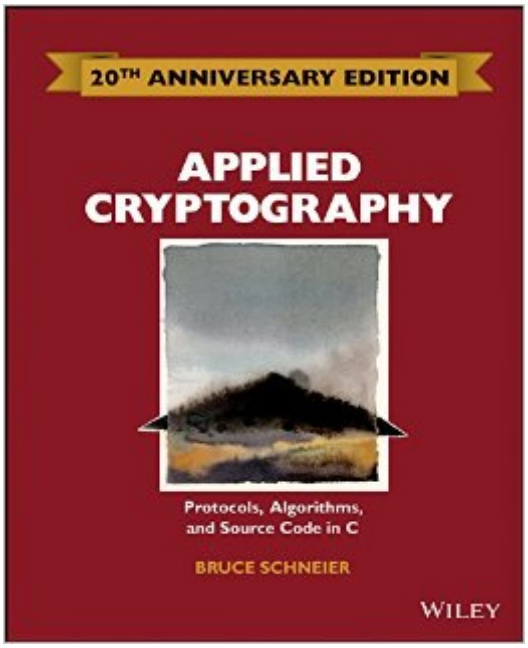
Applied Cryptography: Protocols, Algorithms And Source Code In C



Synopsis

From the world’s most renowned security technologist, Bruce Schneier, this 20th Anniversary Edition is the most definitive reference on cryptography ever published and is the seminal work on cryptography. Cryptographic techniques have applications far beyond the obvious uses of encoding and decoding information. For developers who need to know about capabilities, such as digital signatures, that depend on cryptographic techniques, there’s no better overview than Applied Cryptography, the definitive book on the subject. Bruce Schneier covers general classes of cryptographic protocols and then specific techniques, detailing the inner workings of real-world cryptographic algorithms including the Data Encryption Standard and RSA public-key cryptosystems. The book includes source-code listings and extensive advice on the practical aspects of cryptography implementation, such as the importance of generating truly random numbers and of keeping keys secure. ". . .the best introduction to cryptography I’ve ever seen. . . .The book the National Security Agency wanted never to be published. . . ." -Wired Magazine ". . .monumental . . . fascinating . . . comprehensive . . . the definitive work on cryptography for computer programmers . . ." -Dr. Dobb’s Journal ". . .easily ranks as one of the most authoritative in its field." -PC Magazine The book details how programmers and electronic communications professionals can use cryptography-the technique of enciphering and deciphering messages-to maintain the privacy of computer data. It describes dozens of cryptography algorithms, gives practical advice on how to implement them into cryptographic software, and shows how they can be used to solve security problems. The book shows programmers who design computer applications, networks, and storage systems how they can build security into their software and systems. With a new Introduction by the author, this premium edition will be a keepsake for all those committed to computer and cyber security.

Book Information

Hardcover: 784 pages
Publisher: Wiley; 1 edition (March 30, 2015)
Language: English
ISBN-10: 1119096723
ISBN-13: 978-1119096726
Product Dimensions: 7.8 x 1.6 x 9.6 inches
Shipping Weight: 3.2 pounds (View shipping rates and policies)
Average Customer Review: 4.6 out of 5 starsÂ Â See all reviewsÂ (8 customer reviews)

Best Sellers Rank: #410,904 in Books (See Top 100 in Books) #109 inÂ Books > Computers & Technology > Security & Encryption > Encryption #116 inÂ Books > Computers & Technology > Security & Encryption > Cryptography #5383 inÂ Books > Textbooks > Computer Science

Customer Reviews

Be forewarned, this "updated" edition is not updated. I mistakenly assumed the author would have added coverage of AES, which became the standard after DES was defeated, given the recent (2015) issue date. WRONG. This is just an expensive repackaging of the same old 1996 volume I already had in paperback. If you have the older version already, learn from my mistake. You don’t need this. If, however, you don’t have a copy and you work with cryptography, or need a good reference on older tech, you might want it. It is NOT "current" as the description claims, however; not by any measure. Wanna buy a used paperback version? :-)

If you are interested in, working in, purchasing certifications, or doing anything real in cyber security you must read this book. One of the cornerstones of information security is knowing how cryptography works and how it is applied. Bruce Schneier writes all of his books with the reader in mind. He is technical when he needs to be and practical the rest of the time. Yes, this information isn’t required for any certification and you won’t get any kudos for having this information on your resume, yet this is intended for those of us who are professionals in our jobs.If you have never read any of Mr. Schneier’s work, start with any of his other outstanding books first. This publication is not meant for the causal reader. This book is in-depth, detailed, and built for those who are serious about their profession. Bruce takes extremely complex subjects and breaks them down into digestible chunks for those non-mathematicians such as myself. I missed those physics and quantum mechanics classes in college but Mr. Schneier eases the reader into the wild world of modern day cryptography (with a splash of history).It isn’t a book that you can read just once. This document needs to sit near your desk for ready access. If you work with AES, PKI, SSL, or any other cyber security field that has lots of initials in it, you should consider whether or not you want to continue pretending to know everything or are you ready to start your real education.If you buy this book, you better have a highlighter and a pen to take notes. You will enjoy this materiel, unless you don’t understand it. If you don’t have dog-eared pages, just buy some "Knuckelheads Guide to Security" and call it a day. This book should make you squirm in your seat. It doesn’t have a happy ending but neither does our profession.Buy it, read it, read it again, and use what you have read. Trust me.

I’ve used this book as a resource for teaching and for my own personal learning. Bruce Schneier is an incredible leader in the field, and he is know for his explanations that makes difficult concepts easy to grasp.That said, this book is a bit out of date if you are interested in studying any of the currently used technologies. Also, there is some errata that can confuse people not familiar with the topics already. Finally, some topics contain incomplete discussions.I would love to see an updated version of this book!

I bought this book because, with all the discussion in the news about Apple and IBM and the security of the iphone, I thought it was time I took a deep dive into understanding how this "stuff" actually works. This book has been quite eye-opening.

Protocols Nessus Network Auditing: Jay Beale Open Source Security Series (Jay Beale's Open Source Security) Combinatorial Optimization: Theory and Algorithms (Algorithms and Combinatorics) Geometric Algorithms and Combinatorial Optimization (Algorithms and Combinatorics) Algorithms in C, Parts 1-5 (Bundle): Fundamentals, Data Structures, Sorting, Searching, and Graph Algorithms (3rd Edition) Evolutionary Algorithms in Theory and Practice: Evolution Strategies, Evolutionary Programming, Genetic Algorithms