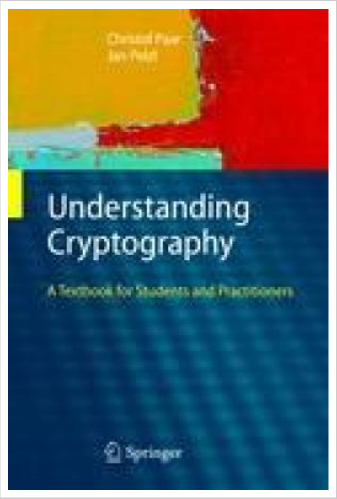
Christof Paar
Jan Pelzl
Understanding Cryptography
A Textbook for Students and Practitioners
Springer

Understanding Cryptography : A Textbook for Students and Practitioners

By Christof Paar

Springer Berlin Heidelberg Okt 2011, 2011. Buch. 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
[5.93 MB]

Reviews

It in a single of my personal favorite ebook. Better then never, though i am quite late in start reading this one. I am effortlessly will get a satisfaction of reading a published ebook.

-- ***Ms. Lavada Krajcik***

Comprehensive guideline for book lovers. It can be filled with knowledge and wisdom I realized this publication from my dad and i suggested this pdf to find out.

-- ***Ted Schumm***