METADATA

Title: Computational Cryptography

Other Titles: -

Language: Greek

ISBN: 978-960-603-276-9

Subject: MATHEMATICS AND COMPUTER SCIENCE, NATURAL SCIENCES AND AGRICULTURAL SCIENCES, ENGINEERING AND TECHNOLOGY

Keywords: Computational Complexity / Computational Number Theory / Symmetric Cryptography / Public Key Cryptography / Cryptographic Protocols

Bibliographic Reference: Zachos, E., Pagourtzis, A., & Grontas, P. (2015). Computational Cryptography [Undergraduate textbook]. Kallipos, Open Academic Editions. http://dx.doi.org/10.57713/kallipos-492

Abstract

This book aims to introduce the reader to the fundamental concepts and techniques of modern cryptography, with an emphasis on their algorithmic and computational aspects. Concretely, the book contains the following topics: - Introduction to basic algorithmic and computational complexity concepts such as: algorithm analysis, efficiency, polynomial time, probabilistic algorithms, complexity classes. - Elements of number theory and group theory: modular arithmetic, groups, rings, fields, Chinese Remainder Theorem, Fermat's, Euler's, and Lagrange's Theorems, primitive roots, Euler's totient function, quadratic residues, Legendre and Jacobi symbols. - Computational complexity and algorithms for fundamental number-theoretic problems: repeated squaring, Euclidean and extended Euclidean algorithms, Jacobi symbol computation, roots modulo n, primality tests (Fermat, Solovay-Strassen, Miller-Rabin, AKS algorithm), factorization methods (ρ method, Dixon's method), discrete logarithm (Shanks, Pohling-Hellman, index-calculus). - Symmetric cryptosystems: block ciphers (DES, AES), stream ciphers, modes of operation. - Public-key cryptosystems: RSA, ElGamal, Diffie-Hellman key exchange. - Digital signature schemes: RSA, DSS, special-purpose signatures (one-time, blind, undeniable). - Cryptographic protocols: secret sharing, coin flipping, key exchange. - Security proofs based on computational hardness assumptions, security models (KPA, CPA, CCA, IND-CPA, IND-CCA), cryptographic reductions. - Hash functions and one-way functions: pseudo-randomness. - Zero-knowledge proofs: identification protocols. - Advanced topics: quantum and post-quantum cryptography, elliptic curves, protocol composition, bilinear maps, lattice-based cryptography.

The Project is funded by the National Development Programme 2021-2025 of the Ministry of Education and Religious Affairs and implemented by the Special Account for Research Funds of the National Technical University of Athens and the Hellenic Academic Libraries Link.