

결	전공주임	교학부장
재		

수업 계획서

< 2017학년도 8월 21일 ~ 12월 8일 >

1. 강의개요							
학습과정명	암호프로토콜	학점	3	교강사명		교강사 전화번호	
강의시간	3	강 의 실		수강대상	정보보호	E-mail	
2. 교육과정 수업목표							
<ul style="list-style-type: none"> - 암호프로토콜의 개요를 이해한다. - 네트워크 부분에서 제공하는 IP 보안프로토콜, SSL, TLS, IPSec등을 이해한다. - 응용어플리케이션의 S/MIME, PGP 등의 원리를 이해한다. 							
3. 교재 및 참고문헌							
주교재	네트워크 보안 에센셜	저자	William Stallings	출판사	생능출판사	출판년도	2013
부교재(참고문헌)		저자		출판사		출판년도	
4. 주차별 강의(실습·실기·실험) 내용							
주별	차시	강의(실습·실기·실험) 내용				과제 및 기타 참고사항	
제 1 주	1	- 강의 주제: 대칭암호 1				- 주:p.63~79 - 전자교탁	
	2	- 강의 목표: 대칭암호의 원리 및 알고리즘 학습					
	3	- 세부 내용: - 대칭암호 원리 - 대칭 암호 알고리즘 - 수업 방법 : 강의 및 실습					
제 2 주	1	- 강의 주제: 대칭암호 2				- 주:p.80~99 - 전자교탁	
	2	- 강의 목표: 대칭암호의 원리 및 알고리즘 학습					
	3	- 세부 내용: - 랜덤넘버와 의사랜덤 넘버 - 스트림 암호화 RC4 - 암호블록 운용 모드 - 수업 방법 : 강의 및 실습					
제 3 주	1	- 강의 주제: 공개키 암호화 메시지 인증1				- 주:p.109~129 - 전자교탁	
	2	- 강의 목표: 비대칭암호의 원리 및 알고리즘 학습					
	3	- 세부 내용: - 메시지 인증 방법 - 안전해쉬 함수 - 메시지 인증 코드 - 수업 방법 : 강의 및 실습					
제 4 주	1	- 강의 주제: 공개키 암호화 메시지 인증2				- 주:p.130~148 - 전자교탁 - 수시시험1	
	2	- 강의 목표: 비대칭암호의 원리 및 알고리즘 학습					
	3	- 세부 내용: - 공개키 암호 원리 - 공개키 암호 알고리즘 - 디지털 서명 - 수업 방법 : 강의 및 실습					
제 5 주	1	- 강의 주제: 키 분배와 사용자 인증 1				- 주:p.158~182 - 전자교탁	
	2	- 강의 목표: 암호에 사용되는 키 분배 알고리즘 학습					

	3	<ul style="list-style-type: none"> - 세부 내용: - 대칭 암호를 이용한 대칭키 분배 - KERBEROS - 비대칭 암호를 이용한 키분배 - 수업 방법 : 강의 및 실습 	
제 6 주	1	<ul style="list-style-type: none"> - 강의 주제: 키 분배와 사용자 인증 2 	<ul style="list-style-type: none"> - 주:p.183~206 - 전자교탁
	2	<ul style="list-style-type: none"> - 강의 목표: 암호에 사용되는 키 분배 알고리즘 학습 - 세부 내용: 	
	3	<ul style="list-style-type: none"> - X.509 인증서 - 공개키 기반구조 - 통합 신원 관리 - 수업 방법 : 강의 및 실습 	
제 7 주	1	<ul style="list-style-type: none"> - 강의 주제: 전송 레벨 보안 1 	<ul style="list-style-type: none"> - 주:p.217~242 - 전자교탁
	2	<ul style="list-style-type: none"> - 강의 목표: 전송 레벨에서 암호 기법 학습 - 세부 내용: 	
	3	<ul style="list-style-type: none"> - 웹 보안 및 소켓 계층 전송 보안 - 전송 계층 보안 - 수업 방법 : 강의 및 실습 	
제 8 주	1	<p>중간고사</p>	<p>총 30점 (주 객관식의 적절한 혼합)</p>
	2		
	3		
제 9 주	1	<ul style="list-style-type: none"> - 강의 주제: 전송 레벨 보안 2 	<ul style="list-style-type: none"> - 주:p.243~260 - 전자교탁
	2	<ul style="list-style-type: none"> - 강의 목표: 전송 레벨에서 암호 기법 학습 - 세부 내용: 	
	3	<ul style="list-style-type: none"> - HTTPS - SSH - 수업 방법 : 강의 및 실습 	
제 10 주	1	<ul style="list-style-type: none"> - 강의 주제: 무선 네트워크 보안 	<ul style="list-style-type: none"> - 주:p.265~318 - 전자교탁
	2	<ul style="list-style-type: none"> - 강의 목표: 무선네트워크 보안 알고리즘 학습 - 세부 내용: 	
	3	<ul style="list-style-type: none"> - IEEE 802.11 무선 LAN 개요 및 보안 - 무선 응용 프로토콜 개요 - 무선 전송층 보안 - 수업 방법 : 강의 및 실습 	
제 11 주	1	<ul style="list-style-type: none"> - 강의 주제: 전자메일 보안 1 	<ul style="list-style-type: none"> - 주:p.325~372 - 전자교탁
	2	<ul style="list-style-type: none"> - 강의 목표: PGP 알고리즘의 이해 및 학습 - 세부 내용: 	
	3	<ul style="list-style-type: none"> - PGP개요 - S/MIME - 수업 방법 : 강의 및 실습 	
제 12 주	1	<ul style="list-style-type: none"> - 강의 주제: 전자메일 보안 2 	<ul style="list-style-type: none"> - 주:p.373~386 - 전자교탁 - 과제1(최신암호 기술 동향)
	2	<ul style="list-style-type: none"> - 강의 목표: PGP 알고리즘의 이해 및 학습 - 세부 내용: 	
	3	<ul style="list-style-type: none"> - 도메인 키 확인 메일 개요 - DKM 전략 - 수업 방법 : 강의 및 실습 	
제 13 주	1	<ul style="list-style-type: none"> - 강의 주제: IP 보안 1 	<ul style="list-style-type: none"> - 주:p.391~413 - 전자교탁
	2	<ul style="list-style-type: none"> - 강의 목표: IPSec에 대한 이해 및 학습 - 세부 내용: 	
	3	<ul style="list-style-type: none"> - IP보안 개요 - IP보안 정책 - 캡슐화 보안 페이로드 - 수업 방법 : 강의 및 실습 	
제 14 주	1	<ul style="list-style-type: none"> - 강의 주제: IP 보안 2 - 강의 목표: IPSec에 대한 이해 및 학습 	<ul style="list-style-type: none"> - 주:p.414~434 - 전자교탁

제 15 주	2	- 세부 내용: - 보안 연관 묵기 - 인터넷 키교환 - 암호도구 - 수업 방법 : 강의 및 실습	총 30점 (주 객관식의 적절한 혼합)
	3		
	1		
	2	기말고사	
	3		

5. 성적평가 방법

중간고사	기말고사	과제물	출결	기타	합계	비고
30 %	30 %	15 %	20 %	5 %	100 %	

6. 수업 방법(강의, 토론, 실습 등)

- 강의 위주
- 토론 및 일부 실습 포함

7. 수업에 특별히 참고하여야 할 사항

해당없음.

8. 문제해결 방법(실험·실습 등의 학습과정의 경우에 작성)

해당없음.