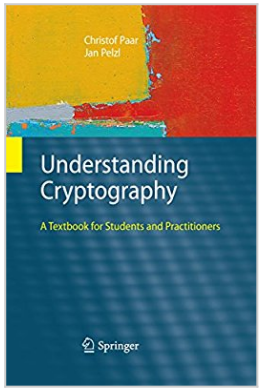

Understanding Cryptography: A Textbook for Students and Practitioners

By Christof Paar, Jan Pelzl

Understanding Cryptography: A Textbook for Students and Practitioners
By 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

By Christof Paar, Jan Pelzl

Understanding Cryptography: A Textbook for Students and Practitioners By 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 By Christof Paar, Jan Pelzl Bibliography

- Rank: #177390 in eBooks
- Published on: 2009-11-27
- Released on: 2009-11-27
- Format: Kindle eBook

Editorial Review

Review

From the reviews:

"The authors have succeeded in creating a highly valuable introduction to the subject of applied cryptography. I hope that it can serve as a guide for practitioners to build more secure systems based on cryptography, and as a stepping stone for future researchers to explore the exciting world of cryptography and its applications." (Bart Preneel, K.U.Leuven)

"The material is very well presented so it is clear to understand. The necessary amount of mathematics is used and complete yet simple examples are used by the authors to help the reader understand the topics. ... [The authors] appear to fully understand the concepts and follow a very good pedagogical process that helps the reader not only understand the different topics but motivate you to perform some of the exercises at the end of each chapter and browse some of the reference materials. I fully recommend this book to any software developer/designer working or considering working on a project that requires security." (John Canessa)

“The book presents a panoramic of modern Cryptography with a view to practical applications. … The book is well written, many examples and figures through it illustrate the theory and the book’s website offers links and supplementary information. The book also discusses the implementation in software and hardware of the main algorithms described.” (Juan Tena Ayuso, Zentralblatt MATH, Vol. 1190, 2010)

About the Author

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 of 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 "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/UC1usFRN4LCMcflV7UjHNuQg) includes video lectures.

Users Review

From reader reviews:

Charles English:

Now a day people who Living in the era where everything reachable by connect with the internet and the resources inside can be true or not call for people to be aware of each data they get. How people have to be smart in receiving any information nowadays? Of course the correct answer is reading a book. Looking at a book can help persons out of this uncertainty Information specifically this Understanding Cryptography: A Textbook for Students and Practitioners book as this book offers you rich facts and knowledge. Of course the details in this book hundred % guarantees there is no doubt in it you may already know.

Kayla Wilson:

This Understanding Cryptography: A Textbook for Students and Practitioners are usually reliable for you who want to certainly be a successful person, why. The explanation of this Understanding Cryptography: A Textbook for Students and Practitioners can be among the great books you must have will be giving you more than just simple examining food but feed an individual with information that possibly will shock your prior knowledge. This book is handy, you can bring it just about everywhere and whenever your conditions at e-book and printed ones. Beside that this Understanding Cryptography: A Textbook for Students and Practitioners giving you an enormous of experience for instance rich vocabulary, giving you trial of critical thinking that we realize it useful in your day task. So , let's have it appreciate reading.

Mary Haskell:

This Understanding Cryptography: A Textbook for Students and Practitioners is fresh way for you who has interest to look for some information given it relief your hunger associated with. Getting deeper you onto it getting knowledge more you know otherwise you who still having small amount of digest in reading this Understanding Cryptography: A Textbook for Students and Practitioners can be the light food for you because the information inside this particular book is easy to get through anyone. These books build itself in the form that is certainly reachable by anyone, that's why I mean in the e-book application form. People who think that in book form make them feel sleepy even dizzy this book is the answer. So there isn't any in reading a e-book especially this one. You can find actually looking for. It should be here for an individual. So , don't miss this! Just read this e-book variety for your better life in addition to knowledge.

Edward Suniga:

A lot of e-book has printed but it is different. You can get it by net on social media. You can choose the most effective book for you, science, witty, novel, or whatever by simply searching from it. It is known as of book Understanding Cryptography: A Textbook for Students and Practitioners. Contain your knowledge by it. Without leaving behind the printed book, it could add your knowledge and make an individual happier to read. It is most crucial that, you must aware about book. It can bring you from one destination to other place.

Read Understanding Cryptography: A Textbook for Students and Practitioners By Christof Paar, Jan Pelzl for online ebook

Understanding Cryptography: A Textbook for Students and Practitioners By Christof Paar, Jan Pelzl Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Understanding Cryptography: A Textbook for Students and Practitioners By Christof Paar, Jan Pelzl books to read online.

Online Understanding Cryptography: A Textbook for Students and Practitioners By Christof Paar, Jan Pelzl ebook PDF download

Understanding Cryptography: A Textbook for Students and Practitioners By Christof Paar, Jan Pelzl Doc

Understanding Cryptography: A Textbook for Students and Practitioners By Christof Paar, Jan Pelzl Mobipocket

Understanding Cryptography: A Textbook for Students and Practitioners By Christof Paar, Jan Pelzl EPub