

HANDBOOK of APPLIED CRYPTOGRAPHY

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



CRC Press

Boca Raton London New York Washington, D.C.

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 0-8493-8523-7 (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

0005.8'2--dc21

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 N.W. Corporate Blvd., Boca Raton, Florida 33431.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation, without intent to infringe.

Visit the CRC Press Web site at www.crcpress.com

© 1997 by CRC Press LLC

No claim to original U.S. Government works

International Standard Book Number 0-8493-8523-7

Library of Congress Card Number 96-27609

Printed in the United States of America

5 6 7 8 9 0

Printed on acid-free paper

To Archie and Lida Menezes

**To Cornelis Henricus van Oorschot
and Maria Anna Buys van Vugt**

To Margaret and Gordon Vanstone

Contents in Brief

- 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
- A Bibliography of Papers from Selected Cryptographic Forums
- References

Table of Contents

1 Overview of Cryptography

- 1.1 Introduction
- 1.2 Information security and cryptography
- 1.3 Background on functions
 - 1.3.1 Functions (1-1, one-way, trapdoor one-way)
 - 1.3.2 Permutations
 - 1.3.3 Involutions
- 1.4 Basic terminology and concepts
- 1.5 Symmetric-key encryption
 - 1.5.1 Overview of block ciphers and stream ciphers
 - 1.5.2 Substitution ciphers and transposition ciphers
 - 1.5.3 Composition of ciphers
 - 1.5.4 Stream ciphers
 - 1.5.5 The key space
- 1.6 Digital signatures
- 1.7 Authentication and identification
 - 1.7.1 Identification
 - 1.7.2 Data origin authentication
- 1.8 Public-key cryptography
 - 1.8.1 Public-key encryption
 - 1.8.2 The necessity of authentication in public-key systems
 - 1.8.3 Digital signatures from reversible public-key encryption
 - 1.8.4 Symmetric-key vs. public-key cryptography
- 1.9 Hash functions
- 1.10 Protocols and mechanisms
- 1.11 Key establishment, management, and certification
 - 1.11.1 Key management through symmetric-key techniques
 - 1.11.2 Key management through public-key techniques
 - 1.11.3 Trusted third parties and public-key certificates
- 1.12 Pseudorandom numbers and sequences
- 1.13 Classes of attacks and security models
 - 1.13.1 Attacks on encryption schemes
 - 1.13.2 Attacks on protocols
 - 1.13.3 Models for evaluating security
 - 1.13.4 Perspective for computational security
- 1.14 Notes and further references

2 Mathematical Background

- 2.1 Probability theory
 - 2.1.1 Basic definitions
 - 2.1.2 Conditional probability
 - 2.1.3 Random variables
 - 2.1.4 Binomial distribution
 - 2.1.5 Birthday problems
 - 2.1.6 Random mappings
- 2.2 Information theory
 - 2.2.1 Entropy
 - 2.2.2 Mutual information
- 2.3 Complexity theory
 - 2.3.1 Basic definitions
 - 2.3.2 Asymptotic notation
 - 2.3.3 Complexity classes
 - 2.3.4 Randomized algorithms
- 2.4 Number theory
 - 2.4.1 The integers
 - 2.4.2 Algorithms in \mathbb{Z}
 - 2.4.3 The integers modulo n
 - 2.4.4 Algorithms in \mathbb{Z}_n
 - 2.4.5 The Legendre and Jacobi symbols
 - 2.4.6 Blum integers
- 2.5 Abstract algebra
 - 2.5.1 Groups
 - 2.5.2 Rings
 - 2.5.3 Fields
 - 2.5.4 Polynomial rings
 - 2.5.5 Vector spaces
- 2.6 Finite fields
 - 2.6.1 Basic properties
 - 2.6.2 The Euclidean algorithm for polynomials
 - 2.6.3 Arithmetic of polynomials
- 2.7 Notes and further references

3 Number-Theoretic Reference Problems

- 3.1 Introduction and overview
- 3.2 The integer factorization problem
 - 3.2.1 Trial division
 - 3.2.2 Pollard's rho factoring algorithm
 - 3.2.3 Pollard's $p - 1$ factoring algorithm
 - 3.2.4 Elliptic curve factoring
 - 3.2.5 Random square factoring methods
 - 3.2.6 Quadratic sieve factoring
 - 3.2.7 Number field sieve factoring
- 3.3 The RSA problem
- 3.4 The quadratic residuosity problem
- 3.5 Computing square roots in \mathbb{Z}_n
 - 3.5.1 Case (i): n prime
 - 3.5.2 Case (ii): n composite

- 3.6 The discrete logarithm problem
 - 3.6.1 Exhaustive search
 - 3.6.2 Baby-step giant-step algorithm
 - 3.6.3 Pollard's rho algorithm for logarithms
 - 3.6.4 Pohlig-Hellman algorithm
 - 3.6.5 Index-calculus algorithm
 - 3.6.6 Discrete logarithm problem in subgroups of \mathbb{Z}_p^*
- 3.7 The Diffie-Hellman problem
- 3.8 Composite moduli
- 3.9 Computing individual bits
 - 3.9.1 The discrete logarithm problem in \mathbb{Z}_p^* — individual bits
 - 3.9.2 The RSA problem — individual bits
 - 3.9.3 The Rabin problem — individual bits
- 3.10 The subset sum problem
 - 3.10.1 The L^3 -lattice basis reduction algorithm
 - 3.10.2 Solving subset sum problems of low density
 - 3.10.3 Simultaneous diophantine approximation
- 3.11 Factoring polynomials over finite fields
 - 3.11.1 Square-free factorization
 - 3.11.2 Berlekamp's Q -matrix algorithm
- 3.12 Notes and further references

4 Public-Key Parameters

- 4.1 Introduction
 - 4.1.1 Approaches to generating large prime numbers
 - 4.1.2 Distribution of prime numbers
- 4.2 Probabilistic primality tests
 - 4.2.1 Fermat's test
 - 4.2.2 Solovay-Strassen test
 - 4.2.3 Miller-Rabin test
 - 4.2.4 Comparison: Fermat, Solovay-Strassen, and Miller-Rabin
- 4.3 (True) Primality tests
 - 4.3.1 Testing Mersenne numbers
 - 4.3.2 Primality testing using the factorization of $n - 1$
 - 4.3.3 Jacobi sum test
 - 4.3.4 Tests using elliptic curves
- 4.4 Prime number generation
 - 4.4.1 Random search for probable primes
 - 4.4.2 Strong primes
 - 4.4.3 NIST method for generating DSA primes
 - 4.4.4 Constructive techniques for provable primes
- 4.5 Irreducible polynomials over \mathbb{Z}_p
 - 4.5.1 Irreducible polynomials
 - 4.5.2 Irreducible trinomials
 - 4.5.3 Primitive polynomials
- 4.6 Generators and elements of high order
 - 4.6.1 Selecting a prime p and generator of \mathbb{Z}_p^*
- 4.7 Notes and further references

5 Pseudorandom Bits and Sequences

- 5.1 Introduction
 - 5.1.1 Background and Classification
- 5.2 Random bit generation
- 5.3 Pseudorandom bit generation
 - 5.3.1 ANSI X9.17 generator
 - 5.3.2 FIPS 186 generator
- 5.4 Statistical tests
 - 5.4.1 The normal and chi-square distributions
 - 5.4.2 Hypothesis testing
 - 5.4.3 Golomb's randomness postulates
 - 5.4.4 Five basic tests
 - 5.4.5 Maurer's universal statistical test
- 5.5 Cryptographically secure pseudorandom bit generation
 - 5.5.1 RSA pseudorandom bit generator
 - 5.5.2 Blum-Blum-Shub pseudorandom bit generator
- 5.6 Notes and further references

6 Stream Ciphers

- 6.1 Introduction
 - 6.1.1 Classification
- 6.2 Feedback shift registers
 - 6.2.1 Linear feedback shift registers
 - 6.2.2 Linear complexity
 - 6.2.3 Berlekamp-Massey algorithm
 - 6.2.4 Nonlinear feedback shift registers
- 6.3 Stream ciphers based on LFSRs
 - 6.3.1 Nonlinear combination generators
 - 6.3.2 Nonlinear filter generators
 - 6.3.3 Clock-controlled generators
- 6.4 Other stream ciphers
 - 6.4.1 SEAL
- 6.5 Notes and further references

7 Block Ciphers

- 7.1 Introduction and overview
- 7.2 Background and general concepts
 - 7.2.1 Introduction to block ciphers
 - 7.2.2 Modes of operation
 - 7.2.3 Exhaustive key search and multiple encryption
- 7.3 Classical ciphers and historical development
 - 7.3.1 Transposition ciphers (background)
 - 7.3.2 Substitution ciphers (background)
 - 7.3.3 Polyalphabetic substitutions and Vigenère ciphers (historical)
 - 7.3.4 Polyalphabetic cipher machines and rotors (historical)
 - 7.3.5 Cryptanalysis of classical ciphers (historical)
- 7.4 DES
 - 7.4.1 Product ciphers and Feistel ciphers
 - 7.4.2 DES algorithm
 - 7.4.3 DES properties and strength

- 7.5 FEAL
- 7.6 IDEA
- 7.7 SAFER, RC5, and other block ciphers
 - 7.7.1 SAFER
 - 7.7.2 RC5
 - 7.7.3 Other block ciphers
- 7.8 Notes and further references

8 Public-Key Encryption

- 8.1 Introduction
 - 8.1.1 Basic principles
- 8.2 RSA public-key encryption
 - 8.2.1 Description
 - 8.2.2 Security of RSA
 - 8.2.3 RSA encryption in practice
- 8.3 Rabin public-key encryption
- 8.4 ElGamal public-key encryption
 - 8.4.1 Basic ElGamal encryption
 - 8.4.2 Generalized ElGamal encryption
- 8.5 McEliece public-key encryption
- 8.6 Knapsack public-key encryption
 - 8.6.1 Merkle-Hellman knapsack encryption
 - 8.6.2 Chor-Rivest knapsack encryption
- 8.7 Probabilistic public-key encryption
 - 8.7.1 Goldwasser-Micali probabilistic encryption
 - 8.7.2 Blum-Goldwasser probabilistic encryption
 - 8.7.3 Plaintext-aware encryption
- 8.8 Notes and further references

9 Hash Functions and Data Integrity

- 9.1 Introduction
- 9.2 Classification and framework
 - 9.2.1 General classification
 - 9.2.2 Basic properties and definitions
 - 9.2.3 Hash properties required for specific applications
 - 9.2.4 One-way functions and compression functions
 - 9.2.5 Relationships between properties
 - 9.2.6 Other hash function properties and applications
- 9.3 Basic constructions and general results
 - 9.3.1 General model for iterated hash functions
 - 9.3.2 General constructions and extensions
 - 9.3.3 Formatting and initialization details
 - 9.3.4 Security objectives and basic attacks
 - 9.3.5 Bitsizes required for practical security
- 9.4 Unkeyed hash functions (MDCs)
 - 9.4.1 Hash functions based on block ciphers
 - 9.4.2 Customized hash functions based on MD4
 - 9.4.3 Hash functions based on modular arithmetic
- 9.5 Keyed hash functions (MACs)
 - 9.5.1 MACs based on block ciphers

- 9.5.2 Constructing MACs from MDCs
- 9.5.3 Customized MACs
- 9.5.4 MACs for stream ciphers
- 9.6 Data integrity and message authentication
 - 9.6.1 Background and definitions
 - 9.6.2 Non-malicious vs. malicious threats to data integrity
 - 9.6.3 Data integrity using a MAC alone
 - 9.6.4 Data integrity using an MDC and an authentic channel
 - 9.6.5 Data integrity combined with encryption
- 9.7 Advanced attacks on hash functions
 - 9.7.1 Birthday attacks
 - 9.7.2 Pseudo-collisions and compression function attacks
 - 9.7.3 Chaining attacks
 - 9.7.4 Attacks based on properties of underlying cipher
- 9.8 Notes and further references

10 Identification and Entity Authentication

- 10.1 Introduction
 - 10.1.1 Identification objectives and applications
 - 10.1.2 Properties of identification protocols
- 10.2 Passwords (weak authentication)
 - 10.2.1 Fixed password schemes: techniques
 - 10.2.2 Fixed password schemes: attacks
 - 10.2.3 Case study – UNIX passwords
 - 10.2.4 PINs and passkeys
 - 10.2.5 One-time passwords (towards strong authentication)
- 10.3 Challenge-response identification (strong authentication)
 - 10.3.1 Background on time-variant parameters
 - 10.3.2 Challenge-response by symmetric-key techniques
 - 10.3.3 Challenge-response by public-key techniques
- 10.4 Customized and zero-knowledge identification protocols
 - 10.4.1 Overview of zero-knowledge concepts
 - 10.4.2 Feige-Fiat-Shamir identification protocol
 - 10.4.3 GQ identification protocol
 - 10.4.4 Schnorr identification protocol
 - 10.4.5 Comparison: Fiat-Shamir, GQ, and Schnorr
- 10.5 Attacks on identification protocols
- 10.6 Notes and further references

11 Digital Signatures

- 11.1 Introduction
- 11.2 A framework for digital signature mechanisms
 - 11.2.1 Basic definitions
 - 11.2.2 Digital signature schemes with appendix
 - 11.2.3 Digital signature schemes with message recovery
 - 11.2.4 Types of attacks on signature schemes
- 11.3 RSA and related signature schemes
 - 11.3.1 The RSA signature scheme
 - 11.3.2 Possible attacks on RSA signatures
 - 11.3.3 RSA signatures in practice

- 11.3.4 The Rabin public-key signature scheme
 - 11.3.5 ISO/IEC 9796 formatting
 - 11.3.6 PKCS #1 formatting
 - 11.4 Fiat-Shamir signature schemes
 - 11.4.1 Feige-Fiat-Shamir signature scheme
 - 11.4.2 GQ signature scheme
 - 11.5 The DSA and related signature schemes
 - 11.5.1 The Digital Signature Algorithm (DSA)
 - 11.5.2 The ElGamal signature scheme
 - 11.5.3 The Schnorr signature scheme
 - 11.5.4 The ElGamal signature scheme with message recovery
 - 11.6 One-time digital signatures
 - 11.6.1 The Rabin one-time signature scheme
 - 11.6.2 The Merkle one-time signature scheme
 - 11.6.3 Authentication trees and one-time signatures
 - 11.6.4 The GMR one-time signature scheme
 - 11.7 Other signature schemes
 - 11.7.1 Arbitrated digital signatures
 - 11.7.2 ESIGN
 - 11.8 Signatures with additional functionality
 - 11.8.1 Blind signature schemes
 - 11.8.2 Undeniable signature schemes
 - 11.8.3 Fail-stop signature schemes
 - 11.9 Notes and further references
- 12 Key Establishment Protocols**
- 12.1 Introduction
 - 12.2 Classification and framework
 - 12.2.1 General classification and fundamental concepts
 - 12.2.2 Objectives and properties
 - 12.2.3 Assumptions and adversaries in key establishment protocols
 - 12.3 Key transport based on symmetric encryption
 - 12.3.1 Symmetric key transport and derivation without a server
 - 12.3.2 Kerberos and related server-based protocols
 - 12.4 Key agreement based on symmetric techniques
 - 12.5 Key transport based on public-key encryption
 - 12.5.1 Key transport using PK encryption without signatures
 - 12.5.2 Protocols combining PK encryption and signatures
 - 12.5.3 Hybrid key transport protocols using PK encryption
 - 12.6 Key agreement based on asymmetric techniques
 - 12.6.1 Diffie-Hellman and related key agreement protocols
 - 12.6.2 Implicitly-certified public keys
 - 12.6.3 Diffie-Hellman protocols using implicitly-certified keys
 - 12.7 Secret sharing
 - 12.7.1 Simple shared control schemes
 - 12.7.2 Threshold schemes
 - 12.7.3 Generalized secret sharing
 - 12.8 Conference keying
 - 12.9 Analysis of key establishment protocols
 - 12.9.1 Attack strategies and classic protocol flaws

12.9.2 Analysis objectives and methods

12.10 Notes and further references

13 Key Management Techniques

- 13.1 Introduction
- 13.2 Background and basic concepts
 - 13.2.1 Classifying keys by algorithm type and intended use
 - 13.2.2 Key management objectives, threats, and policy
 - 13.2.3 Simple key establishment models
 - 13.2.4 Roles of third parties
 - 13.2.5 Tradeoffs among key establishment protocols
- 13.3 Techniques for distributing confidential keys
 - 13.3.1 Key layering and cryptoperiods
 - 13.3.2 Key translation centers and symmetric-key certificates
- 13.4 Techniques for distributing public keys
 - 13.4.1 Authentication trees
 - 13.4.2 Public-key certificates
 - 13.4.3 Identity-based systems
 - 13.4.4 Implicitly-certified public keys
 - 13.4.5 Comparison of techniques for distributing public keys
- 13.5 Techniques for controlling key usage
 - 13.5.1 Key separation and constraints on key usage
 - 13.5.2 Techniques for controlling use of symmetric keys
- 13.6 Key management involving multiple domains
 - 13.6.1 Trust between two domains
 - 13.6.2 Trust models involving multiple certification authorities
 - 13.6.3 Certificate distribution and revocation
- 13.7 Key life cycle issues
 - 13.7.1 Lifetime protection requirements
 - 13.7.2 Key management life cycle
- 13.8 Advanced trusted third party services
 - 13.8.1 Trusted timestamping service
 - 13.8.2 Non-repudiation and notarization of digital signatures
 - 13.8.3 Key escrow
- 13.9 Notes and further references

14 Efficient Implementation

- 14.1 Introduction
- 14.2 Multiple-precision integer arithmetic
 - 14.2.1 Radix representation
 - 14.2.2 Addition and subtraction
 - 14.2.3 Multiplication
 - 14.2.4 Squaring
 - 14.2.5 Division
- 14.3 Multiple-precision modular arithmetic
 - 14.3.1 Classical modular multiplication
 - 14.3.2 Montgomery reduction
 - 14.3.3 Barrett reduction
 - 14.3.4 Reduction methods for moduli of special form
- 14.4 Greatest common divisor algorithms

- 14.4.1 Binary gcd algorithm
- 14.4.2 Lehmer's gcd algorithm
- 14.4.3 Binary extended gcd algorithm
- 14.5 Chinese remainder theorem for integers
 - 14.5.1 Residue number systems
 - 14.5.2 Garner's algorithm
- 14.6 Exponentiation
 - 14.6.1 Techniques for general exponentiation
 - 14.6.2 Fixed-exponent exponentiation algorithms
 - 14.6.3 Fixed-base exponentiation algorithms
- 14.7 Exponent recoding
 - 14.7.1 Signed-digit representation
 - 14.7.2 String-replacement representation
- 14.8 Notes and further references

15 Patents and Standards

- 15.1 Introduction
- 15.2 Patents on cryptographic techniques
 - 15.2.1 Five fundamental patents
 - 15.2.2 Ten prominent patents
 - 15.2.3 Ten selected patents
 - 15.2.4 Ordering and acquiring patents
- 15.3 Cryptographic standards
 - 15.3.1 International standards – cryptographic techniques
 - 15.3.2 Banking security standards (ANSI, ISO)
 - 15.3.3 International security architectures and frameworks
 - 15.3.4 U.S. government standards (FIPS)
 - 15.3.5 Internet standards and RFCs
 - 15.3.6 De facto standards
 - 15.3.7 Ordering and acquiring standards
- 15.4 Notes and further references

A Bibliography of Papers from Selected Cryptographic Forums

- A.1 Asiacrypt/Auscript Proceedings
- A.2 Crypto Proceedings
- A.3 Eurocrypt Proceedings
- A.4 Fast Software Encryption Proceedings
- A.5 Journal of Cryptology papers

References

List of Tables

- 1.1 Some information security objectives
- 1.2 Reference numbers comparing relative magnitudes
- 1.3 Prefixes used for various powers of 10

- 2.1 Bit complexity of basic operations in \mathbb{Z}
- 2.2 Extended Euclidean algorithm (example)
- 2.3 Orders of elements in \mathbb{Z}_{21}^*
- 2.4 Computation of $5^{596} \bmod 1234$
- 2.5 Bit complexity of basic operations in \mathbb{Z}_n
- 2.6 Jacobi symbols of elements in \mathbb{Z}_{21}^*
- 2.7 The subgroups of \mathbb{Z}_{19}^*
- 2.8 Complexity of basic operations in \mathbb{F}_{p^m}
- 2.9 The powers of x modulo $f(x) = x^4 + x + 1$

- 3.1 Some computational problems of cryptographic relevance
- 3.2 Pollard's rho algorithm (example)
- 3.3 Running time estimates for numbers factored with QS

- 4.1 Smallest strong pseudoprimes
- 4.2 Known Mersenne primes
- 4.3 Upper bounds on $p_{k,t}$ for sample values of k and t
- 4.4 Number of Miller-Rabin iterations required so that $p_{k,t} \leq (\frac{1}{2})^{80}$
- 4.5 Upper bounds on the error probability of incremental search
- 4.6 Irreducible trinomials of degree m over \mathbb{Z}_2 , $1 \leq m \leq 722$
- 4.7 Irreducible trinomials of degree m over \mathbb{Z}_2 , $723 \leq m \leq 1478$
- 4.8 Primitive polynomials over \mathbb{Z}_2
- 4.9 Primitive polynomials of degree m over \mathbb{Z}_2 , $2^m - 1$ a Mersenne prime

- 5.1 Selected percentiles of the standard normal distribution
- 5.2 Selected percentiles of the χ^2 (chi-square) distribution
- 5.3 Mean and variance of X_u for Maurer's universal statistical test

- 6.1 Berlekamp-Massey algorithm (example)

- 7.1 Estimated roughness constant κ_p for various languages
- 7.2 DES initial permutation and inverse (IP and IP^{-1})
- 7.3 DES per-round functions: expansion E and permutation P
- 7.4 DES key schedule bit selections (PC1 and PC2)
- 7.5 DES weak keys
- 7.6 DES pairs of semi-weak keys
- 7.7 DES strength against various attacks
- 7.8 DES S-boxes
- 7.9 FEAL functions f, f_K
- 7.10 FEAL strength against various attacks
- 7.11 IDEA decryption subkeys derived from encryption subkeys
- 7.12 IDEA encryption sample: round subkeys and ciphertext

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

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

List of Figures

- 1.1 A taxonomy of cryptographic primitives
- 1.2 A function
- 1.3 A bijection and its inverse
- 1.4 An involution
- 1.5 A simple encryption scheme
- 1.6 Two-party communication using encryption
- 1.7 Two-party encryption with a secure channel for key exchange
- 1.8 Composition of two functions
- 1.9 Composition of two involutions
- 1.10 A signing and verification function for a digital signature scheme
- 1.11 Encryption using public-key techniques
- 1.12 Schematic use of public-key encryption
- 1.13 An impersonation attack on a two-party communication
- 1.14 A digital signature scheme with message recovery
- 1.15 Keying relationships in a simple 6-party network
- 1.16 Key management using a trusted third party (TTP)
- 1.17 Key management using public-key techniques
- 1.18 Impersonation by an active adversary
- 1.19 Authentication of public keys by a TTP

- 2.1 A functional graph
- 2.2 Conjectured relationship between some complexity classes

- 4.1 Relationships between Fermat, Euler, and strong liars

- 5.1 The normal distribution $N(0, 1)$
- 5.2 The χ^2 (chi-square) distribution with $v = 7$ degrees of freedom

- 6.1 General model of a synchronous stream cipher
- 6.2 General model of a binary additive stream cipher
- 6.3 General model of a self-synchronizing stream cipher
- 6.4 A linear feedback shift register (LFSR)
- 6.5 The LFSR $\langle 4, 1 + D + D^4 \rangle$
- 6.6 Linear complexity profile of a 20-periodic sequence
- 6.7 A feedback shift register (FSR)
- 6.8 A nonlinear combination generator
- 6.9 The Geffe generator
- 6.10 The summation generator
- 6.11 A nonlinear filter generator
- 6.12 The alternating step generator
- 6.13 The shrinking generator

- 7.1 Common modes of operation for an n -bit block cipher
- 7.2 Multiple encryption
- 7.3 The Jefferson cylinder

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

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

August 1996

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

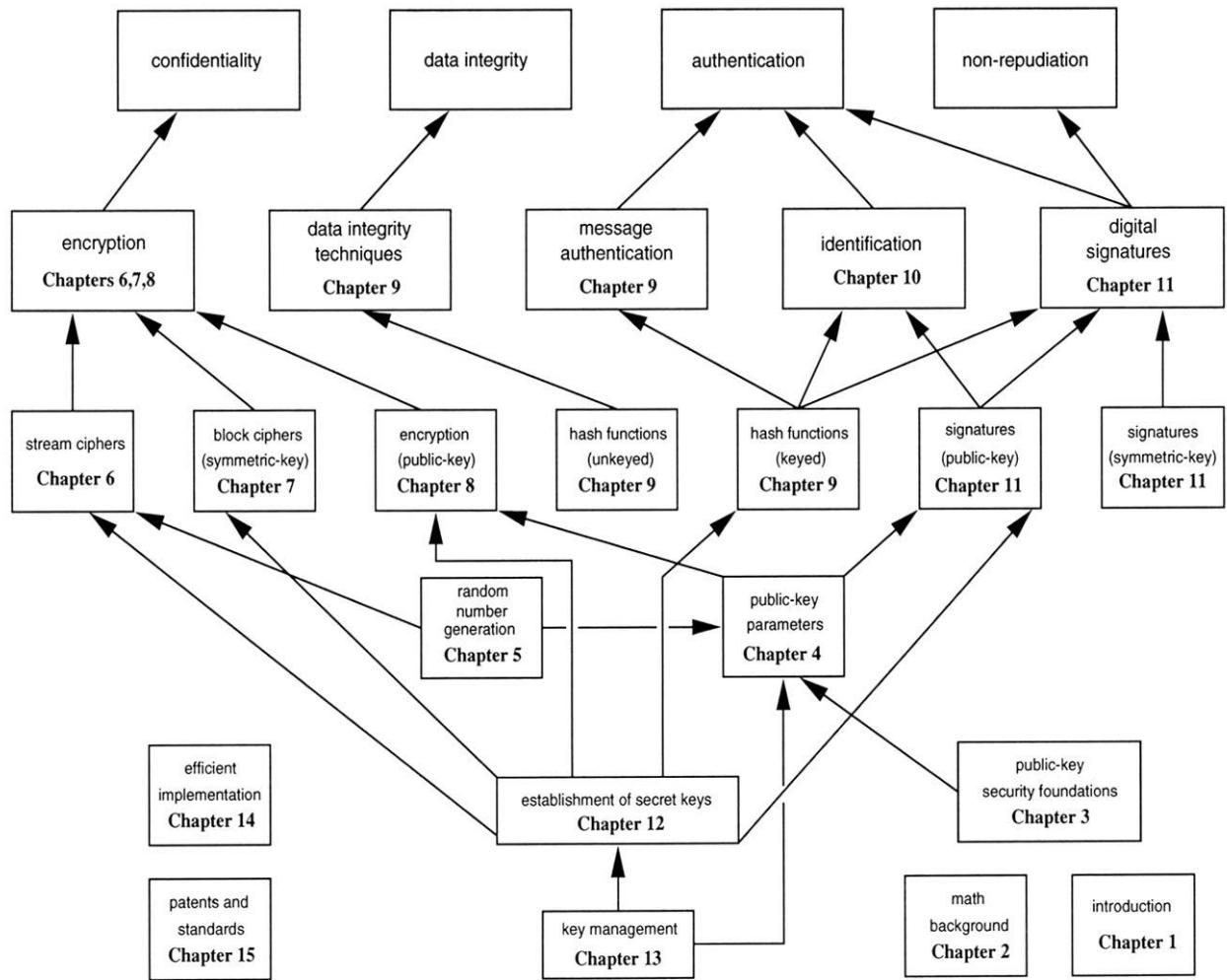
Information Security Objectives	
Confidentiality	
Data integrity	
Authentication (entity and data origin)	
Non-repudiation	
Cryptographic functions	
Encryption	Chapters 6, 7, 8
Message authentication and data integrity techniques	Chapter 9
Identification/entity authentication techniques	Chapter 10
Digital 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,



Chapter	Primary Author		
	AJM	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	*	*	

Table 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	Jørgen Brandt	Mike Burmester
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 Koblitz	Çetin Koç	Judy Koeller
Evangelos Kranakis	David Kravitz	Hugo Krawczyk
Xuejia Lai	Charles Lam	Alan Ling
S. Mike Matyas	Willi Meier	Serge Mister
Peter Montgomery	Mike Mosca	Tim Moses
Volker Müller	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 Schlaefly
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 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. The third author would also like to acknowledge the support of the Natural Sciences and Engineering Research Council.

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

Preface to the 5th printing

The 5th printing includes corrections to all the editorial and technical errors that we are aware of as of June 2001. We thank everyone for the tremendous reception they have given to our book, and for those who have taken the time to draw errors to our attention.

Alfred J. Menezes
Paul C. van Oorschot
Scott A. Vanstone
June 2001