결재	전공주임	교학부장

수 업 계 획 서

< 2017학년도 8월 21일 ~ 12월 8일 >

1. 강의개요

학습과정명	암호학	학점	3	교강사명		교강사 전화번호	
강의시간	3	강 의 실		수강대상	정보보호	E-mail	

2. 교육과정 수업목표

- 암호의 개념을 이해한다.
- 정보시스템 내의 정보처리 및 축적 과정의 정보보호를 위한 암호 메커니즘을 이해한다.
- 정보시스템 간 정보전송 과정에서 발생할 수 있는 정보보호 알고리즘을 이해한다.
- 과제 실습을 통해 메커니즘 및 알고리즘의 적용 과정을 숙지한다.

3. 교재 및 참고문헌

주교재	IT 융합 보안의 길잡이 암호학	저자	양정모	출판사	경문사	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 2 3	1] 강의주제: 암호의 개요 2] 강의목표: 암호의 분류와 암호기술에 의한 정보보호 3] 세부내용: ① 암호의 정의 ② 암호 관련 용어 ③ 암호기술이 제공하는 것 ④ 암호의 역사 ⑤ 암호의 분류 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.2-13 강의교안
제 2 주	1 2 3	1] 강의주제: 고전암호 2] 강의목표: 고전암호의 원리 3] 세부내용: ① 전치암호기법 ② 치환암호기법 ③ 대입암호기법 ④ 곱암호 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.18-23 강의교안
제 3 주	1 2 3	1] 강의주제: 고전암호 2] 강의목표: 고전암호의 종류, 해독 3] 세부내용: ① 단순 대입암호 ② 동음이의 대입암호 ③ 플레이페어 암호 ④ 일회용패드 암호 ⑤ 암호 해독 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.24-59 강의교안
제 4 주	1	1] 강의주제: 정보이론 2] 강의목표: 완전비밀과 엔트로피, 거짓열쇠와 열쇠결정거리	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드

	2 3	3] 세부내용: ① 완전비밀 ② 엔트로피 ③ 거짓열쇠 ④ 열쇠결정거리 ⑤ 암호 시스템의 합성 4] 수업방법: 강의 및 토론(질의/응답)	학습자료 : 주:P.62-92 강의교안
제 5 주	1 2 3	1] 강의주제: 블록암호 2] 강의목표: DES 암호 3] 세부내용: ① DES의 구조 ② DES의 특성 ③ 3중DES ④ DES의 해독 ⑤ 선택된 평문공격 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.94-139 강의교안
제 6 주	1 2 3	1] 강의주제: 블록암호 2] 강의목표: 기타블록암호 3] 세부내용: ① SEED ② AES ③ FEAL ④ IDEA ⑤ 운영방식 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.140-170 강의교안 **[과제 : Report #1(용어 및 핵심정리)]**
제 7 주	1 2 3	1] 강의주제: 스트림암호와 선형점화수열 2] 강의목표: 스트림암호 3] 세부내용: ① 스트림암호 ② 스트림암호의 운영방식 ③ 스트림암호의 공격방법 ④ DES의 해독 ⑤ 선택된 평문공격 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.172-219 강의교안 **[수시평가]**
제 8 주	1 2 3	중 간 고 사	객관식 20점, 주관식 10점 (총 30점)
제 9 주	1 2 3	1] 강의주제: 공개열쇠암호 2] 강의목표: 공개열쇠암호 3] 세부내용: ① 열쇠배송문제 ② DES의 특성 ③ 공개열쇠암호 ④ RSA암호 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.222-226 강의교안
제 10 주	1 2 3	1] 강의주제: 공개열쇠암호 2] 강의목표: RSA암호 3] 세부내용: ① RSA암호 시스템 ② 이론적 배경 ③ 모듈라지수승 계산법 ④ RSA암호의 공격 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.227-273 강의교안
제 11 주	1 2	1] 강의주제: 기타 공개열쇠암호 2] 강의목표: 엘가말암호, 타원곡선암호, 하이브리드 암호 3] 세부내용: ① 엘가말 암호	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.276-312

	3	② 이산로그 문제 ③ 유한체와 타원곡선암호 ④ 하이브리드 암호 4] 수업방법: 강의 및 토론(질의/응답)	강의교안
제 12 주	1	1] 강의주제: 암호계의 응용 2] 강의목표: 서명기법, 해시함수 3] 세부내용: ① RSA 전자서명 ② 전자서명 표준 ③ 전자서명 공격 ④ 해시함수의 성질 ⑤ 해시함수의 공격 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.314-336 강의교안
	2		
	3		
제 13 주	1	1] 강의주제: 암호계의 응용 2] 강의목표: 열쇠분배와 공유, 메시지 인증코드, 3] 세부내용: ① 열쇠사전분배 ② 온라인 열쇠분배 ③ 디피헬만 열쇠교환 ④ 메시지 변경과 위장 ⑤ 메시지 인증 코드를 이용한 사례 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.337-366 강의교안 **[과제 : Report #2(연습문제풀이)]**
	2		
	3		
제 14 주	1	1] 강의주제: 암호계의 응용 2] 강의목표: 신원확인기법, 비밀분산 및 영지식 증명 3] 세부내용: ① 쉐노르 신원확인 기법 ② 오카모토 신원확인 기법 ③ 길로우와 퀴즈쿼터 신원확인 기법 ④ 비밀분산 ⑤ 영지식 증명 4] 수업방법: 강의 및 토론(질의/응답)	기자재: 실습용PC, 빔 프로젝터 스크린, 화이트보드 학습자료 : 주:P.367-398 강의교안
	2		
	3		
제 15 주	1	기 말 고 사	객관식 20점, 주관식 10점 (총 30점)
	2		
	3		

5. 성적평가 방법

중간고사	기말고사	과 제 물	출 결	기 타	합 계	비 고
30 %	30 %	15 %	20 %	5 %	100 %	

6. 수업 방법(강의, 토론, 실습 등)

강의 - 교재를 통한 이론 강의, 질의 및 응답 위주의 수업
토론 - 조별토론 및 문제풀이

7. 수업에 특별히 참고하여야 할 사항

8. 문제해결 방법(실험·실습 등의 학습과정의 경우에 작성)