
보안프로그래밍

OT

숭실대학교 소프트웨어학부 조효진

수업 개요

- 소프트웨어 사회가 가속화되는 것과 더불어 정보보호를 통한 안전한 IT서비스가 필수적인 요소가 되어, 소프트웨어 전공자들은 반드시 정보보호를 기본적인 소양으로 갖추어야 한다. 본 교과목에서는 보안 프리티미브 (암호 기술, 암호 응용, 네트워크 보안) 관련 기초 지식 및 프로그래밍 능력에 대해 학습한다.

수업 개요

□ 참고교재

- Beginning Cryptography with Java/David Hook/Wrox press/2005
- 현대 암호학 (저자: 고려대학교 정보보호대학원 이동훈 교수님)
 - 비매품으로 구매가 불가능 함
 - 단, 교재를 원하는 학생들은 제본된 책을 원가에 구매 가능
 - 정보보호를 전공하는 대학원용 수업교재이므로 상황에 따라 학부 과정에 맞지 않는 내용들은 Skip할 예정
- 교재에 포함되지 않은 내용들은 강의교안으로 제공함

수업 계획

Week	Contents
1	보안 기본 개념
2	암호학적 해쉬 함수
3	대칭키 암호시스템 - 1
4	대칭키 암호시스템 - 2
5	메시지 인증코드
6	공개키 암호 시스템 - 1
7	공개키 암호 시스템 - 2
8	중간시험

수업 계획

Week	Contents
9	개체 인증
10	키 관리 시스템
11	네트워크 보안 – 1 (TLS)
12	네트워크 보안 – 2 (TLS)
13	네트워크 보안 – 3 (IPSec)
14	기타 응용 보안 기술 소개
15	기말 시험

*수업진행 상황에 따라 변동가능

성적 처리 절차

- 중간 시험 35%
- 기말 시험 35%
- 과제물 제출 20%
- 출석 및 수업태도 10%

과제 및 시험에서 윤리에 어긋나는 행동시에 0점 처리함 (Copy Killer 사용)
출석 미달 혹은 수업태도 불량 시, 학교 규정에 의거하여 F학점 부여

기타 사항

□ 강의 자료는 스마트캠퍼스에 업로드됨

□ 건의사항

- 온라인 혹은 대면 상담

□ 선수학습내용

- 자바 프로그래밍

Contacts

- Office: 정보과학관 624호
- E-mail: hyojin.jo@ssu.ac.kr

Thank you 