1. Record Nr. UNINA9910299983103321

Autore	Hoffstein Jeffrey
Titolo	An Introduction to Mathematical Cryptography / / by Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman
Pubbl/distr/stampa	New York, NY : , : Springer New York : , : Imprint : Springer, , 2014
ISBN	1-4939-1711-0
Edizione	[2nd ed. 2014.]
Descrizione fisica	1 online resource (XVII, 538 p. 32 illus.)
Collana	Undergraduate Texts in Mathematics, , 0172-6056
Disciplina	652.80151
Soggetti	Number theory Data structures (Computer science) Data encryption (Computer science) Information theory Algebra Ordered algebraic structures Number Theory Data Structures and Information Theory Cryptology Information and Communication, Circuits Order, Lattices, Ordered Algebraic Structures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references (pages [507]-516) and index.
Nota di contenuto	Preface -- Introduction -- 1 An Introduction to Cryptography -- 2 Discrete Logarithms and Diffie-Hellman -- 3 Integer Factorization and RSA -- 4 Digital Signatures -- 5 Combinatorics, Probability, and Information Theory -- 6 Elliptic Curves and Cryptography -- 7 Lattices and Cryptography -- 8 Additional Topics in Cryptography -- List of Notation -- References -- Index.
Sommario/riassunto	This self-contained introduction to modern cryptography emphasizes the mathematics behind the theory of public key cryptosystems and digital signature schemes. The book focuses on these key topics while developing the mathematical tools needed for the construction and security analysis of diverse cryptosystems. Only basic linear algebra is required of the reader; techniques from algebra, number theory, and

probability are introduced and developed as required. This text provides an ideal introduction for mathematics and computer science students to the mathematical foundations of modern cryptography. The book includes an extensive bibliography and index; supplementary materials are available online. The book covers a variety of topics that are considered central to mathematical cryptography. Key topics include: classical cryptographic constructions, such as Diffie–Hellmann key exchange, discrete logarithm-based cryptosystems, the RSA cryptosystem, and digital signatures; fundamental mathematical tools for cryptography, including primality testing, factorization algorithms, probability theory, information theory, and collision algorithms; an in-depth treatment of important cryptographic innovations, such as elliptic curves, elliptic curve and pairing-based cryptography, lattices, lattice-based cryptography, and the NTRU cryptosystem. The second edition of An Introduction to Mathematical Cryptography includes a significant revision of the material on digital signatures, including an earlier introduction to RSA, Elgamal, and DSA signatures, and new material on lattice-based signatures and rejection sampling. Many sections have been rewritten or expanded for clarity, especially in the chapters on information theory, elliptic curves, and lattices, and the chapter of additional topics has been expanded to include sections on digital cash and homomorphic encryption. Numerous new exercises have been included.