C5513 FL

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.

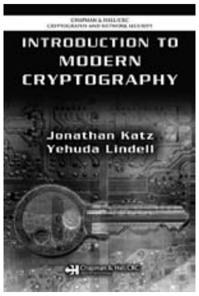
Serving as a textbook, a reference, or for self-study, **Introduction to Modern Cryptography** presents the necessary tools to fully understand this fascinating subject.

> ***"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

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

CONTENTS



See reverse side for continuation of Contents and ordering information

Chapman & Hall/CRC
Taylor & Francis Group

Catalog no. C5513, August 2007, 552 pp.
ISBN: 978-1-58488-551-1, $79.95 / £39.99

Contents continued...

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

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

For priority mail services, please contact your nearest CRC PRESS office.

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

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 3070
Fax: +44 (0) 1264 34 3005
e-mail:
(UK): uk.tandf@thomsonpublishingservices.co.uk
(Int'l): international.tandf@thomsonpublishingservices.co.uk

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
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

www.crcpress.com