METADATA

Title: Introduction to Cryptography

Other Titles: -

Language: Greek

Authors: Draziotis, K., Assistant Professor, AUTH

ISBN: 978-618-85820-5-7

Subject: MATHEMATICS AND COMPUTER SCIENCE

Keywords: Cryptography / Number theory / Information security / Symmetric cryptography / Public key cryptography

Bibliographic Reference: Draziotis, K. (2022). Introduction to Cryptography [Undergraduate textbook]. Kallipos, Open Academic Editions. http://dx.doi.org/10.57713/kallipos-17

Abstract

The book covers basic subjects of cryptography. In the first chapter we provide an introduction to cryptography and we provide some applications of modern cryptography. Chapters two, three and four concern private key cryptography, where we provide stream and block ciphers. Furthermore, some necessary security definitions are given. In the fifth chapter we present hash and MAC functions. After the sixth chapter we present public key cryptography. Sixth chapter is devoted to Diffie-Hellman key agreement protocol and chapter seven provides a brief introduction in complexity theory and Turing machine. In chapters eight, nine and ten we present basic elements of number theory which are necessary to understand RSA cryptosystem and digital signatures. In chapter eleven we present RSA trapdoor function and in the next chapter we provide some attacks to RSA, such as Wiener's attack. In chapter thirteen, an introduction to digital signatures is presented. In chapter fourteen we describe the basic lattice theory and algorithms concerning them, such as LLL, enumeration algorithm with pruning and Babai's algorithm. Finally, the last chapter is devoted to SSL/TLS and PGP protocols, accordingly we present some applications.

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.