

1. Record Nr.	UNINA9910484931803321
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 International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-44074-5
Edizione	[2nd ed. 2020.]
Descrizione fisica	1 online resource (376 pages)
Collana	Springer Undergraduate Mathematics Series, , 2197-4144
Disciplina	512.9
Soggetti	Algebra Computer science - Mathematics Discrete mathematics Mathematical Applications in Computer Science Discrete Mathematics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1 Integers -- 2 Cryptology -- 3 Groups -- 4 Fields -- 5 Polynomials -- 6 Secret Sharing -- 7 Error-Correcting Codes -- 8 Compression -- Appendix A: GAP -- Appendix B: Miscellanea -- Solutions to Exercises -- Index.
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 computationally hard problems and giving insights into how computational complexity can be used to protect the integrity of data. The first undergraduate textbook to cover such a wide range of applications, including some recent developments, this second edition has been thoroughly revised with the addition of new topics and exercises. Based on a one semester lecture course given to third year undergraduates, it is primarily intended for use as a textbook, while numerous worked examples and solved exercises also make it suitable for self-study.
