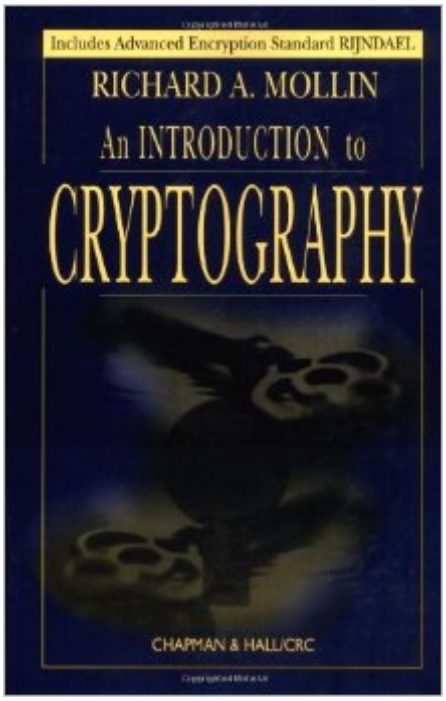
An Introduction To Cryptography (Discrete Mathematics And Its Applications)



Synopsis

INTRODUCTION FOR THE UNINITIATEDHeretofore, there has been no suitable introductory book that provides a solid mathematical treatment of cryptography for students with little or no background in number theory. By presenting the necessary mathematics as needed, An Introduction to Cryptography superbly fills that void. Although it is intended for the undergraduate student needing an introduction to the subject of cryptography, it contains enough optional, advanced material to challenge even the most informed reader, and provides the basis for a second course on the subject. Beginning with an overview of the history of cryptography, the material covers the basics of computer arithmetic and explores complexity issues. The author then presents three comprehensive chapters on symmetric-key cryptosystems, public-key cryptosystems, and primality testing. There is an optional chapter on four factoring methods: Pollard's p-1 method, the continued fraction algorithm, the quadratic sieve, and the number field sieve. Another optional chapter contains detailed development of elliptic curve cryptosystems, zero-knowledge, and quantum cryptography. He illustrates all methods with worked examples and includes a full, but uncluttered description of the numerous cryptographic applications.SUSTAINS INTEREST WITH ENGAGING MATERIALThroughout the book, the author gives a human face to cryptography by including more than 50 biographies of the individuals who helped develop cryptographic concepts. He includes a number of illustrative and motivating examples, as well as optional topics that go beyond the basics presented in the core data. With an extensive index and a list of symbols for easy reference, An Introduction to Cryptography is the essential fundamental text on cryptography.

Book Information

Series: Discrete Mathematics and Its Applications
Hardcover: 392 pages
Publisher: Chapman and Hall/CRC; 1 edition (August 10, 2000)
Language: English
ISBN-10: 1584881275
ISBN-13: 978-1584881278
Product Dimensions: 9.5 x 6.4 x 1.1 inches
Shipping Weight: 1.6 pounds
Average Customer Review: 3.8 out of 5 starsÂ Â See all reviewsÂ (5 customer reviews)
Best Sellers Rank: #2,211,429 in Books (See Top 100 in Books) #32 inÂ Books > Computers & Technology > Programming > Software Design, Testing & Engineering > Coding Theory #414

inÂ Books > Science & Math > Mathematics > Pure Mathematics > Combinatorics #649 inÂ Books > Computers & Technology > Computer Science > Information Theory

Customer Reviews

If you really want to learn cryptology, this is the book.If you just want to know the superficial concept of it, then,this is not the book for you.Mathematics used in this book is very concise and clear.This book also has the complete answers for many exerciseproblems (not just short answer). The answers for exerciseproblems are well written with the full explanations. Well done!! I really enjoy reading this book.

Readers should not be turned away from this book due to the rigorous mathematical content. If one learns the mathematical background (well developed in the text), then understanding of the cryptographic material becomes easier. Readers who only want "plain English' instead of mathematics betray their aversion to mathematics and point to the problem today with trying to teach cryptography. It cannot be effectively done without a rigorous mathematical background. This book does that and much more. Check out the biographical data in the text as well numerous other features.

Only those who fear learning even some moderate math in order to learnthe crypto data will not like this book. The payoff is big time withhistorical bios of people to fill in the background, symmetric-key andpublic-key cryptosystems covered in full, and the facts on primalitytesting and factoring to gear up for the advanced topics which aresuperb. We even get to learn about quantum crypto. This book just makes mewant to learn more about the subject. I'd recommend it to all but thosewho think you can learn crypto without math and who are only interestedin learning how to cryptanalyze algorithms. For them there are manyotherwise useless books out there. This is for those who really want tolearn about crypto and enjoy it in the process!

This is a textbook designed for a one semester undergraduate course in cryptography. This makes it seem a little tamer than what it is. Crypto buffs will enjoy it, and there is little here than is not in some other advanced texts. What is of value is a section on RIJNDAEL, the new advanced encryption standard.Useful as a starting point but not as easy to follow as some other texts. You better like this stuff already or you shouldn't dive into this book.

I had to use this book for cryptography class, and would not recommend it to anyone. The book was very math intensive, which I wouldn't mind if it weren't for the fact that there are no explanations in plain english to follow the math. This book is basically just a bunch of theorems and proofs. Also, there is no cryptanalysis of any of the algorithms included. There are much better books out there, I don't know why anyone would want to get this one.