

Discover the basic principles and techniques underlying modern cryptographic systems and protocols

NEW!

Introduction to Modern Cryptography

Jonathan Katz • University of Maryland, College Park, USA
Yehuda Lindell • Bar-Ilan University, Ramat Gan, Israel

A volume in the **Chapman & Hall/CRC Cryptography and Network Security Series**
Series edited by **Douglas R. Stinson**, University of Waterloo, Ontario, Canada

The Theory, Applications, and Underlying Mathematics of Modern Cryptography

Cryptography plays a key role in ensuring the privacy and integrity of data and the security of computer networks. **Introduction to Modern Cryptography** provides a rigorous yet accessible treatment of modern cryptography, with a focus on formal definitions, precise assumptions, and rigorous proofs.

The authors introduce the core principles of modern cryptography, including the modern, *computational* approach to security that overcomes the limitations of perfect secrecy. An extensive treatment of private-key encryption and message authentication follows. The authors also illustrate design principles for block ciphers, such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), and present provably secure constructions of block ciphers from lower-level primitives. The second half of the book focuses on public-key cryptography, beginning with a self-contained introduction to the number theory needed to understand the RSA, Diffie–Hellman, El Gamal, and other cryptosystems. After exploring public-key encryption and digital signatures, the book concludes with a discussion of the random oracle model and its applications.

Serving as a textbook, a reference, or for self-study, **Introduction to Modern Cryptography** presents the necessary tools to fully understand this fascinating subject.

FEATURES

- Includes formal definitions, precise assumptions, and rigorous proofs
- Discusses many widely used cryptographic algorithms and standards
- Covers topics, such as pseudorandom generators/functions, Paillier encryption, and the random oracle model, often not found in other texts
- Contains suggestions for further reading as well as numerous exercises at the end of each chapter
- Assumes minimal prerequisites—all necessary mathematical background is included in the text

“Over the past 30 years, cryptography has been transformed from a mysterious art into a mathematically rigorous science. The textbook by Jonathan Katz and Yehuda Lindell finally makes this modern approach to cryptography accessible to a broad audience. Readers of this text will learn how to think precisely about the security of protocols against arbitrary attacks, a skill that will remain relevant and useful regardless of how technology and cryptography standards change. The book uses just enough formalism to maintain precision and rigor without obscuring the development of ideas. It manages to convey both the theory’s conceptual beauty and its relevance to practice. I plan to use it every time I teach an undergraduate course in cryptography.”

—Salil Vadhan, Harvard University, Cambridge, Massachusetts, USA

CONTENTS

PREFACE

INTRODUCTION AND CLASSICAL CRYPTOGRAPHY

INTRODUCTION

Cryptography and Modern Cryptography
The Setting of Private-Key Encryption
Historical Ciphers and Their Cryptanalysis
The Basic Principles of Modern Cryptography
PERFECTLY SECRET ENCRYPTION
Definitions and Basic Properties
The One-Time Pad (Vernam’s Cipher)
Limitations of Perfect Secrecy
Shannon’s Theorem
Summary

PRIVATE-KEY (SYMMETRIC) CRYPTOGRAPHY

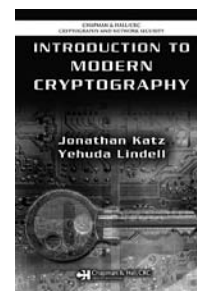
PRIVATE-KEY ENCRYPTION AND PSEUDORANDOMNESS

A Computational Approach to Cryptography
A Definition of Computationally Secure Encryption
Pseudorandomness
Constructing Secure Encryption Schemes
Security against Chosen-Plaintext Attacks (CPA)
Constructing CPA-Secure Encryption Schemes
Security against Chosen-Ciphertext Attacks (CCA)

MESSAGE AUTHENTICATION CODES AND COLLISION-RESISTANT HASH FUNCTIONS

Secure Communication and Message Integrity

See reverse side for continuation of Contents and ordering information



Contents continued...

Encryption vs. Message Authentication
 Message Authentication Codes—Definitions
 Constructing Secure Message Authentication Codes
 CBC-MAC
 Collision-Resistant Hash Functions
 NMAC and HMAC
 Constructing CCA-Secure Encryption Schemes
 Obtaining Privacy and Message Authentication
PRACTICAL CONSTRUCTIONS OF PSEUDORANDOM PERMUTATIONS (BLOCK CIPHERS)
 Substitution-Permutation Networks
 Feistel Networks
 The Data Encryption Standard (DES)
 Increasing the Key Size of a Block Cipher
 The Advanced Encryption Standard (AES)
 Differential and Linear Cryptanalysis—A Brief Look
THEORETICAL CONSTRUCTIONS OF PSEUDORANDOM OBJECTS
 One-Way Functions
 Overview: From One-Way Functions to Pseudorandomness
 A Hard-Core Predicate for Any One-Way Function
 Constructing Pseudorandom Generators
 Constructing Pseudorandom Functions
 Constructing (Strong) Pseudorandom Permutations
 Necessary Assumptions for Private-Key Cryptography
 A Digression—Computational Indistinguishability

PUBLIC-KEY (ASYMMETRIC) CRYPTOGRAPHY
NUMBER THEORY AND CRYPTOGRAPHIC HARDNESS ASSUMPTIONS
 Preliminaries and Basic Group Theory
 Primes, Factoring, and RSA
 Assumptions in Cyclic Groups
 Cryptographic Applications of Number-Theoretic Assumptions
FACTORING AND COMPUTING DISCRETE LOGARITHMS
 Algorithms for Factoring
 Algorithms for Computing Discrete Logarithms
PRIVATE-KEY MANAGEMENT AND THE PUBLIC-KEY REVOLUTION
 Limitations of Private-Key Cryptography
 A Partial Solution—Key Distribution Centers
 The Public-Key Revolution
 Diffie–Hellman Key Exchange
PUBLIC-KEY ENCRYPTION
 Public-Key Encryption—An Overview
 Definitions
 Hybrid Encryption
 RSA Encryption
 The El Gamal Encryption Scheme
 Security against CCA
 Trapdoor Permutations
ADDITIONAL PUBLIC-KEY ENCRYPTION SCHEMES
 The Goldwasser–Micali Encryption Scheme

The Rabin Encryption Scheme
 The Paillier Encryption Scheme
DIGITAL SIGNATURE SCHEMES
 Digital Signatures—An Overview
 Definitions
 RSA Signatures
 The Hash-and-Sign Paradigm
 Lamport’s One-Time Signature Scheme
 Signatures from Collision-Resistant Hashing
 The Digital Signature Standard
 Certificates and Public-Key Infrastructures
PUBLIC-KEY CRYPTOSYSTEMS IN THE RANDOM ORACLE MODEL
 The Random Oracle Methodology
 Public-Key Encryption in the Random Oracle Model
 Signatures in the Random Oracle Model
APPENDIX A: MATHEMATICAL BACKGROUND
 Identities and Inequalities
 Asymptotic Notation
 Basic Probability
 The Birthday Problem
APPENDIX B: SUPPLEMENTARY ALGORITHMIC NUMBER THEORY
 Integer Arithmetic
 Modular Arithmetic
 Finding a Generator of a Cyclic Group
INDEX
Each chapter contains References, Additional Reading, and Exercises.

FREE SHIPPING ON ALL ORDERS when you ORDER ONLINE at WWW.CRCPRESS.COM

Please indicate quantities next to the title(s) ordered below:

INTRODUCTION TO MODERN CRYPTOGRAPHY
Catalog no. C5513, ISBN: 978-1-58488-551-1 at \$79.95 / £39.99 each.

Other titles of interest:

ELLIPTIC CURVES: NUMBER THEORY AND CRYPTOGRAPHY
Catalog no. C3650, ISBN: 978-1-58488-365-4 at \$84.99 / £49.99 each.

CRYPTOGRAPHY: THEORY AND PRACTICE, THIRD EDITION
Catalog no. C5084, ISBN: 978-1-58488-508-5 at \$69.95 / £39.99 each.

AN INTRODUCTION TO CRYPTOGRAPHY, SECOND EDITION
Catalog no. C6188, ISBN: 978-1-58488-618-1 at \$79.95 / £39.99 each.

Ordering Information: Orders must be prepaid or accompanied by a purchase order. Checks should be made payable to CRC Press. Please add the appropriate shipping and handling charge for each book ordered. All prices are subject to change without notice. If purchasing by credit card please be sure to include the 3 digit security code that appears on the back of your card in the "sec code" field provided below.

U.S./Canada: All orders must be paid in U.S. dollars. TAX: As required by law, please add applicable state and local taxes on all merchandise delivered to CA, CT, FL, KY, MO, NY, and PA. For Canadian orders, please add GST. We will add tax on all credit card orders. **European Orders:** All orders must be paid in U.K. £. VAT will be added at the rate applicable. **Textbooks:** Special prices for course adopted textbooks may be available for certain titles. To review a book for class adoption, contact our Academic Sales Department or submit your textbook evaluation request online at www.crcpress.com/eval.htm **Satisfaction Guaranteed:** If the book supplied does not meet your expectations, it may be returned to us in a saleable condition within 30 days of receipt for a full refund.

SHIPPING AND HANDLING				For priority mail services, please contact your nearest CRC PRESS office.
Region	Delivery Time	First Title	Additional Title	
USA/Canada	3-5 Days	\$5.99	\$1.99	
South America	7-14 Days	\$9.99	\$3.99	
Europe	3-5 Days	£2.99	£0.99	
Rest of World	7-21 Days	£4.99	£2.99	

Name
please print clearly

Company/Institution

Address

.....

City State/Province Zip/Postal Code

Country

Visa MasterCard American Express Check Enclosed \$

Sec. Code: _____ Exp. Date: _____
 _____ Month _____ Year

Signature and Telephone Number required on all orders

Signature PO#

Telephone

If you would like to receive information from us by e-mail, please provide your e-mail address below.

E-Mail Address

ORDERING LOCATIONS Corporate Offices

In the Americas:
CRC PRESS
 PO Box 409267
 Atlanta, GA 30384-9267
 Tel: 1-800-272-7737
 Fax: 1-800-374-3401
From Outside the Continental U.S.
 Tel: 1-561-994-0555
 Fax: 1-561-361-6018
 e-mail: orders@taylorandfrancis.com

Rest of the World:
CRC PRESS / ITPS
 Cheriton House, North Way
 Andover, Hants, SP10 5BE, UK
 Tel (UK): +44 (0) 1264 34 2926
 Tel (Int'l): +44 (0) 1264 34 3075
 Fax: +44 (0) 1264 34 3005
 e-mail:
 (UK): uk.tandf@thomsonpublishingservices.co.uk
 (Int'l): international.tandf@thomsonpublishingservices.co.uk

CRC PRESS
 6000 Broken Sound Parkway, NW, Suite 300
 Boca Raton, FL 33487, USA
 Tel: 1-800-272-7737
 Fax: 1-800-374-3401
From Outside the Continental U.S.
 Tel: 1-561-994-0555
 Fax: 1-561-361-6018
 e-mail: orders@taylorandfrancis.com

CRC PRESS UK
 24-25 Blades Court, Deodar Road
 London SW15 2NU, UK
 Tel: 44 (0) 20 7017 6000
 Fax: 44 (0) 20 7017 6747
 e-mail: enquiries@crcpress.com