Module Name: (A.1) Applied Cryptography

Aim

This module focuses on improving knowledge on modern cryptography and on practical techniques about how to appropriately apply cryptographic algorithms, combined with appropriate hardware implementations and cryptographic key management techniques to solve information security problems.

Learning Objectives

The learning objectives include the comprehension, analysis and applicability of the mechanisms of encryption, authentication, integrity, as well as cutting-edge technologies such as digital signatures, homomorphic encryption and Blockchains. The course will analyze the mechanisms and solutions used in real systems focusing on the way the required security is achieved. Such systems include electronic IDs, electronic payments and telecommunications. Participants will have the opportunity to gain important knowledge about the use of cryptography and information systems protection mechanisms and through this familiarity to be able to study, analyze, research and suggest ways to protect information for any processing environment.

Learning Outcomes

On successful completion of this module, students should be able to:

- Analyze scientific research papers and describe the use of cryptographic algorithms to satisfy security requirements.
- Propose appropriate algorithms and cryptosystems based on the system's security requirements.
- Develop cryptosystems to satisfy confidentiality, integrity and authentication requirements.
- Design cryptographic authentication and key agreement protocols, as well as zero-knowledge. Protocols.
- Explain the use of trust services and the corresponding legal framework.
- Analyze security properties for blockchains and propose appropriate uses.
- Deploy blockchain solutions to satisfy security requirements.

Bibliography

[1] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone (1996) Handbook of Applied Cryptography ISBN 0-8493-8523-7. Available online: http://www.cacr.math.uwaterloo.ca/hac/

[2] William Stallings. Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 2017, ISBN-13: 9780134444284.

[3] Xiwei XuIngo WeberMark Staples, Architecture for Blockchain Applications, Springer, 2018, https://doi.org/10.1007/978-3-030-03035-3

[4] Pethuru Raj, Ganesh Chandra Deka (Eds), Blockchain Technology: Platforms, Tools and Use Cases, Volume 111, Advances in Computing, 2018