Download Introduction To Cryptography With Maple

From the Back Cover This introduction to cryptography employs a programming-oriented approach to study the most important cryptographic schemes in current use... A distinctive feature of the author's approach is the use of Maple as a programming environment in which not just the cryptographic...This is the web page of the book "Introduction to Cryptography with Maple", by José Luis Gómez Pardo, published by Springer, January 2013.The Maple programs included in the book can be downloaded from the page "Maple Code",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.Introduction to Cryptography with Maple. The book is useful for a wide range of audiences. It can be used in an introductory course in cryptography for mathematics, computer science and engineering students. It includes some parts of algorithmic number theory, and it covers elementary concepts of number theory and algebra.