# 정보보호론

# 오리엔테이션

박 종 혁 교수

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

1절 교과목 소개

2절 평가 방법

3절 강의 계획

# 제1절 교과목 소개

## 1.1 담당교수 소개

## 1.2 교과목 소개

## 1.3 교과목 개요

## 1.4 학습 목표

## 1.5 수업 교재

# 1.1 담당교수 소개

## 박종혁교수 (Jong Hyuk Park)

- 최종학위: 공학박사 (전공-컴퓨터보안)
- 주 연구분야: 컴퓨터보안, 블록체인, IoT 및 클라우드 보안
- 연구실: 미래관 325호
- 홈페이지: http://www.parkjonghyuk.net

- 대표 약력

| 연도 | 기관명 | 업무 | 직위 |
|---|---|---|---|
| 2009.9 ~ 현재 | 서울과학기술대학교 컴퓨터공학과 | 교육 및 연구 | 교수 |
| 2002.12 ~ 2007.7 | 한화에스앤씨㈜ 기술연구소 | 선임연구원 | 연구 |
| 2011.1 ~ 현재 | 국제 HCIS 논문지 (SCIE, 세계 상위 15%) | 총괄편집위원장 | 편집위원장 |
| 2009.9 ~ 현재 | 한국정보처리학회 | 국제 및 저널 총괄 | 부회장 |

# 1.2 교과목 소개

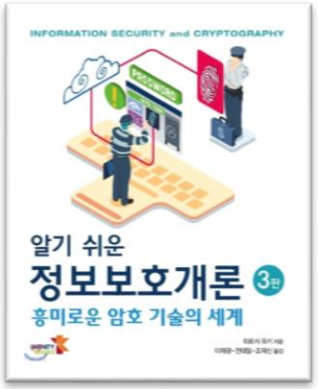
| | |
|---|---|
| **교과목 명** | 정보보호론 (Information Protection Theory) |
| **교과 구분** | 전공 선택 (3학점) |
| **강의 시간** | 월 2,3,4 교시 (미래관 109호) |
| **강의 구성** | 이론 (3) |
| **강의 방법** | 블랜디드 러닝 (비대면+대면) |

- 1~14주차: 대면 비대면 혼합
  (세부 스케쥴 일정표 참조 - 13, 14 ppt)
- 8 주차: 중간고사 (대면)
- 15 주차: 기말고사 (대면)
- 14 주차: 과제 2 발표 수업 (희망자 10명)

# 1.3 교과목 개요

- 정보 (Information)에 대한 훼손, 변조, 유출 등 공격 위협이 점차적으로 증가하고 있으며, 이를 방지하기 위한 대책이 필요함
- 최근 바이러스 및 악성코드 침투, 해킹 등 여러 가지 보안 이슈들이 사회적으로 자주 발생하고 있으며 이러한 보안 이슈들을 예방하기 위한 정보보호 기술이 필수적임
- 본 교과목에서는 정보보호의 개념과 기술 등 기본적인 이론부터 실생활에 필요한 응용기술까지 현대 암호와 함께 정보보호의 전반적인 이론 및 기초 지식에 대해 학습함

# 1.4 학습 교재




- 주교재

  알기 쉬운 정보보호 개론, 히로시 유키 지음 (이재광 외 2 공역), 인피니티북스, 2017

- 보조교재
  - 정보보안 원리 및 실습 (황성운 저, 생능출판, 2017. 11) 등 기타 정보보안 책
  - 최근 정보보호 이슈 사항, 컨퍼런스/워크숍 등 저명 학자/연구자 발표자료
  - 저명 저널 및 매거진 출판 논문
  - 인터넷 미디어 등





# 제2절 평가 방법 및 과제물

## 2.1 학습평가 방법

## 2.2 과제물 설명

# 2.1 학습평가 방법

- 출석 (10%), 과제물 (20%), 중간고사 (30%), 기말고사 (30%), 기타 (10%)*

* 기타: 수강생의 수업태도 (발표, 과제 등)에 대한 가산점 부여

# 2.2 과제물 설명

**과제 #1**

- 최신 암호응용 / 정보보호 관련 인터넷 및 자료조사 등을 통해 기술 동향 보고서 작성하여 기한 내 E-class에 업로드한다.

(8주차 중간고사 전일 23시 까지)

**과제 #2 :**

- 개인과제 #1을 기반으로 정보보호 아이디어 제안 보고서 및 발표 자료를 제작하여 기한 내 E-Class에 업로드 한다.

(14주차 수업 전일 23시 까지)

**기타 발표 :** (14주차 수업 시)

* 희망자 선착순 10명
  - 개인과제# 2 발표 (10분) ← 기타 점수 추가점 부여!!
  - 희망자는 조교선생님한테 3/20일까지 메일을 보내세요 (정보보호론 조교, jhpark.assistant@gmail.lcom)

# 과제 제출 관련 중요사항!!

도서관 표절 검사기 (Copykiller) 활용

– 각 과제 보고서를 도서관의 표절검사기로 유사율을 검사하여 함께 제출 해야 함 (유사율이 높을 경우, 표절로 판정함)

Copy Killer CAMPUS 서울과학기술대학교 https://seoultech.copykiller.com

- 최근 전세계적으로 문서(레포트, 논문 등)에 관한 유사도를 확인하고있며, 연구 윤리 측면에서 심각한 문제로 대두됨
- 우리 수업에서도 **표절률** 이용 감산제를 적용함

- 유사도 검사 결과 표절율이 30% 이상인 학생에게 패널티를 부여함
  – 과제점수 * 표절율 감점 적용

- 예) 과제점수 7점, 표절율 40%
  – 패널티 점수 =3점
  – 과제점수 (7) * 표절율 (40%) = 2.8 (3점 적용)
  – 최종 과제 점수 = 기본점수 (7) – 패널티 점수 (3점) = 4점

- 표절률이 60% 이상인 보고서는 완전 표절로 판단 "0점"을 부여함

# 제3절 강의 계획

## 3.1 주차별 강의 운용 계획

## 3.2 강의 내용 간단 소개

# 3.1 주차별 강의 운용 계획

| 주별 | 날짜 | 강의내용 | 강의방법, 과제, 평가내용 | 수업방식 |
|---|---|---|---|---|
| 1 | 2/21 | 오리엔테이션 및 교과목 개요<br>1장 정보보호 | 강의 개요 소개 및 이론강의 | 대면 강의 |
| 2 | 2/28 | 2장 암호의 세계 | 이론강의 | 온라인 동영상 강의 |
| 3 | 3/7 | 3장 암호의 역사 | 이론강의 | 온라인 동영상 강의 |
| 4 | 3/14 | 4장 대칭 암호 | 이론강의 | 온라인 동영상 강의 |
| 5 | 3/21 | 5장 블록 암호 모드 | 이론강의 | 대면 강의 |
| 6 | 3/28 | 6장 공개 키 암호 | 이론강의 | 온라인 동영상 강의 |
| 7 | 4/4 | 7장 하이브리드 암호 시스템 | 이론강의 및 과제1* | 온라인 동영상 강의 |
| 8 | 4/11 | 중간고사 | 필기시험<br>* 과제 1 제출기간: 당일 23시 | 대면 |

| 주별 | 날짜 | 강의내용 | 강의방법, 과제, 평가 내용 | 수업방식 |
|---|---|---|---|---|
| 9 | 4/18 | 8장 일방향 해시 함수 | 이론강의 | 온라인 동영상 강의 |
| 10 | 4/25 | 9장 메시지 인증 코드 | 이론강의 | 대면 강의 |
| 11 | 5/2 | 10장 디지털 서명 | 이론강의 및 과제2* | 대면 강의 |
| 12 | 5/9 | 11장 인증서 | 이론강의 | 대면 강의 |
| 13 | 5/16 | 12장 키<br>13장 난수 | 이론강의 | 대면 강의 |
| 14 | 5/23 | 1. 최신 정보보호 동향<br>2. 수강생 희망자 발표 | 이론강의<br>* 과제 2 제출기간: 전일 23시 | 대면 강의<br>(발표수업 포함) |
| 15 | 5/30 | 기말고사 | 필기시험 | 대면 |

# 3.2 강의 내용 간단 소개

## 1장. 정보보호

### 1절 네트워크 사회와 정보보호

### 2절 정보보호란?

### 3절 정보의 특성

### 4절 정보보호의 인적 요소

# 2장 암호의 세계

# 3장 암호의 역사

1절 시저 암호

2절 단일 치환 암호

3절 다중 치환 암호

4절 에니그마

5절 전치 암호와 치환 암호

6절 암호 알고리즘과 키

# 4장 대칭 암호

1절 문자 암호에서 비트열 암호로

2절 일회용 패드-절대 해독 불가능한 암호

3절 DES란?

4절 트리플 DES

5절 AES 선정 과정

6절 Rijndael

# 5장 대칭 암호(공통 키 암호)

1절 블록 암호 모드

2절 ECB 모드

3절 CBC 모드

4절 CFB 모드

5절 OFB 모드

6절 CTR 모드

7절 모드 선택

# 6장 공개 키 암호

1절 키 배송 문제

2절 공개 키 암호

3절 정수론

4절 RSA

5절 RSA에 대한 공격

6절 다른 공개키 암호

7절 공개 키 암호에 관한 Q&A

# 7장 하이브리드 암호 시스템

1절 하이브리드 암호 시스템

2절 강한 하이브리드 암호 시스템이란

3절 암호 기술의 조합

# 8장 일방향 해시 함수

1절 일방향 해시 함수

2절 일방향 해시 함수의 응용 예

3절 일방향 해시 함수의 예

4절 일방향 해시 함수 SHA-1

5절 일방향 해시 함수 SHA-512

6절 일방향 해시 함수에 대한 공격

7절 어떤 일방향 해시 함수를 사용하면 좋은가?

8절 일방향 해시 함수로 해결할 수 없는 문제

# 9장 메시지 인증 코드

1절 메시지 인증 코드

2절 메시지 인증 코드 이용 예

3절 메시지 인증 코드의 실현 방법

4절 인증암호

5절 HMAC

6절 메시지 인증 코드에 대한 공격

7절 메시지 인증 코드로 해결할 수 없는 문제

# 10장 디지털 서명

1절 디지털 서명

2절 디지털 서명 방법

3절 디지털 서명에 대한 의문

4절 디지털 서명 활용 예

5절 RSA에 의한 디지털 서명

6절 다른 디지털 서명

7절 디지털 서명에 대한 공격

8절 기타 기술과의 비교

9절 디지털 서명으로 해결할 수 없는 문제

# 11장 인증서

1절 인증서

2절 인증서 만들기

3절 공개 키 기반 구조 (PKI)

4절 인증서에 대한 공격

5절 인증서에 대한 Q&A

# 12장 키

1절 키란 무엇인가?

2절 다양한 키

3절 컨텐츠를 암호화하는 키와 키를 암호화 하는 키

4절 키 관리

5절 Diffie-Hellman 키 교환

6절 패스워드를 기초로 한 암호(PBE)

7절 안전한 패스워드를 만들려면

# 13장 난수

1절 난수가 사용되는 암호 기술

2절 난수의 성질

3절 의사난수 생성기

4절 구체적 의사난수 생성기

5절 의사난수 생성기에 대한 공격

# 16장 암호 기술과 현실 세계

1절 암호 기술의 정리

2절 완전한 암호 기술을 꿈꾸며

3절 완전한 암호 기술과 불완전한 인간

# Q & A

## Thank You!