

[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](#)
[6.01 MB]

Reviews

This created ebook is great. it was writtern very properly and useful. Its been printed in an exceedingly easy way in fact it is just right after i finished reading this pdf where basically modified me, alter the way i think.

-- **Aglae Becker**

This ebook is definitely worth buying. It is definitely basic but excitement within the fifty percent in the ebook. Its been designed in an extremely straightforward way which is merely following i finished reading this ebook where basically changed me, alter the way in my opinion.

-- **Ward Morar**