



METADATA

Title: Foundations and Applications of Modern Cryptography

Other Titles: A review of the main applications of modern cryptography

Language: Greek

Authors: Drosatos, G., Principal Researcher, ATHENA RC, Mavridis, I., Professor, UOM, Rantos, K., Professor, DUTH

ISBN: 978-618-228-316-5

Subject: MATHEMATICS AND COMPUTER SCIENCE, ENGINEERING AND TECHNOLOGY

Keywords: Information security / Cryptography / Privacy / Symmetric Cryptography / Public Key Cryptography

Bibliographic Reference: Drosatos, G., Mavridis, I., & Rantos, K. (2025). Foundations and Applications of Modern Cryptography [Undergraduate textbook]. Kallipos, Open Academic Editions. <http://dx.doi.org/10.57713/kallipos-1067>

Abstract

The book "Foundations and Applications of Modern Cryptography" provides an in-depth analysis of modern cryptographic algorithms, mechanisms, and applications that ensure data confidentiality, integrity, authentication, and key management. Through its 15 standalone chapters, it offers a comprehensive overview of fundamental cryptographic principles, including Symmetric and Asymmetric Encryption, hash functions, random number generators, and data integrity and authentication mechanisms. Additionally, it explores practical cryptographic applications, such as data protection, blockchain, and privacy-enhancing solutions. The book also

includes laboratory exercises and interactive educational material using CrypTool2 and Java/Eclipse, making it a valuable learning resource. In its final section, the book delves into specialized topics such as Lightweight Cryptography, Quantum Cryptography, and Post-quantum Cryptography. Aimed at meeting the needs of information security and privacy courses, it provides a balanced approach between theoretical foundations and practical implementation. Furthermore, it can serve as a complementary resource to existing textbooks in the field, aiding in the understanding and evaluation of cryptographic implementation alternatives.

