

# 강 의 계 획 서

교 과 목 명	한 글	정보보호론				교과목 코드	109820				
	영 문	Information Protection Theory									
개 설 학 과	컴퓨터공학과				교과 구분	교양	MSC	전공	O		
강 좌 번 호	31001				강의 시간	월 2,3,4 교시					
학년 및 학기	3학년 2학기				선수 교과목명	-					
이수구분 및 학점(시수)	교필	교선	전필	전선	기타	강의내용 및 학점(시수)	이론	설계	실험	실습	기타
				3(3)			2(2)			1(1)	
담 당 교 수 (작성자)	성 명	박종혁				작성일시	2018 년 6 월 15 일				
	TEL	02-970-6702				E-mail	jhpark1@seoultech.ac.kr				
	Room	미래관 325호				Homepage	http://www.parkjonghyuk.net				
교과목 개요	<p>최근 정보는 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등의 방법으로 공격을 받는다. 정보의 위협이 점차적으로 증가하고 있기 때문에 이를 방지하기 위한 대책이 필요하다. 바이러스 및 악성코드 침투, 해킹 등 여러 가지 보안 이슈들이 사회적으로 자주 발생하고 있으며 이러한 보안 이슈들을 해결하기 위해 정보보호 기술이 필수적이다.</p> <p>본 교과목에서는 정보보호의 개념과 기술 등 기본적인 이론부터 실생활에 필요한 응용기술까지 현대암호와 함께 정보보호의 전반적인 이론 및 기초 지식에 대해 학습한다.</p>										
교육 목표	<p>1) 정보보호의 개념 및 기술발전의 흐름을 이해하고 필요성을 인식한다.                  2) 현대 컴퓨터 통신/네트워크 사회에서 사용되고 있는 정보보호 기술을 이해한다.                  3) 팀 프로젝트 진행을 통해 실무경험을 쌓도록 한다.</p>										
학 습 성 과  수준(관련도) (L3 = 상) (L2 = 중) (L1 = 하)	<b>프로그램 학습성과 번호(※ 3. 학습 성과 달성 계획서와 일치)</b>						<b>수준</b>	<b>반영률</b>			
	(1) 수학, 기초과학, 공학의 지식과 정보기술을 응용할 수 있는 능력						L2	30%			
	(2) 이론이나 알고리즘을 수식 또는 프로그래밍 등을 통해 검증할 수 있는 능력						L2	20%			
	(4) 컴퓨팅 분야의 문제를 해결하기 위해 최신정보, 연구 결과, 프로그래밍 언어를 포함한 적절한 도구 등을 활용할 수 있는 능력						L3	30%			
	(6) 컴퓨팅 분야의 문제를 해결하는 과정에서 팀 구성원으로서 팀 성과에 기여할 수 있는 능력						L1	20%			
교재 및 참고자료	<p>교재 : 알기 쉬운 정보보호 개론, 히로시 유키 지음 (이재광 외 2 공역), 인피니티북스, 2017</p> <p>실습 보조교재 : 정보보안 원리 및 실습, 황성운 저, 생능출판, 2017. 11.</p>										
활용 기자재	<p>칠판( O ), 빔프로젝터(O ), PC(O ), VTR( ), 실습장비( ), 기타( )</p>										
학습평가 방법	<p>출석 (10%), 발표 (10%), 과제물 (20%), 중간고사 (30%), 기말고사 (30%)</p>										
강의(수업)방법	<p>강의(O), 토론( ), 설계or프로젝트(), 발표(O), 실험( ), 실습( ), 기타(O)</p>										
기 타 사항	<p>*개인과제 #1 : 최신 암호응용 / 정보보호 관련 인터넷 및 자료조사 등을 통해 기술 동향 보고서 작성하여 제출한다.                  *개인과제 #2 : 개인과제 #1을 기반으로 정보보호 아이디어 제안 보고서를 제출한다.                  *발표 : 발표는 수시로 희망자에 한하여 발표할 수 있다. (학습 태도 반영 가능)</p>										

## 2. 강의 진도계획서

주별	강 의 내 용	방법, 실습, 과제, 평가
1주	사전 설문조사 1장 정보보호	수강생 사전설문조사 강의
2주	2장 암호의 세계 3장 암호의 역사	이론 강의
3주	4장 대칭 암호	이론 강의
4주	5장 대칭 암호(공통 키 암호)	이론 강의
5주	6장 공개 키 암호	이론 강의
6주	7장 하이브리드 암호 시스템	이론 강의
7주	8장 일방향 해시 함수	이론 강의
8주	중간고사 및 중간설문 조사	중간 설문조사 중간고사
9주	9장 메시지 인증 코드	이론 강의 *개인과제 #1 제출
10주	10장 디지털 서명	이론 강의
11주	11장 인증서	이론 강의
12주	12장 키	이론 강의
13주	13장 난수 14장 PGP	이론 강의
14주	15장 SSL/TLS 16장 암호 기술과 현실 세계	이론 강의
15주	학기말 고사 및 최종설문 조사	최종설문 조사 기말고사 *개인 과제 #2 제출