Computer Science: Data Structures and Information Theory

Cryptography Made Simple

- Author is a leading researcher and practitioner in cryptography
- Textbook emphasizes security definitions
- Suitable for undergraduate courses in computer science, mathematics and engineering

In this introductory textbook the author explains the key topics in cryptography. He takes a modern approach, where defining what is meant by "secure" is as important as creating something that achieves that goal, and security definitions are central to the discussion throughout. The author balances a largely non-rigorous style — many proofs are sketched only — with appropriate formality and depth. For example, he uses the terminology of groups and finite fields so that the reader can understand both the latest academic research and "real-world" documents such as application programming interface descriptions and cryptographic standards. The text employs colour to distinguish between public and private information, and all chapters include summaries and suggestions for further reading. This is a suitable textbook for advanced undergraduate and graduate students in computer science, mathematics and engineering, and for self-study by professionals in information security. While the appendix summarizes most of the basic algebra and notation required, it is assumed that the reader has a basic knowledge of discrete mathematics, probability, and elementary calculus.

Order online at springer.com/booksellers
Springer Nature Customer Service Center LLC
233 Spring Street
New York, NY 10013
USA
T: +1-800-SPRINGER NATURE
(777-4643) or 212-460-1500
customerservice@springernature.com

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.