Course	Name	: Security and Cryptography
	Code	: EE184930
	Credits	: 3
	Semester	: Elective

Description of Course

With the rapid development of communication and internet networks and the increasingly widespread use of devices and data connected to the network, the challenges to information security and networking are increasingly important. In this course students will study security issues in data, communication systems and networks, and the techniques used to overcome them. Specifically, number theory and finite fields will be discussed to understand cryptographic techniques, both symmetric and asymmetric, and algorithms to protect data integrity. Students will also study cryptographic applications on the security of multimedia content.

Learning Outcomes

Knowledge

(P02) Mastering the concepts and principles of engineering, and implementing them in the form of procedures for analysis and design in power systems, control systems, multimedia telecommunications, or electronics.

Specific Skill

(KK01) Able to formulate engineering problems in power systems, control systems, multimedia telecommunications, or electronics.

General Skill

(KU12) Able to implement information and communication technology (ICT) in the context of implementation of his/her work.

Attitude

(S09) Demonstrating attitude of responsibility on work in his/her field of expertise independently.

Course Learning Outcomes

Knowledge

Mastering the challenges and concepts of security in communication and network systems for data distribution, as well as cryptographic-based techniques to overcome security issues and protect data integrity.

Specific Skill

Able to explain the working principles of symmetric and asymmetric cryptographic techniques and their application to overcome security problems in communication and network systems.

General Skill

Able to use software and tools to implement cryptographic techniques and system security simulations on the network, such as Matlab and ns-3.

Attitude

Able to show an attitude of responsibility for work in his area of expertise independently.

Main Subjects

1. Introduction to the concept of security in communication and network systems
2. Basics of number theory
3. Classic encryption techniques
4. Block Cipher and Data Encryption Standard (DES)
5. Finite field basics
6. Advanced Enryption Standard (AES)
7. Public key cryptography and RSA
8. Hash function and user authentication
9. Network access control and cloud security
10. Wireless network security
11. Security for multimedia content

Reference(s)

[1] William Stallings, “Cryptography and Network Security: Principles and Practice,” 7th ed., Pearson, 2017.
[2] Jonathan Katz & Yehuda Lindell, “Introduction to Modern Cryptography,” 2nd ed., CRC Press, 2015.

Prerequisite(s)

--