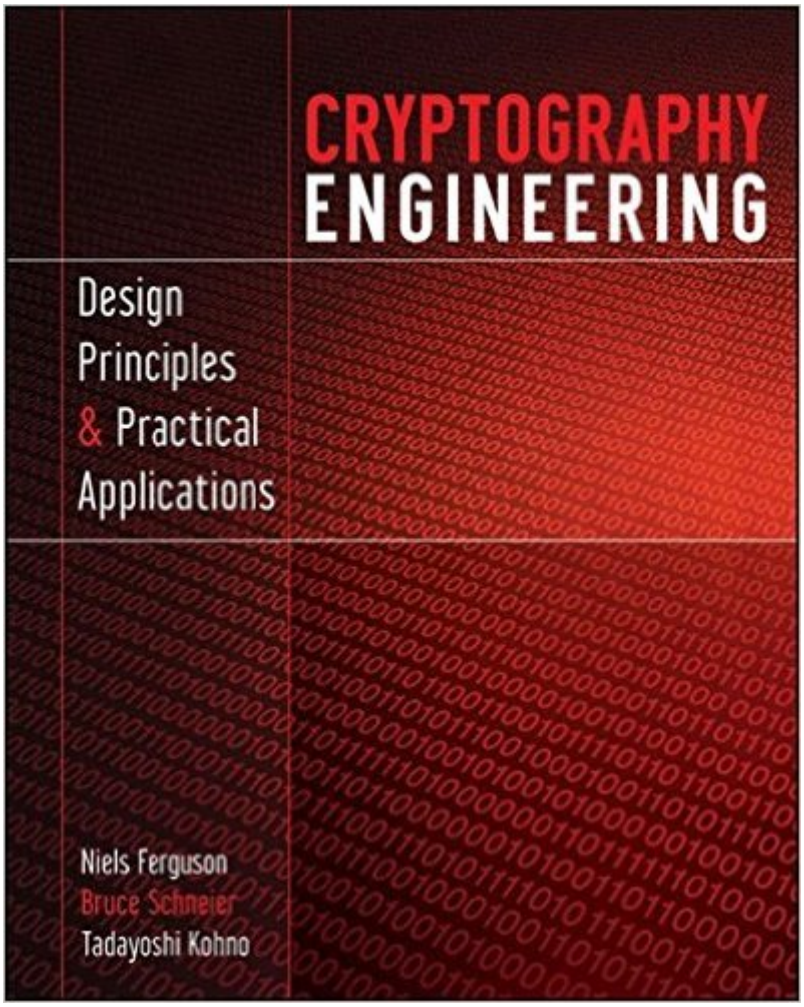
Cryptography Engineering: Design Principles And Practical Applications



Synopsis

The ultimate guide to cryptography, updated from an author team of the world's top cryptography experts. Cryptography is vital to keeping information safe, in an era when the formula to do so becomes more and more challenging. Written by a team of world-renowned cryptography experts, this essential guide is the definitive introduction to all major areas of cryptography: message security, key negotiation, and key management. You'll learn how to think like a cryptographer. You'll discover techniques for building cryptography into products from the start and you'll examine the many technical changes in the field. After a basic overview of cryptography and what it means today, this indispensable resource covers such topics as block ciphers, block modes, hash functions, encryption modes, message authentication codes, implementation issues, negotiation protocols, and more. Helpful examples and hands-on exercises enhance your understanding of the multi-faceted field of cryptography. An author team of internationally recognized cryptography experts updates you on vital topics in the field of cryptography Shows you how to build cryptography into products from the start Examines updates and changes to cryptography Includes coverage on key servers, message security, authentication codes, new standards, block ciphers, message authentication codes, and more Cryptography Engineering gets you up to speed in the ever-evolving field of cryptography.

Book Information

Paperback: 384 pages

Publisher: Wiley; 1 edition (March 15, 2010)

Language: English

ISBN-10: 0470474246

ISBN-13: 978-0470474242

Product Dimensions: 7.4 x 0.8 x 9.3 inches

Shipping Weight: 1.2 pounds (View shipping rates and policies)

Average Customer Review: 4.6 out of 5 starsÂ Â See all reviewsÂ (34 customer reviews)

Best Sellers Rank: #99,368 in Books (See Top 100 in Books) #8 inÂ Books > Engineering & Transportation > Engineering > Design #30 inÂ Books > Computers & Technology > Security & Encryption > Encryption #33 inÂ Books > Computers & Technology > Security & Encryption > Cryptography

Customer Reviews

I just got the book, skimmed over it and compared it with the 1st edition (Practical

Cryptography).First of all, if you don’t have the 1st edition, this is an excellent buy. It’s a "middle ground" book and probably the one you should start with if you are interested in practical cryptography. Then, depending on your interests and needs, you could proceed to a technically and mathematically much deeper (but somewhat obsolete) Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition or to some other direction using the foundation laid down in this book and then getting other book(s) about "hard-core" mathematics of cryptography or about "softer" methods of social engineering and real-life security.I will now assume you know what the book is all about and that you are considering upgrading it so here are some quick things I hope to help you deciding:- first of all, obviously, the errata from the 1st edition is incorporated into the text (there is no errata for the 2nd edition yet but keep checking on the book’s home page [[..

It turns out that cryptography is the least of the issues in cryptographic systems. Good codes are available in good implementations all over the place (one reason the authors warn against implementing your own, since good implementations are very hard). But, as the authors say in their introductory chapter, "Cryptography by itself is fairly useless." They liken strong codes in a weak system to a bank-vault door on a tent. This book provides a first lesson in pouring some concrete into the walls behind that door.Phrased as a text for a one semester graduate or advanced undergrad class, this highly readable text covers a range of basics - the first and most pervasive being the professional paranoia needed to actively seek out ways to defeat your own systems. The authors cover things you might expect in a crypto course, including ciphers, message digests, key exchange, and a smattering of mathematical basics. There’s less of the real crypto material than you might think, however. I mean, what good is the unbreakable code when the bad guy with a root kit can read your passwords from the paging file or /dev/kmem? Instead, this book stands out for things like wiping secrets from memory as fast as you can - if you can, if language design or the physics of computer memory even make it possible. Even things like random numbers and the system clock come under careful scrutiny and analysis of their own. The reader who goes through this book cover to cover comes away with a solid appreciation of the hardware, software, and social issues involved in creating truly secure systems.But, as the authors take pains to state, this is only an introduction. As happened with Schneier’s "Applied Cryptography", it could become "...

Cryptography Engineering: Design Principles and Practical Applications Introduction to Modern Cryptography: Principles and Protocols (Chapman & Hall/CRC Cryptography and Network Security Series) Applied Cryptography: Protocols, Algorithms, and Source Code in C [APPLIED

CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C BY Schneier, Bruce (Author) Nov-01-1995 Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) Cryptography and Network Security: Principles and Practice (7th Edition) Cryptography and Network Security: Principles and Practice Cryptography and Network Security: Principles and Practice (6th Edition) Circuit Engineering & Cryptography & Hacking Circuit Engineering + Cryptography + Raspberry Pi 2 Occupational Ergonomics: Engineering and Administrative Controls (Principles and Applications in Engineering) Ergonomics: Foundational Principles, Applications, and Technologies (Ergonomics Design & Management Theory & Applications) Tissue Engineering: Engineering Principles for the Design of Replacement Organs and Tissues Earthquake Engineering: Damage Assessment and Structural Design (Methods & Applications in Civil Engineering) G.Dieter's Li.Schmidt's Engineering 4th (Fourth) edition(Engineering Design (Engineering Series) [Hardcover])(2008) Radio Frequency Transistors: Principles and practical applications (EDN Series for Design Engineers) Chemical Engineering Design, Second Edition: Principles, Practice and Economics of Plant and Process Design Chemical Engineering Design: Principles, Practice and Economics of Plant and Process Design Microprocessor Design: A Practical Guide from Design Planning to Manufacturing (Professional Engineering) Coding Theory and Cryptography: The Essentials, Second Edition (Chapman & Hall/CRC Pure and Applied Mathematics) Understanding Cryptography: A Textbook for Students and Practitioners