



Springer

2nd
edition

2nd ed. 2002, XXII, 435 p.

Printed book

Hardcover

Printed book

Hardcover

ISBN 978-3-540-43072-8

£ 59,99 | CHF 82,50 | 69,99 € |

76,99 € (A) | 74,89 € (D)

Available

Discount group

Standard (0)

Product category

Undergraduate textbook

Other renditions

Softcover

ISBN 978-3-642-07710-4

Computer Science : Theory of Computation

Yan, Song Y.

Number Theory for Computing

- A good introduction to classical and modern number theory and its applications in computer science
- Self-contained source on number theory for computing professionals
- Useful for self-study or as class text and basic reference
- Only prerequisite is high-school math
- First edition released in 2000

Modern cryptography depends heavily on number theory, with primality testing, factoring, discrete logarithms (indices), and elliptic curves being perhaps the most prominent subject areas. Since my own graduate study had emphasized probability theory, statistics, and real analysis, when I started working in cryptography around 1970, I found myself swimming in an unknown, murky sea. I thus know from personal experience how inaccessible number theory can be to the uninitiated. Thank you for your efforts to ease the transition for a new generation of cryptographers. Thank you also for helping Ralph Merkle receive the credit he deserves. Diffie, Rivest, Shamir, Adleman and I had the good luck to get expedited review of our papers, so that they appeared before Merkle's seminal contribution. Your noting his early submission date and referring to what has come to be called "Diffie-Hellman key exchange" as it should, "Diffie-Hellman-Merkle key exchange", is greatly appreciated. It has been gratifying to see how cryptography and number theory have helped each other over the last twenty-five years. :-Jumber theory has been the source of numerous clever ideas for implementing cryptographic systems and protocols while cryptography has been helpful in getting funding for this area which has sometimes been called "the queen of mathematics" because of its seeming lack of real world applications. Little did they know! Stanford, 30 July 2001 Martin E. Hellman Preface to the Second Edition Number theory is an experimental science.

Order online at springer.com/booksellers**Springer Nature Customer Service Center GmbH**

Customer Service

Tiergartenstrasse 15-17

69121 Heidelberg

Germany

T: +49 (0)6221 345-4301

row-booksellers@springernature.com

ISBN 978-3-540-43072-8 / BIC: UY / SPRINGER NATURE: SCI16005

Prices and other details are subject to change without notice. All errors and omissions excepted. Americas: Tax will be added where applicable. Canadian residents please add PST, QST or GST. Please add \$5.00 for shipping one book and \$ 1.00 for each additional book. Outside the US and Canada add \$ 10.00 for first book, \$5.00 for each additional book. If an order cannot be fulfilled within 90 days, payment will be refunded upon request. Prices are payable in US currency or its equivalent.

Part of **SPRINGER NATURE**