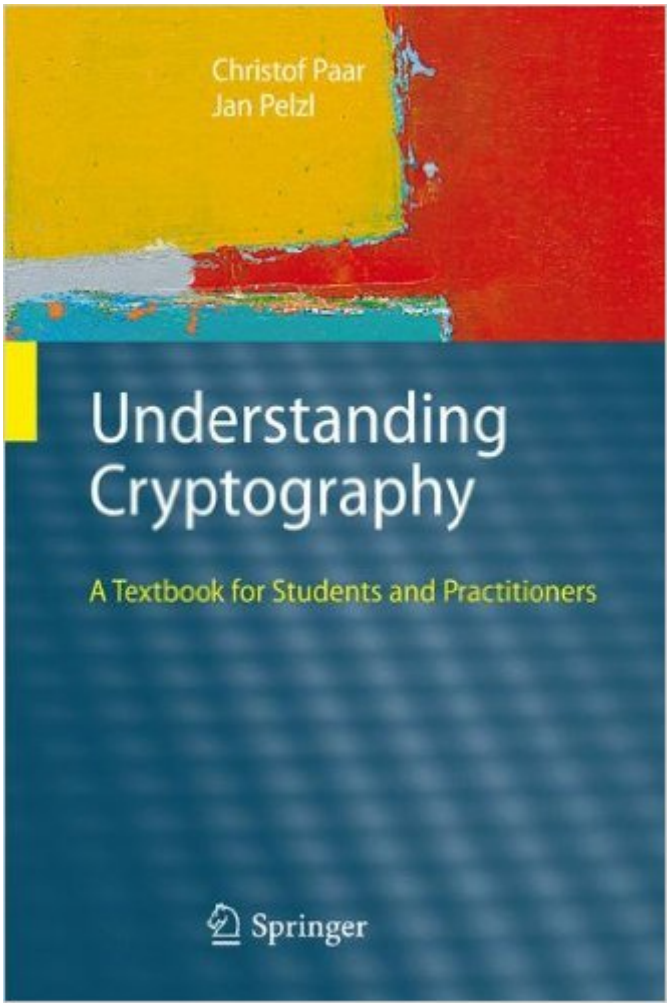
Understanding Cryptography: A Textbook For Students And Practitioners



Synopsis

Cryptography is now ubiquitous â “ moving beyond the traditional environments, such as government communications and banking systems, we see cryptographic techniques realized in Web browsers, e-mail programs, cell phones, manufacturing systems, embedded software, smart buildings, cars, and even medical implants. Today's designers need a comprehensive understanding of applied cryptography. After an introduction to cryptography and data security, the authors explain the main techniques in modern cryptography, with chapters addressing stream ciphers, the Data Encryption Standard (DES) and 3DES, the Advanced Encryption Standard (AES), block ciphers, the RSA cryptosystem, public-key cryptosystems based on the discrete logarithm problem, elliptic-curve cryptography (ECC), digital signatures, hash functions, Message Authentication Codes (MACs), and methods for key establishment, including certificates and public-key infrastructure (PKI). Throughout the book, the authors focus on communicating the essentials and keeping the mathematics to a minimum, and they move quickly from explaining the foundations to describing practical implementations, including recent topics such as lightweight ciphers for RFIDs and mobile devices, and current key-length recommendations. The authors have considerable experience teaching applied cryptography to engineering and computer science students and to professionals, and they make extensive use of examples, problems, and chapter reviews, while the bookâ ™s website offers slides, projects and links to further resources. This is a suitable textbook for graduate and advanced undergraduate courses and also for self-study by engineers.

Book Information

Hardcover: 372 pages

Publisher: Springer; 1st ed. 2010 edition (July 22, 2010)

Language: English

ISBN-10: 3642041000

ISBN-13: 978-3642041006

Product Dimensions: 6.1 x 0.9 x 9.2 inches

Shipping Weight: 1.4 pounds (View shipping rates and policies)

Average Customer Review: 4.6 out of 5 starsÂ Â See all reviewsÂ (57 customer reviews)

Best Sellers Rank: #94,833 in Books (See Top 100 in Books) #14 inÂ Books > Engineering & Transportation > Engineering > Industrial, Manufacturing & Operational Systems > Industrial Design > Products #15 inÂ Books > Computers & Technology > Programming > Software Design, Testing

& Engineering > Structured Design #19 inÂ Books > Engineering & Transportation > Engineering > Electrical & Electronics > Circuits > Design

Customer Reviews

It is a summer tradition for me to pick a technical topic, find a textbook that represents the subject from an introductory point of view, and self-study as much of it as I can. This summer, I picked cryptography. After searching all over the place for a decent introductory book on the subject, I stumbled upon this one. Even though it only had 2 reviews at the time, I could tell that it was exactly what I was looking for. After reading the first 6 chapters of this book, all I can say is this: WOW!Cryptography lies at the intersection of mathematics, computer science, and electrical engineering. This book borrows ideas from all 3 fields in order to describe the core ideas of cryptography in a surprisingly elegant way. The tone of the book is formal enough so that the book isn't disorganized or overly verbose, but not too formal that it makes the readings a chore.As stated above, the content of the book is highly organized. The first 5 chapters deal with symmetric algorithms, and the next 5 or so deal with asymmetric algorithms. The last few chapters deal with hash functions and message authentication algorithms. In between highly-technical sections, you will find informal topics that are concerned with general security topics, history, or similar subjects. These sections are a wonderful break from the technical ones, and make this highly technical book read somewhat like a novel.The figures in this book are wonderful, and really help the reader understand the encryption algorithms more fully. For example, the DES algorithm is somewhat convoluted, but the figures in the chapter make it very simple to see exactly what is happening at each stage of the process. Every permutation, bit slicing operation, and XOR operation is clearly evident from the flow diagrams.

If you've heard people mention things like ECC, HMACs, discrete logarithms and wanted to what they were talking about; or if you wanted to understand who RSA and AES really work along with many other things, then this is the book for you.I had been hunting for something more current than the 1996 Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition when I came across Understanding Cryptography. I could tell from the available samples and the table of contents, that it should meet my needs. It has not only met my needs, but has exceeded them in every respect.This book was absolutely perfect for me, so it would be of some use for you to know my background.I've long had an interest in cryptography but never any training. When I read Martin Gardener's famous 1977 article on RSA I thought it was the coolest thing ever, but I didn't fully

grasp it and didn’t pursue it at the time. In college I studied some math, but my degree is in linguistics, not in math or computing. I have read popularizations of cryptography, and had tried to make it though Applied Cryptography when it first came out in 1996, but I can’t say that I really understood how the algorithms and the more intricate protocols worked. So that is roughly my background.One of the great things about Understanding Cryptography is that it taught me exactly the math that I needed. You need to be comfortable learning new math. (I also found that I had to brush up on basic linear algebra on my own to understand one component of the deals of AES).

(My background is in mathematics only.) In general, the book is very well written and understandable and covers, insofar as I understand it, all the major areas of cryptography (but virtually no cryptanalysis). Were it not for the following, I would give the book five stars.I am puzzled that no one else has mentioned that this book is RIFE with errors. This speaks badly not only for the authors, but also for the publisher. I list a selection of errors, generally putting the most important first. Mathematical typos, which can be difficult to detect by the student, are included if I found them. Other typos are not.p 280. The code is AWFUL. The FOR variable is explicitly initialized and incremented within the loop. Line 2.3 shows arithmetic to the left of the assignment statement. If the authors insist on using = for assignment in 2.3 instead of the more readable arrow, they do NOT want the triple = sign. The number 4096 really should be explained somewhere.p190-191. The explanation of Miller Rabin is impossible to understand as written and the code is incorrect (Input 17 and 4 to see that 17 turns out to be composite). Need to add code to leave loop when z = p-1. Language MUST be included somewhere that the code basically does the Fermat check and the check that x^2=1 has only two solutions in a field (i.e. when variable is prime). It should also be mentioned that we are doing no more than exponentiating in the usual squaring and multiplying fashion.p209 C is NOT, as claimed, a group under complex multiplication; perhaps C â “ was intended.p16 The box is headed as the definition of ring. It is not. It is the definition of Z-m. Oddly, commutativity is not mentioned as a property on the next page.

Interactive Approach: Manual and CD-ROM (Royer, Pain Control for Dental Practitioners) Anatomy of Hatha Yoga: A Manual for Students, Teachers, and Practitioners Tropical Diseases: A Practical Guide for Medical Practitioners and Students Understanding Bergson, Understanding Modernism (Understanding Philosophy, Understanding Modernism) 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) Coding Theory and Cryptography: The Essentials, Second Edition (Chapman & Hall/CRC Pure and Applied Mathematics) Cryptography and Coding: 6th IMA International Conference, Cirencester, UK, December 17-19, 1997, Proceedings (Lecture Notes in Computer Science) Cryptography Engineering: Design Principles and Practical Applications Applied Cryptography: Protocols, Algorithms and Source Code in C Introduction to Cryptography with Coding Theory (2nd Edition) Cryptography InfoSec Pro Guide (Beginner's Guide) Circuit Engineering & Cryptography & Hacking Cryptography For Dummies Circuit Engineering + Cryptography + Raspberry Pi 2