1. Record Nr. UNINA9911003695103321

Autore	Slinko A. M (Arkadii M.)
Titolo	Algebra for Applications : Cryptography, Secret Sharing, Error-Correcting, Fingerprinting, Compression / / by Arkadii Slinko
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-82626-4
Edizione	[3rd ed. 2025.]
Descrizione fisica	1 online resource (686 pages)
Collana	Springer Undergraduate Mathematics Series, , 2197-4144
Disciplina	004.01512
Soggetti	Algebra Computer science - Mathematics Discrete mathematics Mathematical Applications in Computer Science Discrete Mathematics Àlgebra Matemàtica discreta Informàtica Llibres electrònics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Integers -- Cryptology -- Groups -- Fields -- Polynomials -- Secret Sharing -- Error-Correcting Codes -- Compression -- Appendix A: GAP -- Appendix B: Miscellanea -- Solutions to Exercises -- Index.
Sommario/riassunto	This textbook provides mathematical tools and applies them to study key aspects of data transmission such as encryption and compression. Modern societies are awash with data that needs to be manipulated in many ways: encrypted, compressed, shared between users in a prescribed manner, protected from unauthorized access, and transmitted over unreliable channels. All of these operations are based on algebra and number theory. This textbook covers background topics in arithmetic, polynomials, groups, fields, and elliptic curves required for real-life applications like cryptography, secret sharing, error-correcting, fingerprinting, and compression of information. The book illustrates the work of these applications using the free GAP

computational package. It uses this package to help readers understand computationally hard problems and provide insights into protecting data integrity. This textbook covers a wide range of applications including recent developments, primarily intended for use as a textbook, with numerous worked examples and solved exercises suitable for self-study. This edition has been thoroughly revised with new topics and exercises, introducing hash functions for properly describing digital signatures, blockchains, and digital currencies in the latest version.