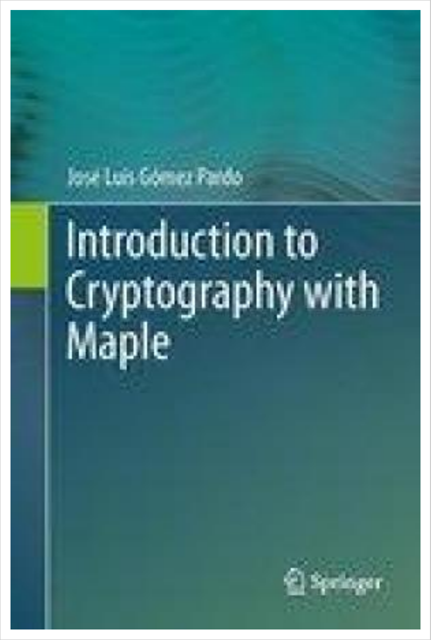

Introduction to Cryptography with Maple

By José Luis Gómez Pardo

Springer Dez 2012, 2012. Buch. Book Condition: Neu. 23.5x15.5x cm. This item is printed on demand - Print on Demand Neuware - This introduction to cryptography employs a programming-oriented approach to study the most important cryptographic schemes in current use and the main cryptanalytic attacks against them. Discussion of the theoretical aspects, emphasizing precise security definitions based on methodological tools such as complexity and randomness, and of the mathematical aspects, with emphasis on number-theoretic algorithms and their applications to cryptography and cryptanalysis, is integrated with the programming approach, thus providing implementations of the algorithms and schemes as well as examples of realistic size. A distinctive feature of the author's approach is the use of Maple as a programming environment in which not just the cryptographic primitives but also the most important cryptographic schemes are implemented following the recommendations of standards bodies such as NIST, with many of the known cryptanalytic attacks implemented as well. The purpose of the Maple implementations is to let the reader experiment and learn, and for this reason the author includes numerous examples. The book discusses important recent subjects such as homomorphic encryption, identity-based cryptography and elliptic curve cryptography. The algorithms and schemes which are treated...

Reviews

It in a single of my personal favorite publication. It usually fails to charge an excessive amount of. Once you begin to read the book, it is extremely difficult to leave it before concluding.

-- Mr. David Friesen IV

This is the greatest book i have got read through till now. I could possibly comprehended almost everything out of this published e book. Your daily life span will probably be enhance the instant you total looking at this book.

-- Bernadette Baumbach