강 의 계 획 서

개설 학기	2015년 제2학기	교과목명	네트워크 보안
학수/강좌번호	CSE4072-01	이수구분 및 학점	3학점
개설 학과/학년	컴퓨터공학과 3/4학년	설계 인정 학점	0학점
담당 교수		담당 조교	
이름	문 봉 교	이름	
연구실	신공학관 10112	연구실	신공학관 5130
이-메일	bkmoon@dongguk.edu	e-메일	
전화번호	2260-8592	전화번호	2260-1425
상담 시간	수업직후 1시간 30분	상담 시간	수업직후 1시간 30분

강좌 구성			권장 선수과목
이론	실험·실습	설계	이산수학
3	0	0	

강의 목표	① 암호수학의 기본 개념을 바탕으로 암호 알고리즘의 기본적인 동작원리를 이해한다. ② 메시지 인증, 사용자 인증, 디지털 서명 및 키 관리 등의 메카니즘을 이해한다. ③ 인터넷의 각 계층별 암호 및 보안 프로토콜을 이해한다.
강의 개요	암호학에 대한 기본적인 이해를 바탕으로 네트워크 보안에서 필수적인 개념에 대해 공부한다. 먼저 암호학에 대한 이론적인 내용을 공부하고 인터넷의 동작 환경에서 발생할 수 있는 다양한 보안 이슈에 대해서 공부한다. 또한 학생들은 다양한 과제를 수행하고 이를 통해 관련 내용을 깊이 있게 이해한다.
강의 내용	본 강좌에서는 암호학의 기본개념과 인터넷의 각 계층별 인증 및 보안 이슈를 공부한다. 즉, 네트워크 환경에서 대칭키/공개키 암호화 방식을 활용한 메시지 인증, 디지털 서명, 키 분배, IP 보안, SSL/TLS 기반의 Web 보안 등을 공부한다.
강의 방법	강의는 기본적으로 매주 1시간 20분씩 2번의 이론 강의를 진행한다. 학생들은 강의진도에 따라 주어진 과제를 수행하고 이를 바탕으로 주어진 논문을 읽고 발표한다.
과제물	총 4번의 연습문제풀이 과제가 부여된다. S/W 과제는 C언어를 이용한 암호시스템의 구현을 포함한다. 주어진 논문들 중에서 팀별로 선택하여 스케쥴에 맞춰 발표를 진행한다.
교재 및 참고서적	- (주교재) Cryptography and Network Security, B. A. Forouzon, McGraw-Hill,2008(번역판 가능) - (부교재) C로 배우는 암호학 프로그래밍, 하재철, 문재상, 도서출판 YOUNG, 2011 - (참고) Quantum Bits and Quantum Secrets, O. Morsch, John Wiley & Sons (북스힐 번역판 2010년) - (참고) Cryptography and Network Security, 6th Ed., William Stallings, Pearson, 2014 - (참고) Introduction to Cryptography, 2nd Ed. W. Trappe, L. Washington, Pearson, 2006 - (참고) Network Security Essentials, 5th Ed., William Stallings, Pearson, 2014 - (참고) Computer Networks and Internets, 5th Ed., Douglas Comer, Pearson, 2009 - (참고) 암호의 해석, 루돌프 케펜한 지음|이일우 옮김, 코리아 하우스
참고사항	네트워크 보안을 개념적으로 이해할 수 있도록 이산수학 범위내에서 수학적인 부분을 최대한 줄여서 암호학과 인터넷 구조에 대한 설명을 바탕으로 강의를 진행함. [**수업태도 불량**] 10분 이상 지각 및 강의중 화장실이나 휴대전화 등 개인용무로 임의로 퇴실한 학생은 결석 처리함. 퇴실후 재입실 및 강의진행 방해하는 학생은 태도점수 불량 처리함

평가 도구 및 비중	중간시험	기말시험	출석	논문발표	연습문제	S/W 과제	수업태도
	20 %	30 %	5 %	10%	10 %	20 %	5 %

주별 강의 일정

week	Lecture Topics	Reading Assignments	과제
1	네트워크 보안 및 양자암호 (물리계층 암호)	Chap.1 및 별도자료(D. Comer)	Tutorial 논문 읽기
2	암호수학 (정수, 모듈로, 행렬, 선형합동)	Chap.2	
3	고전 대칭키 암호	Chap.3	연습문제풀이1
4	대수구조 (Group, Ring, GF(2^n) Field) 현대 대칭키 암호	Chap.4 & 5	DES 및 AES 암호 구현
5	Data Encryption Standard (DES) Advanced Encryption Standard (AES)	Chap.6 & 7	연습문제풀이2
6	현대 대칭키 암호를 이용한 암호화기법	Chap.8	
7	소수, 소인수분해, 원시근, 이산로그	Chap.9	
8	**Midterm Examination**	중간고사	
9	비대칭키 (RSA 공개키) 암호	Chap.10	소수(난수) 발생기 및 RSA 암호 구현
10	메시지 인증 & 암호학적 해쉬 함수	Chap.11 & 12	연습문제풀이3
11	디지털 서명 & 개체인증	Chap.13 & 14	
12	키 관리 (대칭키 분배 및 공개키 배분)	Chap.15	
13	TCP/IP 프로토콜 Review	별도자료(D. Comer)	SHA-1 및 SHA-3 구현 http://csrc.nist.gov/groups/ST/hash/sha-3/
14	전송층 보안 (SSL과 TLS)	Chap.17	연습문제풀이4
15	네트워크층 보안 (IPSec)	Chap.18	
16	**Final Examination**	기말고사	