Dongseo University

Division of Computer Engineering

Information Security

Instructor(s): HoonJae LEE/SangGon LEE
Office:-
Phone: -
Email: -

Classroom: -
Class Time: 3 hour/week
Office Hours: 9:00am - 8:00pm

Course Description:
Information Security is a specialization area that focuses on cryptography research. The goal of this specialization area is to educate future experts in the field that have a strong and broad knowledge of the mathematical aspects of cryptography and data security. Modern symmetric and asymmetric cryptography algorithms and protocols are studied and analyzed from the mathematical point of view. Students will learn to assess the strengths and weaknesses of cryptographic solutions based on a deep understanding of the underlying theory. Students will also gain the ability to design cryptographic algorithms and protocols for real applications.

Course Goals & Objectives:
At the conclusion of this course, the successful (passing) students will understand classical ciphers and modern cryptography including stream cipher, block cipher, PKC(Public-Key Cryptosystem) and Hash codes & MAC codes.

Course Outline:

- **Week 1 Overview of the Information Security**
- **Week 2 Overview of the Cryptography and Network Security**
- **Week 3 CISCO ROUTE & SWITCH security**
- **Week 4 Classical Ciphers**
- **Week 5 Stream Cipher - LFSR and PRNG**
- **Week 6 Block Cipher – DES algorithm**
- **Week 7 Block Cipher – AES algorithm**
- **Week 8 Block Cipher – other block ciphers**
- **Week 9 Hash functions and MAC codes**
- **Week 10 Public-Key Cryptosystem - Diffie-Hellman**
- **Week 11 Public-Key Cryptosystem - RSA**
- **Week 12 Public-Key Cryptosystem - ECC**
- **Week 13 Applications to cryptosystems(1)**
- **Week 14 Applications to cryptosystems(2)**
- **Week 15** Final Week

Textbook(s)

- Required: "**Crytpography and Network Security(by William Stalling)**
- Recommended: PPT slides(uploaded to eclass.dongseo.ac.kr)

Class Website: e-Class

Course Assignments & Grading:

- *Assignments*: 30% (Programming for cipher codes)
- *Bonus Credit*: None
- *Grading*: A/B/C/D/E/F

Grading Policies:

- *Exams: Final 40%*
- *Quizzes*: 10%
- *Course Projects*: None
- *Attendance*: 20%

Course Policies:

- Attendance: 20%
- Academic Misconduct Policy: