

[DOWNLOAD](#)

Understanding Cryptography

By Christof Paar

Springer Berlin Heidelberg Nov 2014, 2014. Taschenbuch. Condition: Neu. Neuware - 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...



[READ ONLINE](#)
[3.29 MB]

Reviews

A whole new electronic book with a new point of view. It can be full of knowledge and wisdom Its been written in an exceedingly simple way which is only following i finished reading through this pdf in which really modified me, modify the way in my opinion.

-- Arianna Nikolaus

This ebook is wonderful. I have got go through and so i am certain that i am going to likely to read through once again again later on. You will like the way the article writer compose this ebook.

-- Miss Ariane Mraz

Other Books



Simultaneous Removal of Iron, Arsenic and Fluoride

LAP Lambert Academic Publishing Okt 2016, 2016. Taschenbuch. Condition: Neu. Neuware - Groundwater is the major source of domestic water for people living in rural and semi-urban area of Assam - a northeastern hilly province of India. However, it contains excessive amounts...



How to Solve Mathematical Problems (Paperback)

Dover Publications Inc., United States, 1995. Paperback. Condition: New. New edition. Language: English. Brand new Book. If you've ever tried to solve mathematical problems without any idea how to go about it, this book is for you. It will improve your ability...



HBR Guide to Getting the Right Work Done

Ingram Publisher Services Feb 2013, 2013. Taschenbuch. Condition: Neu. Neuware - IS YOUR WORKLOAD SLOWING YOU-AND YOUR CAREER-DOWN Your inbox is overflowing. You're paralyzed because you have too much to do but don't know where to start. Your to-do list never seems...



Managing Technical Debt: Reducing Friction in Software Development, 1/e (Paperback)

Pearson Education (US), United States, 2019. Paperback. Condition: New. Language: English. Brand new Book. "This is an incredibly wise and useful book. The authors have considerable real-world experience in delivering quality systems that matter, and their expertise shines through in these pages...."



Arsenic Removal Technologies from ground water

LAP Lambert Academic Publishing Jan 2013, 2013. Taschenbuch. Condition: Neu. Neuware - Ground water is one of the main sources of drinking water especially in rural areas of India. Groundwater is generally regarded as safe to drink. At the same time ground water...



Game Theory : A Very Short Introduction

Oxford University Press Nov 2007, 2007. Taschenbuch. Condition: Neu. Neuware - Games are everywhere: Drivers manoeuvring in heavy traffic are playing a driving game. Bargain hunters bidding on eBay are playing an auctioning game. A firm negotiating next year's wage is playing...