수 업 계 획 서

(2023학년도 1학기)

단과대학	과학기술대학	배정학과	정보보안암호수학과
과목명	공개키암호	교과목코드-분반	1395700-01
학점/시간	3.0 / 3.0	이수학년	3-4
수업시간	목 1A,1B,2A,2B,3A,3B(09:00~12:00)	강의실	과학관 과학관3층12호실
외국어 강의		평가유형	상대평가
선수과목	Number Theory, Abstract Algebra (Recommended)		
면담시간 (office hour)	THU. 13:00 ~ 15:00	강좌홈페이지	

담당교수	성 명 : 김동찬	연락처	전 화 : 02-910-4735
	연구실 : 생활관 D동 508호		E - mail : dckim@kookmin.ac.kr
			홈페이지 : https://sites.google.com/kookmin.ac.kr/fdl

담당조교	성 명 :	연락처	전 화 :
			E - mail :
첨부파일		동영상첨부파일	

키워드	Public Key Cryptography	Integer Factorization	Discrete Logarithm Problem	RSA

대상 및 공적가치

대상#1 : 노인	대상#2 : 장애인	대상#3 : 청소년	대상#4 : 어린이/유아
☐ 건강	☐ 건강	☐ 건강	☐ 건강
☐ 안전	☐ 안전	☐ 안전	☐ 안전
☐ 균등한기회	☐ 균등한기회	☐ 균등한기회	☐ 접근성
☐ 접근성	☐ 접근성	☑ 교육	☑ 교육
☑ (정보보안)	☐ 교육	☑ (정보보안)	☑ (정보보안)
☐	☑ (정보보안)	☐	☐

대상#5 : 여성	대상#6 : 관리자	대상#7 : 대중/시민/고객
☐ 건강	☑ 의사결정	☐ 건강
☐ 안전	☑ 효율성	☐ 안전
☐ 균등한기회	☐ 윤리	☐ 균등한기회
☑ 교육	☐ 사회적책임	☐ 환경(대상)
☑ (정보보안)	☐ 성과역량	☑ 프라이버시
☐	☑ 분석역량	☑ 경제적가치
☐	☑ (정보보안)	☐ 경험적가치
☐	☐	☑ 신뢰
☐	☐	☑ (정보보안)

기술구분(6T)

☐	BT-바이오기술	☑	IT-정보기술	☐	ET-환경기술	☐	NT-나노기술
☐	ST-우주항공기술	☐	CT-문화기술	☐	기타(직접입력)		

경제사회목적별 구분

☐	지구개발및탐사	☐	환경	☐	우주개발및탐사
☐	교통,전기통신 등 기반시설	☐	에너지	☐	건강
☐	농업(공적)	☐	문화,휴양,종교및매스미디어	☐	교육
☐	정치, 사회시스템, 구조 및 과정	☐	국방	☐	섬유,의복 및 가죽
☐	목재,종이 및 인쇄	☐	화학물질 및 화학제품	☐	의료용 물질 및 의약품
☐	비금광석 및 금속제품	☑	전자부품, 컴퓨터, 영상, 음향 및 통신장비	☐	의료,정밀,광학기기 및 시계
☐	전기장비 및 기계장비	☐	자동차 및 운송장비	☑	지식의 일반적 진보

1. 교과목 개요

We cover the following components in this course:
- Security Notion for Public Key Cryptography
- Integer Factorization/Discrete Logarithm Problems and Their Applications
- Elliptic Curve Cryptography
- Post-Quantum Cryptography

2. 수업목표

To familiarize the students with public key cryptography and its usage

3. 국민핵심역량

인문역량	소통역량	글로별역량	창의역량	전문역량
0%	0%	0%	0%	100%

- 인문역량(역사지식, 윤리지식, 문화적 감성, 봉사정신): 도덕성과 문화적 소양을 기반으로 올바른 역사관을 수립하고 봉사를 실천하는 능력
- 소통역량(소통능력, 협동심, 책임감): 적절한 매체를 활용하여 자신의 생각을 전달하고 타인과 공감함으로써 공동체 속에서 협력하여 결과를 도출하는 능력
- 글로벌역량(자기주도성, 도전정신, 글로벌감각, 외국어능력): 글로벌 환경 속에서 자기 정체성과 주도성을 바탕으로 외국어 능력을 배양하고 문화적 다양성을 수용하는 능력
- 창의역량(창의성, 비판적 사고력, 문제해결력): 현상을 비판적으로 분석하고, 발견된 문제를 다양한 시각에서 해결하는 능력
- 전문역량(전공지식, 융합사고력): 깊이 있는 전공지식을 습득하여 다양한 분야에 적용할 수 있는 융합적 사고 능력

4. 선수학습내용

Number Theory, Abstract Algebra (Recommended)

5. 수업방법

강의	토론/토의	실험/실습	현장실습	발표	창작	기타
☑	☑	☑	☐	☑	☐	☐
비고						

6. 평가방법

시험			수행과제			참여		기타	합계
중간고사	기말고사	퀴즈	프로젝트	과제물	발표	출석	수업참여도		
30%	30%	5%		10%		5%	20%		100%
비고									

7. 수행과제

과제유형코드	과제명	제출기한설명
비고		

8. 교재

구분	도서명	저자	출판사	발행년도	ISBN
주교재	Cryptography Made Simple	Nigel P. Smart	Springer	2016	978-3-319-21935-6
부교재	A Course in Number Theory and Cryptography	Neal Koblitz	Springer	1994	978-0387942933
부교재	An Introduction to Mathematical Cryptography	Hoffstein, Jeffrey, Pipher, Jill,	Springer	2010	1441926747
부교재	FIPS PUB. 186-4, Digital Signature Standard (DSS)	NIST		2013	
부교재	PKCS #1: RSA Cryptography Specifications Version 2.2	IETF		2016	
비고					

9. 수업규정 또는 안내사항

주차별 수업계획(Course Schedule)

1주차	2023-03-02	수업내용	Public Key Cryptography in a Nutshell: Classification and Security Notions	비고	PKE, Signature, Key Establishment, Onewayness Trapdoor, IND-CCA, EUF-CMA, etc.
2주차	2023-03-09	수업내용	IFP-based Primitives	비고	Textbook RSA, RSA-CRT, Fermat's Little Theorem, Euler's Theorem, Primality Test, EEA, CRT, etc.
3주차	2023-03-16	수업내용	IFP-based Schemes	비고	RSA-OAEP, RSA-PSS, Random Oracle Model, etc.
4주차	2023-03-23	수업내용	How to Implement IFP-based Schemes Part 1	비고	Integer Multiplication, Division, (Modular) Exponentiation, etc.

5주차	2023-03-30	수업내용	How to Implement IFP-based Schemes Part 2	비고	Barrett Reduction, Montgomery Reduction, etc.
6주차	2023-04-06	수업내용	How to Solve IFP Part 1	비고	Pollard' s p-1 method, Pollard' s rho method, Birthday Bound, Floyd's Cycle Detection, etc.
7주차	2023-04-13	수업내용	How to Solve IFP Part 2	비고	Quadratic Residue mod p (Legendre symbol), Square Roots modulo p, QNFS, GNFS, etc.
8주차	2023-04-20	수업내용	Midterm Exam.	비고	
9주차	2023-04-27	수업내용	DLP-based Schemes	비고	DH, DSA, KCDSA, etc.
10주차	2023-05-04	수업내용	How to Solve DLP Part 1	비고	Baby-Step/Giant-Step Algorithm, Pollard' s rho method, etc.
11주차	2023-05-11	수업내용	How to Solve DLP Part 2	비고	Pohlig-Hellman Algorithm, Index Calculus Method, etc.
12주차	2023-05-18	수업내용	Elliptic Curve Cryptography Part 1	비고	Projective Space, Elliptic Curve, Elliptic Curve Group, ECDH, ECDSA, EC-KCDSA, etc.
13주차	2023-05-25	수업내용	Elliptic Curve Cryptography Part 2	비고	Addition, Doubling, NIST Curves, Curve25519, etc.
14주차	2023-06-01	수업내용	Post-Quantum Cryptography	비고	Lattice-based Schemes, Code-based Schemes, NIST PQC, KpqC, etc.
15주차	2023-06-08	수업내용	Final Exam.	비고	

수업관련 제반 안내사항

1. 수업일수는 매학기 15주이상으로 하며 수업일수의 1/4 이상을 결석할 시는 당해 학기의 성적을 부여하지 않습니다.(학칙 제9조 및 학사규정 제63조 1항)

2. 상대평가의 등급 분포비율
   가. 상대평가 (이론시간이 있는 강좌 중 상대평가 대상인원이 10명 이상인 강좌) :
   A등급(A+・A0)은 35% 이내, A등급(A+・A0)과 B등급(B+・B0)의 합은 80%이내, C+이하 제한 없음
   나. 상대평가II (이론시간이 있는 강좌 중 상대평가 대상인원이 10명 미만인 강좌, 이론시간이 없는 실험실습 및 실기강좌, 원어강좌) : A등급(A+・A0)은 45% 이내, A등급(A+・A0)과 B등급(B+・B0)의 합은 90%이내, C+이하 제한 없음
   다. 절대평가 : P/N 평가 교과목
※ 평가방법은 수강학생의 학적변동에 따라 변동될 수 있습니다.

3. 재수강의 경우 취득할 수 있는 최고성적은 A0까지이며 "2015학번" 부터는 B+로 제한됨
   ※ 재수강 후 성적이 재수강전 성적보다 낮아도 재수강 후 성적으로 반영됨

4. 시험부정 행위, 기타 부정한 방법(예, 표절)으로 취득한 과목의 성적은 취소처리 됩니다.(학사규정 제65조)

5. 실험/실습 교과목의 경우 수업 진행 전 안전교육이 실시됩니다.

6. 장애학생지원센터 운영규정 제4조에 의거하여, 장애학생은 학기 시작 전후에 교과목 담당교수 또는 장애학생지원센터와의 면담을 통해 출석, 강의, 과제 및 시험에 관한 교수학습지원 사항을 요청할 수 있으며, 요청한 사항에 대해 지원을 받을 수 있습니다.

● 장애학생지원센터 : 종합복지관 411호, 02-910-5001,5002

[강의]

- 시각장애 : 대필 도우미, 녹음기, 점자 및 스캔도서 제작
- 지체장애 : 대필 도우미 및 수업보조 도우미, 지정좌석 배정
- 청각장애 : 대필 도우미, 강의 녹취 허용
- 지적장애/자폐성장애 : 대필 도우미 및 수업보조 도우미

[과제 및 시험]

- 시각장애/지체장애/청각장애 : 과제 제출 기한 연장, 과제 및 제출방식 조정, 시험시간 연장 등
- 지적장애/자폐성장애 : 개별화 과제 제출 및 대체 평가 실시 검토

● 실제 지원 내용은 강의 특성에 따라 달라질 수 있습니다.

7. 수업과제 제출 시 표절예방시스템(Copy Killer)검증 결과 제출 상용화

- 사용방법 : 도서관 홈페이지 오른쪽 상단[표절예방시스템]접속 후 로그인