2021학년도 제1학기 강의계획안

교과목명	암호론(Cryptography)	학수번호-분반	35294
개설전공	수학과	학점/시간	3/3
수업시간/강의실	월(14:00-15:15), 수(12:30-13:45) / 비대면 강의		
담당교원	이 향 숙	수학과	
	(E-mail) hsl@ewha.ac.kr	(연락처) 3277-2591	
면담시간/장소	이메일로 면담 예약: 온라인(Zoom)으로 진행		
담당조교	권 지 혜	(연구실) 종합과학관 A동 503호	
	(E-mail) jhkwon704@naver.com	(연락처) 3277-3392	

Ⅰ. 교과목 정보 Course Overview

1. 교과목 개요 Course Description

- 현대 인터넷 통신에서 중요한 정보보호의 핵심이 되는 암호 이론 및 응용에 대해 공부한다.
- 암호의 기본 개념과 성질, 공개키 암호시스템을 배우고, 관련된 수학 이론과 응용을 학습한다.
- 특히, 소인수분해 문제에 기반한 RSA, 이산대수 문제에 기반한 ECC(타원곡선암호) 등의 공개키 암호와 성질, 그리고 Lattice 개념 및 Lattice 기반 암호 등 현대암호 동향에 대해서 공부한다.
- 암호의 핵심 기술을 이루는 알고리즘을 수학 이론에 근거하여 소개한다.

2. 선수학습사항 Prerequisites

3. 강의방식 Course Format

강의 Lecture	발표/토론 Discussion/Presentation	실험/실습 Experiment/Practicum	현장실습 Field Study	기타 Other
100 %	%	%		%

4. 교과목표 Course Objectives

- 암호론의 기본 개념과 성질, 암호에 사용되는 다양한 수학 이론과 응용을 학습한다.
- 고전암호 및 현대암호를 이해하고 차세대 암호의 동향을 이해한다.
- 수학 이론에 기반한 암호기법을 습득하고 구현한다.
- 공개키 암호체계가 현대 인터넷 및 네트워크 등 실생활에서 중요한 역할을 하고 있음을 이해한다.

5. 학습평가방식 Evaluation System

☐ 상대평가(Relative evaluation) ☒ **절대평가(Absolute evaluation)** ☐ 기타(Others): _____

- 평가방식 설명 (explanation of evaluation system)

- 상대평가에 기반한 자율 평가
- 결석 1/3 이상: 학점 F (학칙에 의함)
- 특별한 사유가 아닌 한 재시는 불허

중간고사 Midterm Exam	기말고사 Final Exam	퀴즈 Quizzes	발표 Presentation	프로젝트 Projects	과제물 Assignments	참여도 Participation	기타 Other
40 %	45 %	%	%	%	10 %	5 %	%

*그룹 프로젝트 수행 시 팀원평가(PEER EVALUATION)이 평가항목에 포함됨. Evaluation of group projects may include peer evaluations.

Ⅱ. 교재 및 참고문헌 Course Materials and Additional Readings

1. 주교재 Required Materials

- 교재명: An Introduction to Mathematical Cryptography
- 저자명: J. Hoffstein, J. Piper and J. H. Silverman
- 출판사명: Springer Verlag

2. 부교재 Supplementary Materials

3. 참고문헌 Optional Additional Readings

- 기타 암호 관련 서적 및 인터넷 자료

Ⅲ. 수업운영규정 Course Policies

* 실험, 실습실 진행 교과목 수강생은 본교에서 진행되는 법정 '실험실안전교육(온라인과정)' 을 필수로 이수하여야 함.
* For laboratory courses, all students are required to complete lab safety training.

Ⅳ. 차시별 강의계획 Course Schedule (최소 15주차 강의)

* 아래 강의계획안은 수업 진행시 상황에 따라 진도 일정이 변경될 수 있습니다.

주차	날짜	주요강의내용 및 자료, 과제(Topics & Class Materials, Assignments)
1주차	3월 3일 (수요일)	Chapter 1. An Introduction to Cryptography - An Introduction to cryptography
	3월 8일 (월요일)	- Mathematical Background : Modular arithmetic etc. - Fast powering exponentiation
2주차	3월 10일 (수요일)	Chapter 2. Discrete Logarithm and Diffie-Hellman - Complexity of Computation
	3월 15일 (월요일)	- Public Key Cryptography(PKC)
3주차	3월 17일 (수요일)	- Discrete Log Problem/Diffie-Hellman key exchange - A overview of the theory of groups
	3월 22일 (월요일)	- ElGamal PKC
4주차	3월 24일 (수요일)	- A collision algorithm for the DLP: Baby step & Giant step - The Chinese remainder theorem
	3월 29일 (월요일)	- The Pohlig-Hellman algorithm
5주차	3월 31일 (수요일)	- Ring, polynomials and finite fields
	4월 5일 (월요일)	Chapter 3. Integer Factorization and RSA - RSA cryptosystem
6주차	4월 7일 (수요일)	- Implementation and security issues
	4월 12일 (월요일)	- Primality testing, Factoring
7주차	4월 14일 (수요일)	- Factorization algorithm(Pollard p-1)
	4월 19일 (월요일)	- Factorization algorithm
8주차	4월 21일 (수요일)	- **중간고사(오후 6시 30분 - 8시 30분)**
	4월 26일 (월요일)	- Factorization algorithm(difference of squares)
9주차	4월 28일 (수요일)	- Index Calculus Method
	5월 3일 (월요일)	- Quadratic residues and quadratic reciprocity
10주차	5월 5일 (수요일)	- Quadratic Sieve Factorization, Probabilistic encryption
	5월 10일 (월요일)	Chapter 4. Combinatorics, Probability, and Information Theory - Probability theory
11주차	5월 12일 (수요일)	- Collision algorithms, Birthday paradox
	5월 17일 (월요일)	- Perfect Secrecy
12주차	5월 19일 (수요일)	Chapter 5. Elliptic Curve Cryptography - Elliptic curves
	5월 24일 (월요일)	- Elliptic curves over finite fields
13주차	5월 26일 (수요일)	- The Elliptic Curve Discrete Log Problem
	5월 31일 (월요일)	- Elliptic Curve Cryptography
14주차	6월 2일 (수요일)	- Lenstra' s elliptic curve factorization algorithm
	6월 7일 (월요일)	Chapter 6. Lattices and Cryptography - A congruential public key cryptography
15주차	6월 9일 (수요일)	- Lattices: definitions and properties
	6월 14일 (월요일)	- **학기말고사(오후 6시 30분 - 8시 30분)**

※ 강의 진도는 수업 진행 상황에 따라 일부 차이가 있을 수 있음

Ⅴ. 참고사항 Special Accommodations

* 장애학생은 학칙 제57조의3에 따라, 학기 첫 주에 교과목 담당교수와의 면담을 통해 출석, 강의, 과제 및 시험에 관한 교수학습지원 사항을 요청할 수 있으며, 요청한 사항에 대해 담당교수 또는 장애학생지원센터를 통해 지원받을 수 있습니다. 강의, 과제 및 평가 부분에 있어 가능한 지원 유형의 예는 아래와 같습니다.

강의 관련	과제 관련	평가 관련
· 시각장애 : 점자, 확대자료 제공 · 청각장애 : 대필도우미 배치 · 지체장애 : 휠체어 접근이 가능한 강의실 제공, 대필도우미 배치	제출일 연장, 대체과제 제공	· 시각장애 : 점자, 음성 시험지 제공, 시험시간 연장, 대필도우미 배치 · 청각장애 : 구술시험은 서면평가로 실시 · 지체장애 : 시험시간 연장, 대필도우미 배치

- 실제 지원 내용은 강의 특성에 따라 달라질 수 있습니다.

* According to the University regulation section #57-3, students with disabilities can request for special accommodations related to attendance, lectures, assignments, or tests by contacting the course professor at the beginning of semester. Based on the nature of the students' request, students can receive support for such accommodations from the course professor or from the Support Center for Students with Disabilities (SCSD). Please refer to the below exam

ples of the types of support available in the lectures, assignments, and evaluations.

Lecture	Assignments	Evaluation
. Visual impairment : braille, enlarged reading materials . Hearing impairment : note-taking assistant . Physical impairment : access to classroom, note-taking assistant	Extra days for submission, alternative assignments	. Visual impairment : braille examination paper, examination with voice support, longer examination hours, note-taking assistant . Hearing impairment : written examination instead of oral . Physical impairment : longer examination hours, note-taking assistant

- Actual support may vary depending on the course.

Ⅵ. 조교

조교	(성명) 권지혜 (연구실) 종합과학관 A동 503호 (전화) 3277-3392 (이메일) jhkwon704@naver.com