1.

Record Nr.	UNINA9910485593303321
Autore	Buell Duncan A.
Titolo	Fundamentals of Cryptography : Introducing Mathematical and Algorithmic Foundations / / by Duncan Buell
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-73492-7
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (283 pages)
Collana	Undergraduate Topics in Computer Science, , 2197-1781
Disciplina	005.82
Soggetti	Data protection Cryptography Data encryption (Computer science) Computer science Data and Information Security Cryptology Theory and Algorithms for Application Domains
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1. Introduction -- 2. Simple Ciphers -- 3. Divisibility, Congruences, and Modular Arithmetic -- 4. Groups, Rings, Fields -- 5. Square Roots and Quadratic Symbols -- 6. Finite Fields of Characteristic 2 -- 7. Elliptic Curves -- 8. Mathematics, Computing, and Arithmetic -- 9. Modern Symmetric Ciphers — DES and AES -- 10. Asymmetric Ciphers — RSA and Others -- 11. How to Factor a Number -- 12. How to Factor More Effectively -- 13. Cycles, Randomness, Discrete Logarithms, and Key Exchange -- 14. Elliptic Curve Cryptography -- 15. Quantum Computing and Cryptography -- 16. Lattice-Based Cryptography -- 17. Homomorphic Encryption -- 18. Exercises.
Sommario/riassunto	Cryptography, as done in this century, is heavily mathematical. But it also has roots in what is computationally feasible. This unique and accessible textbook balances the theorems of mathematics against the feasibility of computation. Cryptography is something one actually “does”, not a mathematical game about which one proves theorems. There is deep math; there are some theorems that must be proven; and

there is a need to recognize the brilliant work done by those who focus on theory. But at the level of an undergraduate course, the emphasis should be first on knowing and understanding the algorithms and how to implement them, and also to be aware that the algorithms must be implemented carefully to avoid the “easy” ways to break the cryptography. Hence, this text covers the algorithmic foundations and is complemented by core mathematics and arithmetic. Topics and features: Provides an exhaustive set of useful examples, to optimally convey thecryptographic computations Focuses on doing cryptography, rather than on proving theorems Includes detailed source code and a test suite Describes NTRU as a lattice-based cryptographic algorithm Addresses, among other topics, factoring attacks (including their history), elliptic curve cryptography, quantum cryptography, and homomorphic encryption This clearly written introductory textbook emphasizes how implementation issues affect algorithm decisions and will reinforce learning for computer science (or mathematics) students studying cryptography at the undergraduate level. In addition, it will be ideal for professional short courses or self-study. Duncan Buell, professor emeritus in the Dept. of Computer Science and Engineering at University of South Carolina, also has 15 years of experience at a research lab doing high-performance computing research in support of the U.S. National Security Agency.