1. Record Nr. UNINA9910338255203321

Autore	Childs Lindsay N
Titolo	Cryptology and Error Correction : An Algebraic Introduction and Real-World Applications / / by Lindsay N. Childs
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-15453-X
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XIV, 351 p. 7 illus., 1 illus. in color.)
Collana	Springer Undergraduate Texts in Mathematics and Technology, , 1867-5506
Disciplina	652.8 003.54
Soggetti	Algebra Data encryption (Computer science) Number theory Cryptology Number Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Preface -- 1. Secure, Reliable Information -- 2. Modular Arithmetic -- 3. Linear Equations Modulo m -- 4. Unique Factorization in Z -- 5. Rings and Fields -- 6. Polynomials -- 7. Matrices and Hamming Codes -- 8. Orders and Euler's theorem -- 9. RSA Cryptography and Prime Numbers -- 10. Groups, Cosets, and Lagrange's theorem -- 11. Solving Systems of Congruences -- 12. Homomorphisms and Euler's Phi function -- 13. Cyclic Groups and Cryptography -- 14. Applications of Cosets -- 15. An Introduction to Reed–Solomon codes -- 16. Blum–Goldwasser Cryptography -- 17. Factoring by the Quadratic Sieve -- 18. Polynomials and Finite Fields -- 19. Reed-Solomon Codes II -- Bibliography. .
Sommario/riassunto	This text presents a careful introduction to methods of cryptology and error correction in wide use throughout the world and the concepts of abstract algebra and number theory that are essential for understanding these methods. The objective is to provide a thorough understanding of RSA, Diffie–Hellman, and Blum–Goldwasser

cryptosystems and Hamming and Reed–Solomon error correction: how they are constructed, how they are made to work efficiently, and also how they can be attacked. To reach that level of understanding requires and motivates many ideas found in a first course in abstract algebra—rings, fields, finite abelian groups, basic theory of numbers, computational number theory, homomorphisms, ideals, and cosets. Those who complete this book will have gained a solid mathematical foundation for more specialized applied courses on cryptology or error correction, and should also be well prepared, both in concepts and in motivation, to pursue more advanced study in algebra and number theory. This text is suitable for classroom or online use or for independent study. Aimed at students in mathematics, computer science, and engineering, the prerequisite includes one or two years of a standard calculus sequence. Ideally the reader will also take a concurrent course in linear algebra or elementary matrix theory. A solutions manual for the 400 exercises in the book is available to instructors who adopt the text for their course.