Cryptography and Information Security

1. 일반사항 2021학년도 1학기

교과목명	암호이론및정보보안실무	과정	일반대학원	개설학과	컴퓨터 공학과
이수단위	3	교과목코드	9441042	강좌시간	화 2, 3, 4 교시
담당교수	박종혁	연구실	02-970-6702	홈페이지	parkjonghyuk.net

2. 교과목 개요 및 강의목표

본 교과목에서는 정보보안의 기본 이론인 암호학과 그 응용분야에 대해 학습한다. 암호학과 관련된 알고리즘에 대해 심도있게 논의 하며, 응용분야에서는 보안 취약점과 대응방안, 정보보호시스템 등에 대해 실무관련 분야에 대해 논의한다. 최근 암호학 및 보안관련 논문, 저서, 연구보고서 등을 분석하며 심도 있는 토론을 진행한다.

3. 수업 형식

· Presentation / discussion (Face to face or Non face to face)

4. 학습평가 방법

출결	발표	증간고사	기말고사	총합
0%	30%	40%	30%	100%

발표: 수강원이 3~4명 팀을 이루어 본수업과 관련한 논문을 작성하여 중간고사 이전에 제출해야 한다.
(수강정정 기간 후 팀 배정 예정)

중간고사: 팀별 작성한 논문에 대한 평가를 진행한다.

기말고사: 팀별 작성한 논문에 대한 발표 동영상 자료(15분)를 제작하여 기한 내 eClass에 업로드 한다.

5. 교재 및 참고 문헌

1) 주교재:
   - Cryptography and Network Security, William Stallings, Pearson
   - 컴퓨터보안과 암호, William Stallings (최용락 외 2 명 옮김), 그린출판
   - Cryptography Engineering: Design Principles and Practical Applications, Niels Ferguson
2) 보조교재
   - IEEE Xplore Digital Library, http://www.ieeexplore.ieee.org/
   - ACM Digital Library, http://dl.acm.org/dl.cfm
· - Elsevier, http://www.elsevier.com
   - Springer, http://springer.com

6. 주차 수업내용

주별 학습활동	
주 차	**수 업 주 제**
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	**Middle Term / Team paper submission**
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 Term / Presentation video data submit**