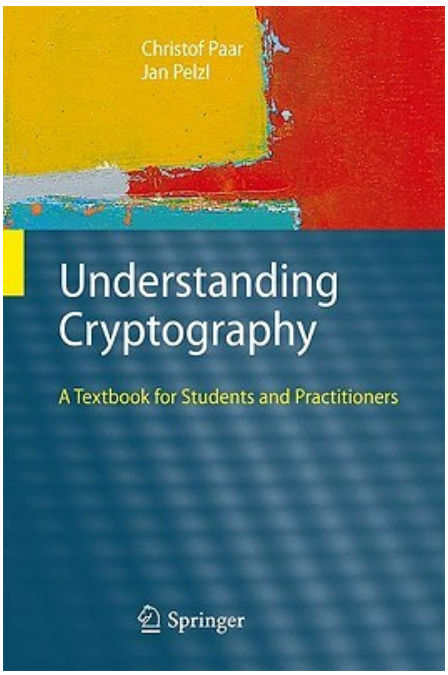

Understanding Cryptography: A Textbook For Students And Practitioners

Christof Paar , Jan Pelzl

Understanding Cryptography: A Textbook For Students And Practitioners

Christof Paar , Jan Pelzl

Understanding Cryptography: A Textbook For Students And Practitioners Christof Paar , Jan Pelzl Cryptography is now ubiquitous - 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 book'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.

Understanding Cryptography: A Textbook For Students And Practitioners Details

Date	:	Published October 19th 2011 by Springer (first published December 10th 2009)
ISBN	:	9783642041006
Author	:	Christof Paar , Jan Pelzl
Format	:	Hardcover 372 pages
Genre	:	Computer Science, Programming, Science, Mathematics

Practitioners Christof Paar , Jan Pelzl

From Reader Review Understanding Cryptography: A Textbook For Students And Practitioners for online ebook

Ro Drop says

Good book. Watched videos of his class too. Videos definitely helped with understanding the math and processes. His lectures are on youtube.

Murray says

The only book on the subject I actually read, from cover to cover. Parts of it were tough sledding, especially the stuff about Galois Fields (aka Finite Fields). Galois was an interesting, but profoundly tragic guy. He certainly didn't live long. His work didn't gain prominence or recognition til the 20th century. There is a book on his life, but I already know how it ends. There it was... the familiar twang of irony.

Kamal says

It's a awesome book for learning cryptography I highly recommend this book to everyone that wants to start learning cryptography and L also recommend to watch prof. Christof Paar's course in youtube based on this book.

Michael says

I used this as a companion to the author's 2-semester lecture series, which is freely available on YouTube or on the book's own website: http://www.crypto-textbook.com. I found it very useful for brushing up on some topics in some more detail after watching the lectures. In general this is a very practical introduction to the topic of cryptography that doesn't shy away from the maths but also does not require any prior knowledge of any of the advanced mathematical topics.

Ro Givens says

This book was a good foundation for my cryptography class, although a few points about ciphers used are now a bit out of date. Some of the math is a little advanced for undergraduate computer science students, but general ideas can be gleaned about ciphers requiring Galois theory or elliptic curves, for instance, without formally covering those topics. Overall I enjoyed reading and using this book for my class.

Scott Johnson says

This was a mistake on my part. I eventually just skimmed a lot of this for the principles and overall concepts, as this isn't a topic to study any more in depth than that without the ability to actually take notes, do the math, and work out the problems.

That said, it seems thorough and well-written. I think the expectations of mathematical prerequisites could be more detailed, as there is a great deal of number theory and the author mentions you really just need calculus.

Maybe my cursory reading glossed over it, but I was also hoping for more discussion of the information entropy relating to these systems. But I guess that's more of a theoretical discussion and this was largely aimed at practice instead.

Amelia Treader says

A book from my alternative reality (i.e. what I do to eat) has sneaked in. One of the better expositions, though not quite as broad-based as it could be. Thorough, correct and comprehensible. It's hard to expect much more from a book.

Areej M. says

you can watch a lecture of Prof. paar based on this book on you tube : introduction to cryptography (24 lecture / 1.30 h)

Marco says

Interesting introduction, with a good balance between mathematical aspects and practical protocols.

Aventinus says

Εξαιρετικ? γραμμ?νο.

Αρκετ? απ? τα κεφ?λαια τα γν?ριζα ?δη, για αυτ? η αν?γνωσ? μου ?ταν επιλεκτικ? και κυρ?ως αφορο?σε τα σημε?α που ?θελα φρεσκ?ρω. Παρ?λα αυτ? δεν δυσκολε?ομαι να πω πως το βιβλ?ο ?χει καταπληκτικ? δομ?, απλ? γλ?σσα και αποφε?γει τα πολλ? μαθηματικ?, ?πως ακριβ?ς θα ?πρεπε να ε?ναι ?να εισαγωγικ? βιβλ?ο κρυπτογραφ?ας.

Σ?γουρα θα το επισκεπτ? ξαν? ?ταν χρειαστε? να θυμηθ? κ?ποιο συγκεκριμ?νο κεφ?λαιο και το προτε?νω ανεπιφ?λακτα σε ?ποιον ξεκιν?ει την ενασχ?ληση του με την κρυπτογραφ?α.

Απ? ?σα βιβλ?α κρυπτογραφ?ας ?χω πι?σει στα χ?ρια μου, το Understanding Cryptography: Textbook for Students and Practitioners ε?ναι με διαφορ? το πιο φιλικ? και ευαν?γνωστο.