COURSE	Name	: Information Security and Cryptography
	Code	: EE185536
	Credit(s)	: 2
	Semester	: (Elective Course)

Description of Course

With the rapid development of communication and internet networks and the wider 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 and techniques to overcome them from two aspects: aspects of information theory and computational or cryptographic aspects. Specifically the course covers the basic of information theory, security capacity, effective security, secure coding, secret key generation, number theory and finite field cryptographic techniques, both symmetric and asymmetric, and algorithms to protect data integrity.

Learning Outcomes

Knowledge

(P01) Mastering the concepts and principles of science in a comprehensive manner, and to develop procedures and strategies needed for the analysis and design of systems related to the field of power systems, control systems, multimedia telecommunications, electronics, intelligent multimedia network, or telematics as a preparation for further education or professional career.

Specific Skill

(KK01) Being able to formulate engineering problems with new ideas for the development of technology in power systems, control systems, multimedia telecommunications, electronics, intelligent multimedia network, or telematics.

General Skill

(KU11) Being able to implement information and communication technology in the context of execution 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 the distribution of data from aspects of information theory and aspects of computing, as well as cryptographic-based techniques to overcome security issues and to protect data integrity.

Specific Skill

Able to explain the principles of physical layer security and implement secret key generation and explain 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

Demonstrating attitude of responsibility for work in his/her area of expertise independently.

Main Subjects

1. Introduction to the concept of security in communication and network systems
2. Basic information theory and physical layer security
3. Security capacity
4. Secret key generation
5. Basics of number theory
6. Block Cipher and Data Encryption Standard (DES)
7. Finite field basics
8. Advanced Enryption Standard (AES)
9. Public key cryptography and RSA
10. Wireless network security

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.

[3] Rafael F. Schaefer, Holger Boche, Ashish Khisti, & H. Vincent Poor, “Information Theoretic Security and Privacy of Information Systems,” Cambridge University Press, 2017.

Prerequisite(s)

--