1. Record Nr. UNICAMPANIAVAN00248643

Autore	Slinko, Arkadii
Titolo	Algebra for applications : cryptography, secret sharing, error-correcting, fingerprinting, compression / Arkadii Slinko
Pubbl/distr/stampa	Cham, : Springer, 2020
Titolo uniforme	Algebra for applications
Edizione	[2. ed]
Descrizione fisica	1 testo elettronico (xiv, 368 p. : ill.)
Soggetti	11A05 - Multiplicative structure; Euclidean algorithm; greatest common divisors [MSC 2020] 11A51 - Factorization; primality [MSC 2020] 11C08 - Polynomials in number theory [MSC 2020] 11C20 - Matrices, determinants in number theory [MSC 2020] 11T06 - Polynomials over finite fields [MSC 2020] 11T71 Algebraic coding theory; cryptography [MSC 2020] 11Y05 - Factorization [MSC 2020] 11Y11 - Primality [MSC 2020] 11Y16 - Number-theoretic algorithms; complexity [MSC 2020] 12E20 - Finite fields (field-theoretic aspects) [MSC 2020] 14G50 - Applications to coding theory and cryptography of algebraic geometry [MSC 2020] 14H52 - Elliptic curves [MSC 2020] 20A05 - Axiomatics and elementary properties of groups [MSC 2020] 20B30 - Symmetric groups [MSC 2020] 68P25 - Data encryption [MSC 2020] 68P30 - Coding and information theory (compaction, compression, models of communication, encoding schemes, etc.) [MSC 2020] 94A60 - Cryptography [MSC 2020] 94A62 - Authentication, digital signatures and secret sharing [MSC 2020]
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

Sommario/riassunto

Modern societies are awash with data that needs to be manipulated in many different ways: encrypted, compressed, shared between users in a prescribed manner, protected from unauthorised access, and transmitted over unreliable channels. All of these operations are based on algebra and number theory and can only be properly understood with a good knowledge of these fields. This textbook provides the mathematical tools and applies them to study key aspects of data transmission such as encryption and compression.
Designed for an undergraduate lecture course, this textbook provides all of the background in arithmetic, polynomials, groups, fields, and elliptic curves that is required to understand real-life applications such as cryptography, secret sharing, error-correcting, fingerprinting, and compression of information. It explains in detail how these applications really work. The book uses the free GAP computational package, allowing the reader to develop intuition about computationallyhard problems and giving insights into how computational complexity can be used to protect the integrity of data [...]. (Estratto dal sito dell'editore)