference keying	528
12.9	Analysis of key establishment protocols	530
12.9.1	Attack strategies and classic protocol flaws	530

12.9.2	Analysis objectives and methods	532
12.10	Notes and further references	534
13	Key Management Techniques	543
13.1	Introduction	543
13.2	Background and basic concepts	544
13.2.1	Classifying keys by algorithm type and intended use	544
13.2.2	Key management objectives, threats, and policy	545
13.2.3	Simple key establishment models	546
13.2.4	Roles of third parties	547
13.2.5	Tradeoffs among key establishment protocols	550
13.3	Techniques for distributing confidential keys	551
13.3.1	Key layering and cryptoperiods	551
13.3.2	Key translation centers and symmetric-key certificates	553
13.4	Techniques for distributing public keys	555
13.4.1	Authentication trees	556
13.4.2	Public-key certificates	559
13.4.3	Identity-based systems	561
13.4.4	Implicitly-certified public keys	562
13.4.5	Comparison of techniques for distributing public keys	563
13.5	Techniques for controlling key usage	567
13.5.1	Key separation and constraints on key usage	567
13.5.2	Techniques for controlling use of symmetric keys	568
13.6	Key management involving multiple domains	570
13.6.1	Trust between two domains	570
13.6.2	Trust models involving multiple certification authorities	572
13.6.3	Certificate distribution and revocation	576
13.7	Key life cycle issues	577
13.7.1	Lifetime protection requirements	578
13.7.2	Key management life cycle	578
13.8	Advanced trusted third party services	581
13.8.1	Trusted timestamping service	581
13.8.2	Non-repudiation and notarization of digital signatures	582
13.8.3	Key escrow	584
13.9	Notes and further references	586
14	Efficient Implementation	591
14.1	Introduction	591
14.2	Multiple-precision integer arithmetic	592
14.2.1	Radix representation	592
14.2.2	Addition and subtraction	594
14.2.3	Multiplication	595
14.2.4	Squaring	596
14.2.5	Division	598
14.3	Multiple-precision modular arithmetic	599
14.3.1	Classical modular multiplication	600
14.3.2	Montgomery reduction	600
14.3.3	Barrett reduction	603
14.3.4	Reduction methods for moduli of special form	605
14.4	Greatest common divisor algorithms	606

14.4.1	Binary gcd algorithm	606
14.4.2	Lehmer's gcd algorithm	607
14.4.3	Binary extended gcd algorithm	608
14.5	Chinese remainder theorem for integers	610
14.5.1	Residue number systems	611
14.5.2	Garner's algorithm	612
14.6	Exponentiation	613
14.6.1	Techniques for general exponentiation	614
14.6.2	Fixed-exponent exponentiation algorithms	620
14.6.3	Fixed-base exponentiation algorithms	623
14.7	Exponent recoding	627
14.7.1	Signed-digit representation	627
14.7.2	String-replacement representation	628
14.8	Notes and further references	630
15	Patents and Standards	635
15.1	Introduction	635
15.2	Patents on cryptographic techniques	635
15.2.1	Five fundamental patents	636
15.2.2	Ten prominent patents	638
15.2.3	Ten selected patents	641
15.2.4	Ordering and acquiring patents	645
15.3	Cryptographic standards	645
15.3.1	International standards – cryptographic techniques	645
15.3.2	Banking security standards (ANSI, ISO)	648
15.3.3	International security architectures and frameworks	653
15.3.4	U.S. government standards (FIPS)	654
15.3.5	Internet standards and RFCs	655
15.3.6	De facto standards	656
15.3.7	Ordering and acquiring standards	656
15.4	Notes and further references	657
A	Bibliography of Papers from Selected Cryptographic Forums	663
A.1	Asiacrypt/Auscrypt Proceedings	663
A.2	Crypto Proceedings	667
A.3	Eurocrypt Proceedings	684
A.4	Fast Software Encryption Proceedings	698
A.5	Journal of Cryptology papers	700
	References	703
	Index	755