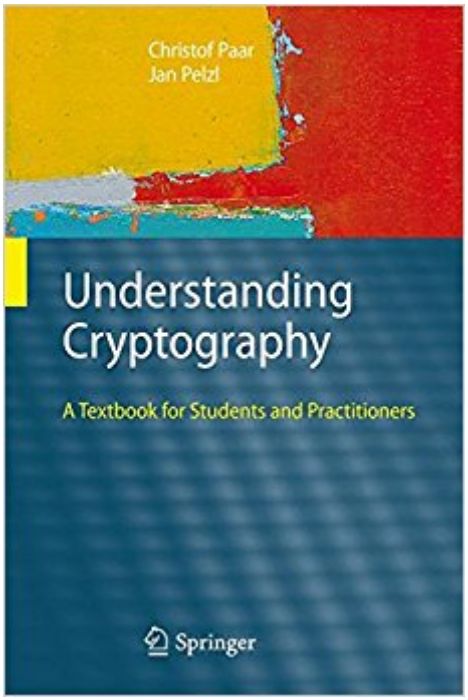
Understanding Cryptography: A Textbook For Students And Practitioners



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 stars 62 customer reviews

Best Sellers Rank: #27,861 in Books (See Top 100 in Books) #5 inÂ Books > Computers & Technology > Programming > Software Design, Testing & Engineering > Structured Design #6 inÂ Books > Engineering & Transportation > Engineering > Industrial, Manufacturing & Operational

Systems > Industrial Design > Products #7 inÂ Books > Engineering & Transportation > Engineering > Electrical & Electronics > Circuits > Design

Customer Reviews

requires security." (John Canessa)â œThe book presents a panoramic of modern Cryptography with a view to practical applications. â | The book is well written, many examples and figures through it illustrate the theory and the bookâ ™s website offers links and supplementary information. The book also discusses the implementation in software and hardware of the main algorithms described.â • (Juan Tena Ayuso, Zentralblatt MATH, Vol. 1190, 2010)

Prof. Dr.-Ing. Christof Paar has the Chair for Embedded Security at the University of Bochum, Germany, and is Adjunct Professor at the University of Massachusetts at Amherst, USA. Prof. Paar has taught cryptography for 15 years to engineering and computer science students in the US and in Europe, and he has taught many industrial practitioners at organizations such as Motorola, Philips and NASA. He has more than 100 publications in applied cryptography and is a cofounder ofÂ the Workshop on Cryptographic Hardware and Embedded Systems (CHES), the key academic event in this field.Prof. Dr.-Ing. January Pelzl started his career at Bosch Telecom GmbH. He has a Ph.D. in applied cryptography, and as a researcher he investigated the practical aspects of elliptic-curve-based cryptography and cryptanalysis. He has published extensively about his theoretical and industrial work through leading international conferences and journals, and he has taught many IT security and cryptography courses in industry. He was the Managing Director of "ESCRYPT GmbH" in Bochum. Since January 2015 he is the professor of Â "Computer Security" in Hochschule Hamm-Lippstadt.The authors' website (http://www.crypto-textbook.com/) provides extensive notes, slides, video lectures; the authors' YouTube channel (https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg) includes video lectures.

There are dozens of hours of youtube lectures of Christof Paar lecturing in his class in Germany (in English) which I found extraordinarily helpful in really getting into the nitty gritty of Cryptography which I needed on product development. Picking up Cryptography in bits and pieces from reading articles and watching short videos really doesn't give you a proper overview if you are planning on designing a system using cryptography as there are so many choices and it'snot easy to understand places and situations that may be right for one or the other.Christof's classes are excellent, I bought the book to use as a reference while going through the online courses but you probably wouldn't

need it.I do feel that people like Christof should be rewarded for making serious donations of a life long study and in their ability to crystallize the teachings and then put it up on something like youtube FREE. So be nice and give back.. buy the book, you will find it useful in it’s own right.

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 1996Â Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second EditionÂ 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).Working though this book on my own through self study took time. It is extremely well presented (with the possible exception of the final chapter, which could do with another round of copy-editing). The subject matter is not simple, so if you really wish to understand them you need to go through things very slowly, stopping frequently to check understanding, but everything you need is in the book without it being overly long. The excellent organization and presentation of the material means that I was able to get far, far more out of this book than anything else I have read on the topic.The problem sets at the end of each chapter progress from easy to more challenging. I still need to go back and take on some of the more challenging ones I skipped the first time through. Often I was too eager to get to the new chapter than to work through the problems. As a consequence I missed some of the extended material that was presented through those problems sets.Personally, my second favorite chapter is the chapter on AES which really steps through how it works and why each component does what it does. My favorite is the chapter on ECC. I had known wat ECC was used for, but before reading this, I had no idea of what it really was. Now I find it "the

coolest thing ever". (OK, I may over use that phrase.) The authors' presentation of it is just right. They lead you though the process so that you can share in the delight of how ECC works.Although I have worked though this as complete self-study, I would have preferred to do this as part of a class or at least some study group. Sometimes because I could have more quickly gotten through things that I held me up a few times, but mostly because I would have liked to share the experience. My wife and daughter are not entirely happy with the fact that I've been trying to teach them bits of what I've been learning over the month.There are still bits that I don't fully understand. Some are questions not addressed in the book, but the further readings and bibliography are excellent. So I have the resources to investigate those. There are also bits that I don't fully understand because I haven't gone back and worked through the relevant exercises in the problem sets.What I would like to see in a second addition:(1) A bibliography for each chapter as well as the comprehensive one at the end(2) A reworking of the final chapter, which appears rushed and not as well presented as everything else(3) More on hash functions reflecting what is being learned now as part of the SHA3 process.I am sure that this makes an outstanding textbook for a college course in the matter, but I want to add that it is so clearly presented, organized with introductions to the necessary math that it works for self-study as well.

I was searching for information on AES encryption algorithms and came across this book online; yes, online. The critical information was published and readily available for the reader, made available by the author for free.I honor those who are willing to open their hands and to share their wealth of knowledge with others without demanding anything in return. You can learn a good amount of information from this book for free, which is why you should honor these authors and purchase this book!I do not regret purchasing this book. The information is presented in a very readable format, and is helpful for those looking for a great introduction to the subject of cryptography.

Started an online course in this subject, but I found the course and other presentations fragmented and incoherent. My interest in Cryptography was rom earlier days, before number theory and calculus notation were a part of it.Cristof's videos and this book provided a coherent and clear presentation of this subject, allowing me to continue my expansion of knowledge in cryptography,

Great book! The topics in this book are intellectually stimulating and cover modern cryptosystems. The reason I do not give it a 5 is because there are many uncaught text errors/inconsistencies in the

chapters/examples. However, it is always deducible what the intention of the author is. The PDF version of this book contains much fewer errors.

Great book for those whos passion is cryptography. I've spent whole weekend reading it. All complicated explanations are clear thankfully to Christof Paar.

I work in information security and have a math background. This book is great! It really walks the dog but has gotten as complicated as I have needed to design implementations in python. I've recommended it to several friends.

I am reading this book and watching the YouTube videos of the classroom lectures. The book is very well written and is a great resource to understand cryptography with the addition of some general security concepts. Combining the book with the lectures gives you all of the benefit of a college class without the pressures of testing, etc.

Espionage (Cryptography: Code Making and Code Breaking) Uncracked Codes and Ciphers (Cryptography: Code Making and Code Breaking) Cryptography and Network Security: Principles and Practice (7th Edition) A Course in Number Theory and Cryptography (Graduate Texts in Mathematics)