



2nd ed. 2002, XXII, 435 p.

Printed book

Hardcover

69,99 € | £59.99 | \$84.99

^[1]74,89 € (D) | 76,99 € (A) | CHF

82,50

Softcover

59,99 € | £54.99 | \$74.99

^[1]64,19 € (D) | 65,99 € (A) | CHF

71,00

eBook

51,16 € | £43.99 | \$59.99

^[2]51,16 € (D) | 51,16 € (A) | CHF

56,50

Available from your library or

springer.com/shop

MyCopy ^[3]

Printed eBook for just

€ | \$ 24.99

springer.com/mycopy

Song Y. Yan

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 / or for the Americas call (toll free) 1-800-SPRINGER / or email us at: customerservice@springernature.com. / For outside the Americas call +49 (0) 6221-345-4301 / or email us at: customerservice@springernature.com.

The first € price and the £ and \$ price are net prices, subject to local VAT. Prices indicated with [1] include VAT for books; the €(D) includes 7% for Germany, the €(A) includes 10% for Austria. Prices indicated with [2] include VAT for electronic products; 19% for Germany, 20% for Austria. All prices exclusive of carriage charges. Prices and other details are subject to change without notice. All errors and omissions excepted. [3] No discount for MyCopy.

