# Introduction to Cryptography with Maple

*José Luis Gómez Pardo*

# Introduction to Cryptography with Maple

*José Luis Gómez Pardo*

**Introduction to Cryptography with Maple** José Luis Gómez Pardo

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 in detail and implemented in Maple include AES and modes of operation, CMAC, GCM/GMAC, SHA-256, HMAC, RSA, Rabin, Elgamal, Paillier, Cocks IBE, DSA and ECDSA. In addition, some recently introduced schemes enjoying strong security properties, such as RSA-OAEP, Rabin-SAEP, Cramer--Shoup, and PSS, are also discussed and implemented. On the cryptanalysis side, Maple implementations and examples are used to discuss many important algorithms, including birthday and man-in-the-middle attacks, integer factorization algorithms such as Pollard's rho and the quadratic sieve, and discrete log algorithms such as baby-step giant-step, Pollard's rho, Pohlig--Hellman and the index calculus method.

This textbook is suitable for advanced undergraduate and graduate students of computer science, engineering and mathematics, satisfying the requirements of various types of courses: a basic introductory course; a theoretically oriented course whose focus is on the precise definition of security concepts and on cryptographic schemes with reductionist security proofs; a practice-oriented course requiring little mathematical background and with an emphasis on applications; or a mathematically advanced course addressed to students with a stronger mathematical background. The main prerequisite is a basic knowledge of linear algebra and elementary calculus, and while some knowledge of probability and abstract algebra would be helpful, it is not essential because the book includes the necessary background from these subjects and, furthermore, explores the number-theoretic material in detail. The book is also a comprehensive reference and is suitable for self-study by practitioners and programmers.

**From reader reviews:**

**Dan Flood:**

The book Introduction to Cryptography with Maple make one feel enjoy for your spare time. You can use to make your capable more increase. Book can being your best friend when you getting stress or having big problem with the subject. If you can make looking at a book Introduction to Cryptography with Maple to get your habit, you can get much more advantages, like add your own capable, increase your knowledge about a number of or all subjects. You are able to know everything if you like available and read a e-book Introduction to Cryptography with Maple. Kinds of book are a lot of. It means that, science reserve or encyclopedia or others. So , how do you think about this reserve?

**Renee Chagnon:**

Book is to be different for every single grade. Book for children until eventually adult are different content. As it is known to us that book is very important normally. The book Introduction to Cryptography with Maple seemed to be making you to know about other knowledge and of course you can take more information. It is very advantages for you. The e-book Introduction to Cryptography with Maple is not only giving you far more new information but also to become your friend when you sense bored. You can spend your spend time to read your book. Try to make relationship with all the book Introduction to Cryptography with Maple. You never experience lose out for everything should you read some books.

**Robert Lyman:**

Reading a book to get new life style in this yr; every people loves to study a book. When you read a book you can get a great deal of benefit. When you read guides, you can improve your knowledge, simply because book has a lot of information on it. The information that you will get depend on what kinds of book that you have read. If you wish to get information about your analysis, you can read education books, but if you want to entertain yourself look for a fiction books, this kind of us novel, comics, and soon. The Introduction to Cryptography with Maple provide you with a new experience in studying a book.

**Betty Peoples:**

As a student exactly feel bored to reading. If their teacher inquired them to go to the library or make summary for some reserve, they are complained. Just small students that has reading's heart or real their passion. They just do what the educator want, like asked to go to the library. They go to right now there but nothing reading really. Any students feel that studying is not important, boring as well as can't see colorful images on there. Yeah, it is for being complicated. Book is very important for you personally. As we know that on this time, many ways to get whatever we wish. Likewise word says, many ways to reach Chinese's country. Therefore , this Introduction to Cryptography with Maple can make you sense more interested to read.

# Read Introduction to Cryptography with Maple by José Luis Gómez Pardo for online ebook

Introduction to Cryptography with Maple by José Luis Gómez Pardo Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Introduction to Cryptography with Maple by José Luis Gómez Pardo books to read online.

## Online Introduction to Cryptography with Maple by José Luis Gómez Pardo ebook PDF download

### Introduction to Cryptography with Maple by José Luis Gómez Pardo Doc

**Introduction to Cryptography with Maple by José Luis Gómez Pardo Mobipocket**

**Introduction to Cryptography with Maple by José Luis Gómez Pardo EPub**