

Librería
Bonilla y Asociados
desde 1950



Título:

Autor:

Precio: \$1079.32

Editorial:

Año: 2009

Tema:

Edición: 1ª

Sinopsis

ISBN: 9783540691990

In this volume one finds basic techniques from algebra and number theory (e.g. congruences, unique factorization domains, finite fields, quadratic residues, primality tests, continued fractions, etc.) which in recent years have proven to be extremely useful for applications to cryptography and coding theory. Both cryptography and codes have crucial applications in our daily lives, and they are described here, while the complexity problems that arise in implementing the related numerical algorithms are also taken into due account. Cryptography has been developed in great detail, both in its classical and more recent aspects. In particular public key cryptography is extensively discussed, the use of algebraic geometry, specifically of elliptic curves over finite fields, is illustrated, and a final chapter is devoted to quantum cryptography, which is the new frontier of the field. Nice, elementary introduction to number theory on two of its real-world applications Each chapter ends with several complements and an extensive list of exercises, the solutions to most of which are included in the last chapter Coding theory is not discussed in full; however a chapter, sufficient for a good introduction to the subject, has been devoted to linear codes