1. Record Nr. UNINA9910874679803321

Autore	Nita Stefania Loredana
Titolo	Cryptography and Cryptanalysis in Java : Creating and Programming Advanced Algorithms with Java SE 21 LTS and Jakarta EE 11 / / by Stefania Loredana Nita, Marius Iulian Mihailescu
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2024
ISBN	9798868804410 9798868804403
Edizione	[2nd ed. 2024.]
Descrizione fisica	1 online resource (306 pages)
Disciplina	652.8
Soggetti	Java (Computer program language) Programming languages (Electronic computers) Cryptography Data encryption (Computer science) Computer science Mathematics - Data processing Algorithms Java Programming Language Cryptology Computer Science Computational Mathematics and Numerical Analysis
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	1. Getting Started -- 2. JDK 21 Java New Features -- 3. The New Jakarta EE 11 -- 4. Java Cryptography Architecture -- 5. Classical Cryptography -- 6. Quantum Cryptography -- 7. Formal Techniques for Cryptography -- 8. Pseudo-random Generators -- 9. Hash Functions -- 10. Symmetric Encryption Algorithms -- 11. Asymmetric Encryption Schemes -- 12. Advanced Encryption Schemes -- 13. Identification Schemes -- 14. Signature Schemes -- 15. Lattice based Cryptography and NTRU -- 16. Cryptography Tools.
Sommario/riassunto	Here is your in-depth guide to cryptography and cryptanalysis in Java.

This book includes challenging cryptographic solutions that are implemented in Java 21 and Jakarta EE 11. It provides a robust introduction to Java 21's new features and updates, a roadmap for Jakarta EE 11 security mechanisms, a unique presentation of the "hot points" (advantages and disadvantages) from the Java Cryptography Architecture (JCA), a new chapter on Quantum cryptography, and more. The book dives into the classical simple cryptosystems that form the basis of modern cryptography, with fully working solutions (encryption/decryption operations). Pseudo-random generators are discussed as well as real-life implementations. Hash functions are covered along with practical cryptanalysis methods and attacks, asymmetric and symmetric encryption systems, signature and identification schemes. The book wraps up with a presentation of lattice-based cryptography and the NTRU framework library. Modern encryption schemes for cloud and big data environments (homomorphic encryption and searchable encryption) also are included. After reading and using this book, you will be proficient with crypto algorithms and know how to apply them to problems you may encounter. New to This Edition: The modernized Second Edition is updated to reflect the latest language features in Java 21 and Jakarta 11, along with the introduction of a new chapter on Quantum Cryptography (Chapter 6). What You Will Learn Develop programming skills for writing cryptography algorithms in Java Dive into security schemes and modules using Java Explore “good” vs “bad” cryptography based on processing execution times and reliability Play with pseudo-random generators, hash functions, etc. Leverage lattice-based cryptography methods, the NTRU framework library, and more .