Introduction to
Modern Cryptography

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

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

“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

Chapman & Hall/CRC
Taylor & Francis Group

Catalog no. C5513, August 2007, 552 pp.
**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 OBJECTS**

- 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

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

<table>
<thead>
<tr>
<th>Region</th>
<th>Delivery Time</th>
<th>First Title</th>
<th>Additional Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA/Canada</td>
<td>3-5 Days</td>
<td>$5.99</td>
<td>$1.99</td>
</tr>
<tr>
<td>South America</td>
<td>7-14 Days</td>
<td>$6.99</td>
<td>$3.99</td>
</tr>
<tr>
<td>Europe</td>
<td>2-5 Days</td>
<td>$2.99</td>
<td>$0.99</td>
</tr>
<tr>
<td>Rest of World</td>
<td>7-21 Days</td>
<td>$4.99</td>
<td>$2.99</td>
</tr>
</tbody>
</table>

**SHIPPING AND HANDLING**

- Visa  
- MasterCard  
- American Express  
- Check Enclosed $  
- Signature and Telephone Number required on all orders

**ORDERING LOCATIONS**

**In the Americas:**

**CRC PRESS**  
PO Box 400267  
Atlanta, GA 30384-9267  
Tel: 1-800-272-7737  
Fax: 1-800-374-3401

**From Outside the Continental U.S.:**  
Tel: 1-561-984-0555  
Fax: 1-561-361-6018  
e-mail: orders@taylorandfrancis.com

**Rest of the World:**

**CRC PRESS / ITPS**  
Cherton House, North Way  
Andover, Hants, SP10 5BE, UK  
Tel: +44 (0) 1264 34 3006  
Fax: +44 (0) 1264 34 3007  
e-mail: orders@taylorandfrancis.com

**Corporate Offices**

**CRC PRESS**

6000 Broken Sound Parkway, NW, Suite 300  
Boca Raton, FL 33487, USA  
Tel: 1-800-272-7737  
Fax: 1-800-374-3401

**CRC PRESS UK**

24-25 Blades Court, Deodar Road  
London SW15 2NU, UK  
Tel: 44 (0) 20 7017 6700  
Fax: 44 (0) 20 7017 6747  
e-mail: enquiries@crcpress.com

**www.crcpress.com**