1. Record Nr. UNINA9910734874003321

Autore	Mihailescu Marius Iulian
Titolo	Pro Cryptography and Cryptanalysis with C++23 : Creating and Programming Advanced Algorithms / / by Marius Iulian Mihailescu, Stefania Loredana Nita
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2023
ISBN	9781484294505 1484294505
Edizione	[2nd ed. 2023.]
Descrizione fisica	1 online resource (499 pages)
Disciplina	005.824
Soggetti	C++ (Computer program language) Cryptography Data encryption (Computer science) Programming languages (Electronic computers) Data protection C++ Cryptology Programming Language Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Part I: Foundations -- 1: Introduction -- 2: Cryptography Fundamentals -- 3: Mathematical Background and Its Applicability -- 4: Large Integer Arithmetic -- 5: Floating Point Arithmetic -- 6: New Features in C++23 -- 7: Secure Coding Guidelines -- 8: Cryptography Libraries in C/C++23 -- Part II: Pro Cryptography -- 9: Elliptic Curve Cryptography -- 10: Lattice-based Cryptography -- 11: Searchable Encryption -- 12: Homomorphic Encryption -- 13: (Ring) Learning with Errors Cryptography -- 14: Chaos-based Cryptography -- 15: Big Data Cryptography16:Cloud Computing Cryptography -- Part III: Pro Cryptanalysis -- 17: Getting Started with Cryptanalysis -- 18: Cryptanalysis Attacks and Techniques -- 19: Linear and Differential Cryptanalysis -- 20: Integral Cryptanalysis -- 21: Brute Force and

Buffer Overflow Attacks -- 22: Text Characterization -- 23: Implementation and Practical Approach of Cryptanalysis Methods.

Sommario/riassunto

Develop strong skills for writing cryptographic algorithms and security schemes/modules using C++23 and its new features. This book will teach you the right methods for writing advanced cryptographic algorithms, such as elliptic curve cryptography algorithms, lattice-based cryptography, searchable encryption, and homomorphic encryption. You'll also examine internal cryptographic mechanisms and discover common ways in which the algorithms can be implemented and used correctly in practice. The authors explain the mathematical basis of cryptographic algorithms in terms that a programmer can easily understand. They also show how “bad” cryptography can creep in during implementation and what “good” cryptography should look like by comparing advantages and disadvantages based on processing time, execution time, and reliability. You will: Discover what modern cryptographic algorithms and methods are used for Design and implement advanced cryptographic mechanisms See how C++23 and its new features are impact the implementation of cryptographic algorithms Practice the basics of public key cryptography, including ECDSA signatures and more See how most of the algorithms can be broken.