MAKE AND BREAK "UNBREAKABLE" CIPHERS

Cryptanalysis of Number Theoretic Ciphers

NEW!

Samuel S. Wagstaff

Purdue University, Center for Education Research in Information Assurance and Security (CERIAS), West Layfayette, Indiana, USA

At the heart of modern cryptographic algorithms lies computational number theory. Whether you're encrypting or decrypting ciphers, a solid background in number theory is essential for success. Written by a number theorist and practicing cryptographer, **Cryptanalysis of Number Theoretic Ciphers** takes you from basic number theory, through the inner workings of ciphers and protocols, to their strengths and weaknesses.

The first part of the book provides the mathematical background needed in cryptography as well as definitions and simple examples from cryptography. It includes summaries of elementary number theory and group theory, as well as common methods of finding or constructing large random primes, factoring large integers, and computing discrete logarithms. Part Two describes a selection of cryptographic algorithms, most of which use number theory. Finally the book presents methods of attack on the cryptographic algorithms and assesses their effectiveness. For each attack method the author lists the systems it applies to and tells how they may be broken with it. If a problem can be avoided, he tells how to avoid it.

Computational number theorists are some of the most successful cryptanalysts against public key systems. **Cryptanalysis of Number Theoretic Ciphers** builds a solid foundation in number theory and shows you how to apply it not only when breaking ciphers, but also when designing ones that are difficult to break.

Catalog no. C1534, December 2002, c.320 pp.
ISBN: 1-58488-153-4, $79.95 / £39.99

Chapman & Hall / CRC
A CRC Company

FEATURES

- Provides a thorough analysis of the modern ciphers that are based on number theory
- Decribes various known ways to break certain ciphers and other cryptosystems — including some private key ciphers, some signatures, and some protocols — and assesses their effectiveness
- Lists and explains each pitfall you may encounter
- Provides numerous examples of ciphers in use today and describes many algorithms in pseudocode for easy programming
- Presents cryptosystems as practical, workable algorithms, not just as oversimplified mathematical objects

CONTENTS

See reverse side for
Other Titles of Interest and ordering information

Cryptanalysis of Number Theoretic Ciphers

Other Titles of Interest

Bestseller!

HANDBOOK OF DISCRETE AND COMBINATORIAL MATHEMATICS

Editor-in-Chief

Ken Rosen

AT&T Laboratories, Middletown, New Jersey

"…a valuable reference tool for professionals and students using discrete mathematics… The coverage is vast…This book is a must-buy for research libraries."

— Journal of Mathematical Psychology, February 2002

"No other book covers such a wide range of topics in discrete mathematics …a useful resource."

— CHOICE

Catalog no. 149, 2000, 1,248 pp.
ISBN: 0-8493-0149-1, $109.95 / £76.99

Bestseller!

AN INTRODUCTION TO CRYPTOGRAPHY

Richard A. Mollin

University of Calgary, Alberta, Canada

"This is a great book! It can be used in many ways: for a university course at one extreme, and as selective light reading for pleasure at the other. The author's enthusiasm carries the reader along clearly and easily, spilling over to scores of fascinating, beautifully written footnotes, which include more than fifty mini-biographies. …excellent and highly recommended."

— Short Book Reviews, Vol. 21, No. 2

"…Mollin has written a readable text on a subject that can be challenging. It deserves your attention."

— The Cryptogram

Catalog no. C1275, August 2000, c. 392 pp.
ISBN: 1-5848-8-1275, $83.95 / £30.99

Bestseller!

CRYPTOGRAPHY

Theory and Practice, Second Edition

Douglas Stinson

University of Waterloo, Ontario, Canada

Major advances over the last five years precipitated this major revision of the bestselling **Cryptography: Theory and Practice**. With more than 40 percent new or updated material, the second edition now provides an even more comprehensive treatment of modern cryptography. It focuses on the new Advanced Encryption Standards (AES) and features an entirely new chapter on that subject. Another new chapter explores the applications of secret sharing schemes, including ramp schemes, visual cryptography, threshold cryptography, and broadcast encryption.

Catalog no. C2069, February 2002, 360 pp.
ISBN: 1-5848-8206-9, $79.95 / £39.99

PLEASE USE THIS ORDER FORM OR THE ORDER CARD IF AVAILABLE

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

CRYPTANALYSIS OF NUMBER THEORETIC CIPHERS
.....Catalog no. C1534, ISBN: 1-58488-153-4 at $79.95 / £39.99 each.

Other titles of interest:

HANDBOOK OF DISCRETE AND COMBINATORIAL MATHEMATICS
.....Catalog no. 149, ISBN: 0-8493-0149-1 at $109.95 / £76.99 each.

AN INTRODUCTION TO CRYPTOGRAPHY
.....Catalog no. C1275, ISBN: 1-5848-8-1275 at $83.95 / £30.99 each.

CRYPTOGRAPHY: THEORY AND PRACTICE, SECOND EDITION
.....Catalog no. C2069, ISBN: 1-5848-8206-9 at $79.95 / £39.99 each.

Name .....
please print clearly

Company/Institution.....

Address.....

.....

City .....State/Province.....Zip/Postal Code.....

Country .....

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. **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, FL, GA, IL, MA, NJ, NY, and Washington, DC. 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
America/Asia/Australia	7-14 Days	$9.99	$3.99
Europe	3-5 Days	£2.99	£0.99
Middle East/Africa	7-21 Days	£4.99	£2.99

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

❑ Visa ❑ MasterCard ❑ American Express ❑ Check Enclosed $ .....

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 North & South America, Asia, and Australasia:

CRC PRESS
2000 N.W. Corporate Blvd.
Boca Raton, FL 33431-9868, 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@crcpress.com

In Europe, Middle East, and Africa:

CRC PRESS / ITPS
Cheriton House, North Way
Andover, Hants, SP10 5BE, UK
Tel: 44 (0) 1264 342932
Fax: 44 (0) 1264 342788
e-mail: crcpress@itps.co.uk

Corporate Offices

CRC PRESS
2000 N.W. Corporate Blvd.
Boca Raton, FL 33431-9868, 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@crcpress.com

CRC PRESS UK
23-25 Blades Court, Deodar Road
London SW15 2NU, UK
Tel: 44 (0) 20 8875 4370
Fax: 44 (0) 20 8871 3443
e-mail: enquiries@crcpress.com

www.crcpress.com

8.30.02bh