Course Introduction

1. Course Information

Course Name	Cryptography and Information Security (Theory and Practice)	Department	Computer Science & Engineering
Credit	3	Class Number	9441042
Year/Semester	2017 Spring Semester	Class Hour	Monday 14:00~17:00

2. Professor

Name	Jong Hyuk Park	E-Mail	jhpark1@seoultech.ac.kr
Tel	02-970-6702	Homepage	www.parkjonghyuk.net
Room	Mirae Hall #325	Office Hour	Mon~Fri(10:00~18:00)

3. Course Outline and Goals

In this course we will learn about the basic theory of cryptography and its applications in information security. And in-depth discussion about the algorithm related to cryptography. In addition, we discuss the practical areas for security vulnerabilities and countermeasures and information protection systems. Furthermore, we will discuss recent research issues in good journal papers.

4. Evaluation Methods(Grading):

Midterm	FinalExam	Project/ Presentation	Attendance	Total
20%	30%	40%	10%	100 %

5. Assignment

- Summary and presentation of a chapter (in textbook)
- Survey and presentation of recent research issues in good journal papers

6. Textbook and References :

1) TextBook:

Cryptography And Network Security, William Stallings, Pearson

Cryptography Engineering: Design Principles and Practical Applications, Niels Ferguson

2) Auxiliary Textbook:

IEEE Xplore Digital Library, http://www.ieeexplore.ieee.org/

ACM Digital Library, http://dl.acm.org/dl.cfm

7. Keyword

: Information Security, Cryptography, Hash Function, User Authentication

Week	Contents
1st	* Orientation CHAPTER 01 Computer Security Overview
2nd	CHAPTER 02 Classical Encryption Technology
	CHAPTER 03 Block Cipher and DES
3rd	CHAPTER 04 Basic Concepts in Number Theory and Finite Fields
	CHAPTER 05 Advanced Encryption Standard (AES)
4th	CHAPTER 06 Block Cipher Operation
5th	CHAPTER 07 PSEUDORANDOM NUMBER GENERATION AND STREAM CIPHERS
	CHAPTER 08 More Number Theory
6th	CHAPTER 09 Public-Key Cryptography and RSA
7th	CHAPTER 10 Other Public-Key Cryptosystems
8th	Midterm
9th	CHAPTER 11 Cryptographic Hash Function
	CHAPTER 12 Meesage Authentication Codes
10th	CHAPTER 13 Digital Signatures
	CHAPTER 14 Key Management and Distribution
11th	CHAPTER 15 User Authentication Protocols
12th	CHAPTER 16 Transport-Level Security
13th	CHAPTER 17 Wireless Network Security
14th	CHAPTER 19 IP Security
15th	Final Exam