



Introduction to Cryptography with Maple (Paperback)

By José Luis Gomez-Pardo

Springer-Verlag Berlin and Heidelberg GmbH Co. KG, Germany, 2015. Paperback. Book Condition: New. 2013 ed.. 235 x 155 mm. Language: English . Brand New Book ***** Print on Demand *****.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...



READ ONLINE
[9.39 MB]

Reviews

This type of book is everything and taught me to hunting ahead of time and more. It is actually rally interesting throgh looking at time period. You can expect to like just how the article writer write this publication.

-- **Murphy Price**

Definitely one of the best ebook We have possibly go through. It usually does not charge a lot of. I am just pleased to inform you that this is actually the greatest ebook i have got study in my own lifestyle and may be he greatest publication for actually.

-- **Ms. Patsy D'Amore III**