

HANDBOOK of
APPLIED
CRYPTOGRAPHY

The CRC Press Series on

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor

Kenneth H. Rosen, Ph. D.

AT&T Bell Laboratories

*Charles J. Colbourn and Jeffery H. Dinitz, The CRC
Handbook of Combinatorial Designs*

*Steven Furino, Ying Miao, and Jianxing Yin,
Frames and Resolvable Designs:
Uses, Constructions, and Existence*

*Daryl D. Harms, Miroslav Kraetzl, Charles J. Colbourn,
and Stanley J. Devitt, Network Reliability:
Experiments with A Symbolic Algebra Environment*

Richard A. Mollin, Quadratics

Douglas R. Stinson, Cryptography: Theory and Practice

HANDBOOK of APPLIED CRYPTOGRAPHY

Alfred J. Menezes
Pall C. van Oorschot
Scott A. Vanstone



CRC Press
Boca Raton New York London Tokyo

Library of Congress Cataloging-in-Publication Data

Menezes, A. J. (Alfred J.), 1965-

Handbook of applied cryptography / Alfred Menezes, Paul van Oorschot,
Scott Vanstone.

p. cm. -- (CRC Press series on discrete mathematics and its
applications)

Includes bibliographical references and index.

ISBN O-8493-8523-7 (alk. paper)

1. Computers--Access control--Handbooks, manuals, etc.

2. Cryptography--Handbooks, manuals, etc. I. Van Oorschot, Paul C.

II. Vanstone, Scott A. III. Title. IV. Series: Discrete
mathematics and its applications.

QA76.9.A25M463 1996

005.8&2--dc20

96-27609

CIP

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

The consent of CRC Press LLC does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press LLC for such copying.

Direct all inquiries to CRC Press LLC, 2000 Corporate Blvd., N.W., Boca Raton, Florida 33431.

© 1997 by CRC Press LLC

No claim to original U.S. Government works

International Standard Book Number O-8493-8523-7

Library of Congress Card Number 96-27609

Printed in the United States of America 2 3 4 5 6 7 8 9 0

Printed on acid-free paper

Contents in Brief

	Table of Contents
	List of Tables..xv
	List of Figuresxix
	Forewordxxi
	Prefacexxiii
1	Overview of Cryptography	1
2	Mathematical Background49
3	Number-Theoretic Reference Problems87
4	Public-Key Parameters	133
5	Pseudorandom Bits and Sequences	169
6	Stream Ciphers	191
7	Block Ciphers223
8	Public-Key Encryption283
9	Hash Functions and Data Integrity321
10	Identification and Entity Authentication385
11	Digital Signatures425
12	Key Establishment Protocols489
13	Key Management Techniques543
14	Efficient Implementation591
15	Patents and Standards635
A	Bibliography of Papers from Selected Cryptographic Forums663
	References703
	Index..755

To Archie and Lida Menezes

To Cornelis Henricus van Oorschot
and Maria Anna Buys van Vugt

To Margret and Gordon Vanstone

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 Vigenere 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

List of Tables

1.1	Some information security objectives	3
1.2	Reference numbers comparing relative magnitudes	44
1.3	Prefixes used for various powers of 10	45
2.1	Bit complexity of basic operations in \mathbb{Z}	66
2.2	Extended Euclidean algorithm (example)	67
2.3	Orders of elements in \mathbb{Z}_{21}^*	69
2.4	Computation of $5^{596} \bmod 1234$	72
2.5	Bit complexity of basic operations in \mathbb{Z}_n	72
2.6	Jacobi symbols of elements in \mathbb{Z}_{21}^*	74
2.7	The subgroups of \mathbb{Z}_{19}^*	76
2.8	Complexity of basic operations in \mathbb{F}_{p^m}	84
2.9	The powers of x modulo $f(z) = x^4 + x + 1$	86
3.1	Some computational problems of cryptographic relevance	88
3.2	Pollard's rho algorithm (example)	107
3.3	Running time estimates for numbers factored with QS	127
4.1	Smallest strong pseudoprimes	140
4.2	Known Mersenne primes	143
4.3	Upper bounds on $p_{k,t}$ for sample values of k and t	147
4.4	Number of Miller-Rabin iterations required so that $p_{k,t} \leq (\frac{1}{2})^{80}$	148
4.5	Upper bounds on the error probability of incremental search	149
4.6	Irreducible trinomials of degree m over \mathbb{Z}_2 , $1 \leq m \leq 722$	158
4.7	Irreducible trinomials of degree m over \mathbb{Z}_2 , $723 \leq m \leq 1478$	159
4.8	Primitive polynomials over \mathbb{Z}_2	161
4.9	Primitive polynomials of degree m over \mathbb{Z}_2 , $2^m - 1$ a Mersenne prime	162
5.1	Selected percentiles of the standard normal distribution	177
5.2	Selected percentiles of the χ^2 (chi-square) distribution	178
5.3	Mean and variance of X_u for Maurer's universal statistical test	184
6.1	Berlekamp-Massey algorithm (example)	202
7.1	Estimated roughness constant κ_p for various languages	250
7.2	DES initial permutation and inverse (IP and IP^{-1})	253
7.3	DES per-round functions: expansion E and permutation P	253
7.4	DES key schedule bit selections (PC1 and PC2)	256
7.5	DES weak keys.	258
7.6	DES pairs of semi-weak keys	258
7.7	DES strength against various attacks	259
7.8	DES S-boxes	260
7.9	FEAL functions f, f_K	261
7.10	FEAL strength against various attacks	262
7.11	IDEA decryption subkeys derived from encryption subkeys	265
7.12	IDEA encryption sample: round subkeys and ciphertext	265

7.13	IDEA decryption sample: round subkeys and variables	266
7.14	RC5 magic constants	270
8.1	Public-key encryption schemes and related computational problems . . .	284
9.1	Resistance properties required for specified data integrity applications . .	327
9.2	Design objectives for n-bit hash functions (t-bit MAC key)	335
9.3	Upper bounds on strength of selected hash functions	339
9.4	Summary of selected hash functions based on n-bit block ciphers	340
9.5	Summary of selected hash functions based on MD4	345
9.6	Test vectors for selected hash functions	345
9.7	Notation for MD4-family algorithms	345
9.8	RIPEMD-160 round function definitions	349
9.9	RIPEMD- 160 word-access orders and rotate counts	35 1
9.10	Properties of various types of authentication	362
9.11	Definition of preimage and collision attacks	372
10.1	Bitsize of password space for various character combinations	392
10.2	Time required to search entire password space	392
10.3	Identification protocol attacks and counter-measures	418
11.1	Notation for digital signature mechanisms	427
11.2	Definition of sets and functions for modified-Rabin signatures	440
11.3	ISO/IEC 9796 notation	442
11.4	PKCS #1 notation	445
11.5	Variations of the ElGamal signing equation	457
11.6	The elements of \mathbb{F}_{2^5} as powers of a generator	459
11.7	Notation for the Rabin one-time signature scheme	463
11.8	Parameters and signatures for Merkle's one-time signature scheme . . .	467
11.9	Parameters and signatures for Merkle's one-time signature scheme . . .	467
12.1	Authentication summary - various terms and related concepts	492
12.2	Key transport protocols based on symmetric encryption	497
12.3	Selected key transport protocols based on public-key encryption	507
12.4	Selected key agreement protocols	5 16
12.5	Selected MTI key agreement protocols	5 18
13.1	Private, public, symmetric, and secret keys	544
13.2	Types of algorithms commonly used to meet specified objectives	545
13.3	Key protection requirements: symmetric-key vs. public-key systems . . .	551
14.1	Signed-magnitude and two's complement representations of integers . .	594
14.2	Multiple-precision subtraction (example)	595
14.3	Multiple-precision multiplication (example)	596
14.4	Multiple-precision squaring (example)	597
14.5	Multiple-precision division (example)	598
14.6	Multiple-precision division after normalization (example)	599
14.7	Montgomery reduction algorithm (example)	602
14.8	Montgomery multiplication (example)	603
14.9	Reduction modulo $m = b^t - c$ (example)	605
14.10	Lehmer's gcd algorithm (example)	609
14.11	Single-precision computations in Lehmer's gcd algorithm (example) . .	609

14.12	Binary extended gcd algorithm (example)	610
14.13	Inverse computation using the binary extended gcd algorithm (example) .	611
14.14	Modular representations (example)	612
14.15	Sliding-window exponentiation (example)	617
14.16	Number of squarings and multiplications for exponentiation algorithms .	617
14.17	Single-precision multiplications required by Montgomery exponentiation	620
14.18	Binary vector-addition chain exponentiation (example)	623
14.19	Fixed-base Euclidean method for exponentiation (example)	625
14.20	Signed-digit exponent recoding (example)	628
15.1	Five fundamental U.S. cryptographic patents	636
15.2	Ten prominent U.S. cryptographic patents	638
15.3	Ten selected U.S. cryptographic patents	641
15.4	ISO and ISO/IEC standards for generic cryptographic techniques	646
15.5	Characteristics of retail vs. wholesale banking transactions	648
15.6	ANSI encryption and banking security standards	649
15.7	ISO banking security standards	652
15.8	ISO and ISO/IEC security architectures and frameworks	653
15.9	Selected security-related U.S. FIPS Publications	654
15.10	Selected Internet RFCs	655
15.11	PKCS specifications	656

List of Figures

1.1	A taxonomy of cryptographic primitives	5
1.2	A function	7
1.3	A bijection and its inverse	8
1.4	An involution.	11
1.5	A simple encryption scheme	12
1.6	Two-party communication using encryption	13
1.7	Two-party encryption with a secure channel for key exchange . .	16
1.8	Composition of two functions	19
1.9	Composition of two involutions	19
1.10	A signing and verification function for a digital signature scheme	22
1.11	Encryption using public-key techniques	26
1.12	Schematic use of public-key encryption	27
1.13	An impersonation attack on a two-party communication	28
1.14	A digital signature scheme with message recovery	29
1.15	Keying relationships in a simple 6-party network	36
1.16	Key management using a trusted third party (TTP)	36
1.17	Key management using public-key techniques	37
1.18	Impersonation by an active adversary	38
1.19	Authentication of public keys by a TTP	38
2.1	A functional graph	55
2.2	Conjectured relationship between some complexity classes . .	62
4.1	Relationships between Fermat, Euler, and strong liars	141
5.1	The normal distribution $N(0, 1)$	176
5.2	The χ^2 (chi-square) distribution with $\nu = 7$ degrees of freedom	177
6.1	General model of a synchronous stream cipher	193
6.2	General model of a binary additive stream cipher	194
6.3	General model of a self-synchronizing stream cipher	194
6.4	A linear feedback shift register (LFSR)	196
6.5	The LFSR $(4, I + D + D^4)$	197
6.6	Linear complexity profile of a 20-periodic sequence	200
6.7	A feedback shift register (FSR)	202
6.8	A nonlinear combination generator	205
6.9	The Geffe generator	206
6.10	The summation generator	207
6.11	A nonlinear filter generator	208
6.12	The alternating step generator	210
6.13	The shrinking generator	211
7.1	Common modes of operation for an n-bit block cipher	229
7.2	Multiple encryption	234
7.3	The Jefferson cylinder	243

7.4	A rotor-based machine	244
7.5	Frequency of single characters in English text	247
7.6	Frequency of 15 common digrams in English text	248
7.7	Substitution-permutation (SP) network	251
7.8	DES input-output	252
7.9	DES computation path	254
7.10	DES inner function f	255
7.11	IDEA computation path	263
7.12	SAFER K-64 computation path	267
8.1	Bellare-Rogaway plaintext-aware encryption scheme	312
9.1	Simplified classification of cryptographic hash functions	324
9.2	General model for an iterated hash function	332
9.3	Three single-length, rate-one MDCs based on block ciphers	340
9.4	Compression function of MDC-2 hash function	342
9.5	Compression function of MDC-4 hash function	344
9.6	CBC-based MAC algorithm	353
9.7	The Message Authenticator Algorithm (MAA)	357
9.8	Three methods for providing data integrity using hash functions	360
10.1	Use of one-way function for password-checking	390
10.2	UNIX crypt password mapping	394
10.3	Functional diagram of a hand-held passcode generator	403
11.1	A taxonomy of digital signature schemes	428
11.2	Overview of a digital signature scheme with appendix	429
11.3	Overview of a digital signature scheme with message recovery	431
11.4	Signature scheme with appendix from one providing message recovery	432
11.5	Signature and verification processes for ISO/IEC 9796	443
11.6	Signature and verification processes for PKCS #1	446
11.7	An authentication tree for the Merkle one-time signature scheme	467
11.8	A full binary authentication tree of level 2 for the GMR scheme	471
12.1	Simplified classification of key establishment techniques	491
12.2	Summary of Beller-Yacobi protocol (2-pass)	515
13.1	Simple key distribution models (symmetric-key)	546
13.2	In-line, on-line, and off-line third parties	548
13.3	Third party services related to public-key certification	549
13.4	Key management: symmetric-key vs. public-key encryption	552
13.5	A binary tree	557
13.6	An authentication tree	558
13.7	Key management in different classes of asymmetric signature systems	564
13.8	Establishing trust between users in distinct domains	571
13.9	Trust models for certification	574
13.10	Key management life cycle	579
13.11	Creation and use of LEAF for key escrow data recovery	585

Foreword

by R.L. Rivest

As we draw near to closing out the twentieth century, we see quite clearly that the information-processing and telecommunications revolutions now underway will continue vigorously into the twenty-first. We interact and transact by directing flocks of digital packets towards each other through cyberspace, carrying love notes, digital cash, and secret corporate documents. Our personal and economic lives rely more and more on our ability to let such ethereal carrier pigeons mediate at a distance what we used to do with face-to-face meetings, paper documents, and a firm handshake. Unfortunately, the technical wizardry enabling remote collaborations is founded on broadcasting everything as sequences of zeros and ones that one's own dog wouldn't recognize. What is to distinguish a digital dollar when it is as easily reproducible as the spoken word? How do we converse privately when every syllable is bounced off a satellite and smeared over an entire continent? How should a bank know that it really is Bill Gates requesting from his laptop in Fiji a transfer of \$10,000,000,000 to another bank? Fortunately, the magical mathematics of cryptography can help. Cryptography provides techniques for keeping information secret, for determining that information has not been tampered with, and for determining who authored pieces of information.

Cryptography is fascinating because of the close ties it forges between theory and practice, and because today's practical applications of cryptography are pervasive and critical components of our information-based society. Information-protection protocols designed on theoretical foundations one year appear in products and standards documents the next. Conversely, new theoretical developments sometimes mean that last year's proposal has a previously unsuspected weakness. While the theory is advancing vigorously, there are as yet few true guarantees; the security of many proposals depends on unproven (if plausible) assumptions. The theoretical work refines and improves the practice, while the practice challenges and inspires the theoretical work. When a system is "broken," our knowledge improves, and next year's system is improved to repair the defect. (One is reminded of the long and intriguing battle between the designers of bank vaults and their opponents.)

Cryptography is also fascinating because of its game-like adversarial nature. A good cryptographer rapidly changes sides back and forth in his or her thinking, from attacker to defender and back. Just as in a game of chess, sequences of moves and counter-moves must be considered until the current situation is understood. Unlike chess players, cryptographers must also consider all the ways an adversary might try to gain by breaking the rules or violating expectations. (Does it matter if she measures how long I am computing? Does it matter if her "random" number isn't one?)

The current volume is a major contribution to the field of cryptography. It is a rigorous encyclopedia of known techniques, with an emphasis on those that are both (believed to be) secure and practically useful. It presents in a coherent manner most of the important cryptographic tools one needs to implement secure cryptographic systems, and explains many of the cryptographic principles and protocols of existing systems. The topics covered range from low-level considerations such as random-number generation and efficient modular exponentiation algorithms and medium-level items such as public-key signature techniques, to higher-level topics such as zero-knowledge protocols. This book's excellent organization and style allow it to serve well as both a self-contained tutorial and an indispensable desk reference.

In documenting the state of a fast-moving field, the authors have done incredibly well at providing error-free comprehensive content that is up-to-date. Indeed, many of the chapters, such as those on hash functions or key-establishment protocols, break new ground in both their content and their unified presentations. In the trade-off between comprehensive coverage and exhaustive treatment of individual items, the authors have chosen to write simply and directly, and thus efficiently, allowing each element to be explained together with their important details, caveats, and comparisons.

While motivated by practical applications, the authors have clearly written a book that will be of as much interest to researchers and students as it is to practitioners, by including ample discussion of the underlying mathematics and associated theoretical considerations. The essential mathematical techniques and requisite notions are presented crisply and clearly, with illustrative examples. The insightful historical notes and extensive bibliography make this book a superb stepping-stone to the literature. (I was very pleasantly surprised to find an appendix with complete programs for the CRYPTO and EUROCRYPT conferences!)

It is a pleasure to have been asked to provide the foreword for this book. I am happy to congratulate the authors on their accomplishment, and to inform the reader that he/she is looking at a landmark in the development of the field.

Ronald L. Rivest
Webster Professor of Electrical Engineering and Computer Science
Massachusetts Institute of Technology

Preface

This book is intended as a reference for professional cryptographers, presenting the techniques and algorithms of greatest interest to the current practitioner, along with the supporting motivation and background material. It also provides a comprehensive source from which to learn cryptography, serving both students and instructors. In addition, the rigorous treatment, breadth, and extensive bibliographic material should make it an important reference for research professionals.

Our goal was to assimilate the existing cryptographic knowledge of industrial interest into one consistent, self-contained volume accessible to engineers in practice, to computer scientists and mathematicians in academia, and to motivated non-specialists with a strong desire to learn cryptography. Such a task is beyond the scope of each of the following: research papers, which by nature focus on narrow topics using very specialized (and often non-standard) terminology; survey papers, which typically address, at most, a small number of major topics at a high level; and (regretably also) most books, due to the fact that many book authors lack either practical experience or familiarity with the research literature or both. Our intent was to provide a detailed presentation of those areas of cryptography which we have found to be of greatest practical utility in our own industrial experience, while maintaining a sufficiently formal approach to be suitable both as a trustworthy reference for those whose primary interest is further research, and to provide a solid foundation for students and others first learning the subject.

Throughout each chapter, we emphasize the relationship between various aspects of cryptography. Background sections commence most chapters, providing a framework and perspective for the techniques which, follow. Computer source code (e.g. C code) for algorithms has been intentionally omitted, in favor of algorithms specified in sufficient detail to allow direct implementation without consulting secondary references. We believe this style of presentation allows a better understanding of how algorithms actually work, while at the same time avoiding low-level implementation-specific constructs (which some readers will invariably be unfamiliar with) of various currently-popular programming languages.

The presentation also strongly delineates what has been established as fact (by mathematical arguments) from what is simply current conjecture. To avoid obscuring the very applied nature of the subject, rigorous proofs of correctness are in most cases omitted; however, references given in the Notes section at the end of each chapter indicate the original or recommended sources for these results. The trailing Notes sections also provide information (quite detailed in places) on various additional techniques not addressed in the main text, and provide a survey of research activities and theoretical results; references again indicate where readers may pursue particular aspects in greater depth. Needless to say, many results, and indeed some entire research areas, have been given far less attention than they warrant, or have been omitted entirely due to lack of space; we apologize in advance for such major omissions, and hope that the most significant of these are brought to our attention.

To provide an integrated treatment of cryptography spanning foundational motivation through concrete implementation, it is useful to consider a hierarchy of thought ranging from conceptual ideas and end-user services, down to the tools necessary to complete actual implementations. Table 1 depicts the hierarchical structure around which this book is organized. Corresponding to this, Figure 1 illustrates how these hierarchical levels map

Information Security Objectives	
Confidentiality	
Data integrity	
Authentication (entity and data origin)	
Non-repudiation	
Cryptographic functions	
Encryption	Chapters 6,7,8
Message authentication and data integrity techniques	Chapter 9
Identification/entity authentication techniques	Chapter 10
Digital signatures -	Chapter 11
Cryptographic building blocks	
Stream ciphers	Chapter 6
Block ciphers (symmetric-key)	Chapter 7
Public-key encryption	Chapter 8
One-way hash functions (unkeyed)	Chapter 9
Message authentication codes	Chapter 9
Signature schemes (public-key, symmetric-key)	Chapter 11
Utilities	
Public-key parameter generation	Chapter 4
Pseudorandom bit generation	Chapter 5
Efficient algorithms for discrete arithmetic	Chapter 14
Foundations	
Introduction to cryptography	Chapter 1
Mathematical background	Chapter 2
Complexity and analysis of underlying problems	Chapter 3
Infrastructure techniques and commercial aspects	
Key establishment protocols	Chapter 12
Key installation and key management	Chapter 13
Cryptographic patents	Chapter 15
Cryptographic standards	Chapter 15

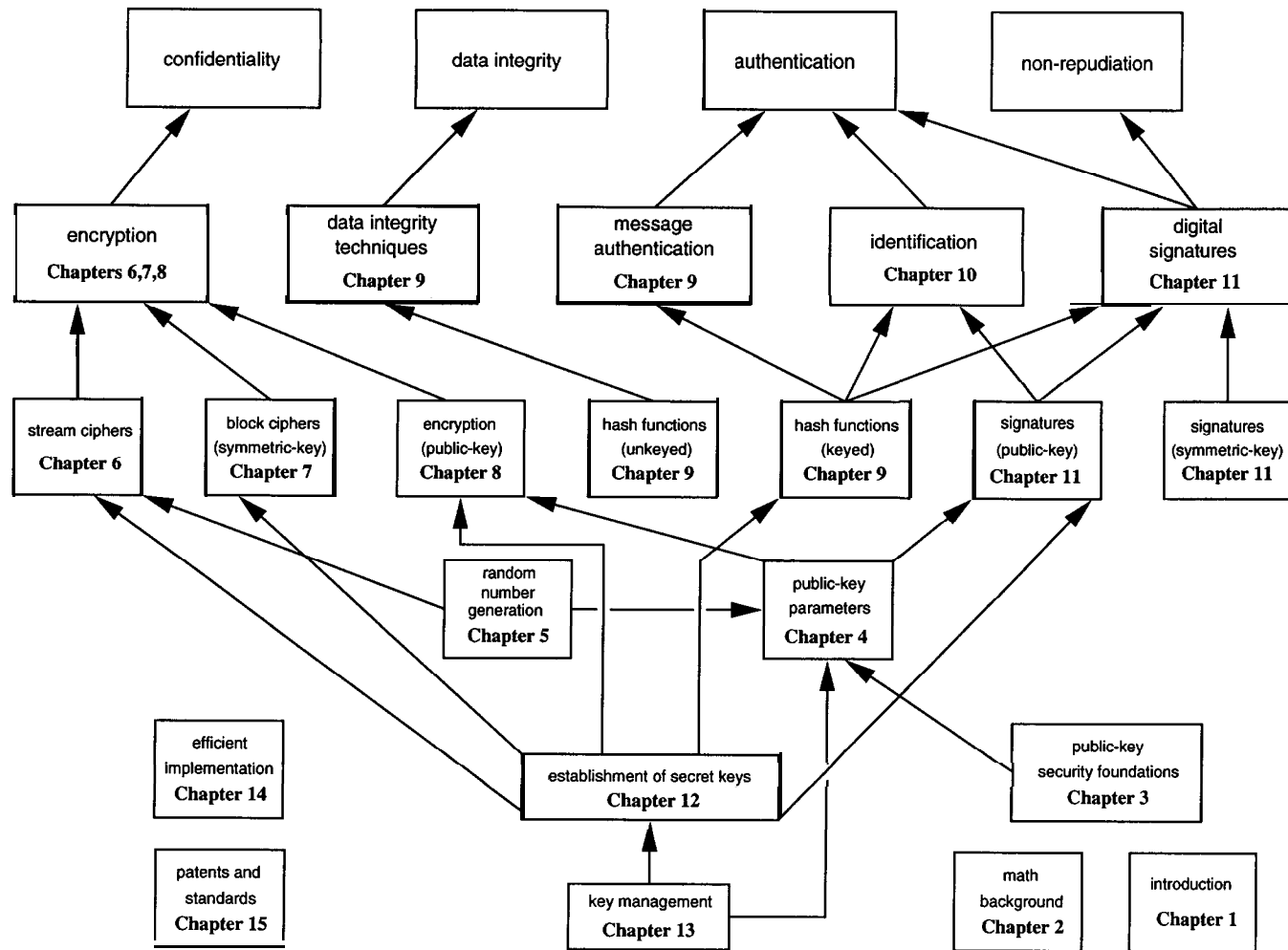
Table 1: Hierarchical levels of applied cryptography.

onto the various chapters, and their inter-dependence.

Table 2 lists the chapters of the book, along with the primary author(s) of each who should be contacted by readers with comments on specific chapters. Each chapter was written to provide a self-contained treatment of one major topic. Collectively, however, the chapters have been designed and carefully integrated to be entirely complementary with respect to definitions, terminology, and notation. Furthermore, there is essentially no duplication of material across chapters; instead, appropriate cross-chapter references are provided where relevant.

While it is not intended that this book be read linearly from front to back, the material has been arranged so that doing so has some merit. Two primary goals motivated by the “handbook” nature of this project were to allow easy access to stand-alone results, and to allow results and algorithms to be easily referenced (e.g., for discussion or subsequent cross-reference). To facilitate the ease of accessing and referencing results, items have been categorized and numbered to a large extent, with the following classes of items jointly numbered consecutively in each chapter: **Definitions**, **Examples**, **Facts**, **Notes**, **Remarks**, **Algorithms**, **Protocols**, and **Mechanisms**. In more traditional treatments, **Facts** are usually identified as propositions, lemmas, or theorems. We use numbered **Notes** for additional technical points,

Figure 1: Roadmap of the book.



Chapter	Primary Author		
	AIM	PVO	SAV
1. Overview of Cryptography	*	*	*
2. Mathematical Background	*		
3. Number-Theoretic Reference Problems	*		
4. Public-Key Parameters	*	*	
5. Pseudorandom Bits and Sequences	*		
6. Stream Ciphers			
7. Block Ciphers		*	
8. Public-Key Encryption	*		
9. Hash Functions and Data Integrity		*	
10. Identification and Entity Authentication		*	
11. Digital Signatures			*
12. Key Establishment Protocols		*	
13. Key Management Techniques		*	
14. Efficient Implementation			*
15. Patents and Standards		*	
- Overall organization	*	*	

Tab/e 2: Primary authors of each chapter.

while numbered **Remarks** identify non-technical (often non-rigorous) comments, observations, and opinions. **Algorithms**, **Protocols** and **Mechanisms** refer to techniques involving a series of steps. **Examples**, **Notes**, and **Remarks** generally begin with parenthetical summary titles to allow faster access, by indicating the nature of the content so that the entire item itself need not be read in order to determine this. The use of a large number of small subsections is also intended to enhance the handbook nature and accessibility to results.

Regarding the partitioning of subject areas into chapters, we have used what we call a **functional organization** (based on functions of interest to end-users). For example, all items related to entity authentication are addressed in one chapter. An alternative would have been what may be called an **academic organization**, under which perhaps, all protocols based on zero-knowledge concepts (including both a subset of entity authentication protocols and signature schemes) might be covered in one chapter. We believe that a functional organization is more convenient to the practitioner, who is more likely to be interested in options available for an entity authentication protocol (Chapter 10) or a signature scheme (Chapter 11), than to be seeking a zero-knowledge protocol with unspecified end-purpose.

In the front matter, a top-level Table of Contents (giving chapter numbers and titles only) is provided, as well as a detailed Table of Contents (down to the level of subsections, e.g., §5.1.1). This is followed by a List of Figures, and a List of Tables. At the start of each chapter, a brief Table of Contents (specifying section number and titles only, e.g., §5.1, §5.2) is also given for convenience.

At the end of the book, we have included a list of papers presented at each of the Crypto, Eurocrypt, Asiacrypt/Auscrypt and Fast Software Encryption conferences to date, as well as a list of all papers published in the **Journal of Cryptology** up to Volume 9. These are in addition to the **References** section, each entry of which is cited at least once in the body of the handbook. Almost all of these references have been verified for correctness in their exact titles, volume and page numbers, etc. Finally, an extensive Index prepared by the authors is included. The Index begins with a List of Symbols.

Our intention was not to introduce a collection of new techniques and protocols, but

rather to selectively present techniques from those currently available in the public domain. Such a consolidation of the literature is necessary from time to time. The fact that many good books in this field include essentially no more than what is covered here in Chapters 7, 8 and 11 (indeed, these might serve as an introductory course along with Chapter 1) illustrates that the field has grown tremendously in the past 15 years. The mathematical foundation presented in Chapters 2 and 3 is hard to find in one volume, and missing from most cryptography texts. The material in Chapter 4 on generation of public-key parameters, and in Chapter 14 on efficient implementations, while well-known to a small body of specialists and available in the scattered literature, has previously not been available in general texts. The material in Chapters 5 and 6 on pseudorandom number generation and stream ciphers is also often absent (many texts focus entirely on block ciphers), or approached only from a theoretical viewpoint. Hash functions (Chapter 9) and identification protocols (Chapter 10) have only recently been studied in depth as specialized topics on their own, and along with Chapter 12 on key establishment protocols, it is hard to find consolidated treatments of these now-mainstream topics. Key management techniques as presented in Chapter 13 have traditionally not been given much attention by cryptographers, but are of great importance in practice. A focused treatment of cryptographic patents and a concise summary of cryptographic standards, as presented in Chapter 15, are also long overdue.

In most cases (with some historical exceptions), where algorithms are known to be insecure, we have chosen to leave out specification of their details, because most such techniques are of little practical interest. Essentially all of the algorithms included have been verified for correctness by independent implementation, confirming the test vectors specified.

Acknowledgements

This project would not have been possible without the tremendous efforts put forth by our peers who have taken the time to read endless drafts and provide us with technical corrections, constructive feedback, and countless suggestions. In particular, the advice of our Advisory Editors has been invaluable, and it is impossible to attribute individual credit for their many suggestions throughout this book. Among our Advisory Editors, we would particularly like to thank:

Mihir Bellare	Don Coppersmith	Dorothy Denning	Walter Fumy
Burt Kaliski	Peter Landrock	Arjen Lenstra	Ueli Maurer
Chris Mitchell	Tatsuaki Okamoto	Bart Preneel	Ron Rivest
Gus Simmons	Miles Smid	Jacques Stern	Mike Wiener
Yacov Yacobi			

In addition, we gratefully acknowledge the exceptionally large number of additional individuals who have helped improve the quality of this volume, by providing highly appreciated feedback and guidance on various matters. These individuals include:

Carlisle Adams	Rich Ankney	Tom Berson
Simon Blackburn	Ian Blake	Antoon Bosselaers
Colin Boyd	Jörgen Brandt	Mike Burrnester
Ed Dawson	Peter de Rooij	Yvo Desmedt
Whit Diffie	Hans Dobbertin	Carl Ellison
Luis Encinas	Warwick Ford	Amparo Fuster
Shuhong Gao	Will Gilbert	Marc Girault
Jovan Golić	Dieter Gollmann	Li Gong

Carrie Grant	Blake Greenlee	Helen Gustafson
Darrel Hankerson	Anwar Hasan	Don Johnson
Mike Just	Andy Klapper	Lars Knudsen
Neal Koblit	Çetin Koç	Judy Koeller
Evangelos Kranakis	David Kravitz	Hugo Krawczyk
Xuejia Lai	Charles Lam	Alan Ling
S. Mike Matyas	Willi Meier	Peter Montgomery
Mike Mosca	Tim Moses	Serge Mister
Volker Mueller	David Naccache	James Nechvatal
Kaisa Nyberg	Andrew Odlyzko	Richard Outerbridge
Walter Penzhorn	Birgit Pfitzmann	Kevin Phelps
Leon Pintsov	Fred Piper	Carl Pomerance
Matt Robshaw	Peter Rodney	Phil Rogaway
Rainer Rueppel	Mahmoud Salmasizadeh	Roger Schlafly
Jeff Shallit	Jon Sorenson	Doug Stinson
Andrea Vanstone	Serge Vaudenay	Klaus Vedder
Jerry Veeh	Fausto Vitini	Lisa Yin
Robert Zuccherato		

We apologize to those whose names have inadvertently escaped this list. Special thanks are due to Carrie Grant, Darrel Hankerson, Judy Koeller, Charles Lam, and Andrea Vanstone. Their hard work contributed greatly to the quality of this book, and it was truly a pleasure working with them. Thanks also to the folks at CRC Press, including Tia Atchison, Gary Bennett, Susie Carlisle, Nora Konopka, Mary Kugler, Amy Morrell, Tim Pletscher, Bob Stern, and Wayne Yuhasz. The second author would also like to thank his colleagues past and present at Nortel Secure Networks (Bell-Northern Research), many of whom are mentioned above, for their contributions on this project, and in particular Brian O'Higgins for his encouragement and support; all views expressed, however, are entirely that of the author.

Any errors that remain are, of course, entirely our own. We would be grateful if readers who spot errors, missing references or credits, or incorrectly attributed results would contact us with details. It is our hope that this volume facilitates further advancement of the field, and that we have helped play a small part in this.

Alfred J. Menezes
Paul C. van Oorschot
Scott A. Vanstone