# 2020학년도 1학기 수업계획서

**· 기본정보**

| | | | |
|---|---|---|---|
| 과목명 | 정보보호및암호학 | | |
| 학점(시간) | 3(3) | | |
| 이수구분 | 전공선택 | | |
| 수강번호 | 1641 | 반번호 | 01 |
| 강의시간 | | | |
| 강의실 | | | |
| 담당교수 | 이기동 | 소속 | 로봇기계공학과 |
| 면담시간 | 수 14:00~16:00 | | |

**· 과목 관련 정보**

| | |
|---|---|
| 동일과목 | |
| 선수과목 | |

**· 세부내용**

※선행과제 : 대수학의 기본 개념
프로그램밍(C 또는 Java) 테스트

1.강의소개 :
암호학의 핵심분야인 DES, 스트림 암호시스템, 공개키 암호시스템과 디지털 서명, 해쉬함수, 암호화 프로토콜, 네트웍 보호 등의 이론적인 측면과 실제 실습을 통하여 실용적인 측면을 보완한다.

2.수업목표 :
컴퓨터와 각종 전산망의 정보를 보호하기 위해서는 물리적인 접근을 통제하는 것으로부터 비밀번호의 다단계 이용, 컴퓨터 윤영체제의 강화 등 많은 방법이 있으나, 정보의 직접적인 보호가 가장 기본적이고 안전한 수단이며 또한 최후의 방법이다. 이러한 정보 보호의 가장 근원적인 방법에 대한 이해를 통하여, 향 후 각자의 전공분야에서 정보 보안에 대한 마인드 및 그 방법론을 인식하게 하고, 국가적인 정보 보안 인력 양성에 도움이 되고자 한다.

3.수업진행방법 :

강의는 주로 파워포인트 자료와 각종 멀티미디어 자료를 활용하며, 실습을 위한 프로그램을 제공한다.

※ 장애학생을 위한 학습지원 : 학습도우미(이동보조, 강의·보고서 대필, 학습보조), 보조기기, 휠체어 접근이 가능한 강의실, 좌석 우선배정, 점자, 확대자료 등이 필요한 수강자는 사전 문의 바랍니다.
(장애학생지원센터 : 053-810-1164)

**• 세부내용**

스마트교육:

4.중요교재 및 문헌 :
주교재 : 정보보호및암호학1, 이기동, 영냄대지방대특성화사업단
부교재 : 암호학과네트워크보안, 손승원 외, Mcgraw-Hill
기타 Power Point 자료

5.수업의 효율성 제고를 위한 기타사항 :
없음.

※ 장애학생의 요구가 있을 경우 장애유형에 따라 편의를 제공한다.
(장애학생지원센터 : 053-810-1164)

6.학습평가 :

본 강좌에서는 상대평가를 합니다. 그리고 제출한 과제물 및 시험에서 단 한 항목이라도 복사한 사실이 적발되면 학점을 받을 수 없으므로 주의하시기 바랍니다. 기한을 어긴 과제물은 점수를 받을 수 없습니다.

평가기준 : 중간고사 : 30%, 과제물 : 30%, 출석:10%, TermProject : 30%

※ 장애학생을 위한 평가지원 : 학습도우미(이동보조, 시험 대필), 점자, 음성 시험지, 확대 문제지, 시험시간 연장, 대필 도우미, 별도시험장소, 보조기기가 필요한 수강자는 사전 문의 바랍니다.
(장애학생지원센터 : 053-810-1164)

평가비율
중간시험 : 0%, 기말시험 : 0%, 출결 : 0%, 예·복습 : 0%, 기타 : 0%

※ 스마트교육: 학생의 수업 활동 참여에 대한 평가 권장
예: 수업참여도(발표, 토론, 학생 간 상호 평가), 포트폴리오 등

**• 주별계획**

| 주 | 학습목표 및 목차 | 주교재 및 참고자료 | 퀴즈/과제/토론 유무 |
|---|---|---|---|
| 1 | 암호학의 전체적인 개요 설명 | | 과제1: 다빈치코드 reading assignment |
| 2 | 단순대치법 등의 고전적인 암호화 기법 소개 | | |

• **주별계획**

| 주 | 학습목표 및 목차 | 주교재 및 참고자료 | 퀴즈/과제/토론 유무 |
|---|---|---|---|
| | | | |
| 3 | 기본적인 스트림 암호 시스템 설명(LFSR 등등) | | 과제2: 단순치환과제 |
| 4 | DES(data encryption standard) 설명 | | 과제3: DES 또는 AES프로그래밍 |
| 5 | 공개키 암호시스템 설명<br>(기본 원리, RSA 방식 등) | | |
| 6 | 현재 사용되고 있는 공개키 암호 시스템 설명 | | |
| 7 | 타원곡선 방식 | | |
| 8 | 전반기 정리 중간고사 | | |
| 9 | 디지탈서명과 인증 원리 설명 | | |
| 10 | RSA디지탈 서명,<br><br>ShamirID 방식의 디지탈서명 | | 과제4: 디지털인증 방식 프로그래밍 |
| 11 | OSS 디지털 서명<br>DSS | | |
| 12 | 다양한 해쉬함수 소개 | | |
| 13 | 암호화 프로토콜 및 네트워크 보호기술 소개 | | |
| 14 | 해킹의 기본 원리 설명, 현재 많이 사용되고 있는 해킹 방법 설명 | | 과제5: 해킹 실습과제 |
| 15 | 기말고사(Term project) | | 프로젝트 과제 발표 |