

수학과

(Dept. of Mathematics)

설치 과정 : 석사과정, 박사과정, 석·박사통합과정

학과 소개

수학과에서는 지식기반 산업이 확대되고 수학의 역할이 증대됨에 따라 새로운 이론을 정립하고 응용할 수 있는 학문적 경쟁력을 갖춘 전문 수학인을 양성하기 위하여 이론분야와 응용분야의 교과목을 균형 있게 개설하고 있다. 국가 경쟁력 강화를 위하여 필수적이고 과학기술의 기본이 되는 수학적 이론을 다루고 수학적 사고를 표현 할 수 있도록 지도한다. 석사과정에서는 기본적인 과목과 전공 분야 및 그 응용을 폭넓게 다루어 박사과정 진학이나 취업의 기회를 넓혀 주며, 박사과정에서는 전공에 대한 깊은 지식과 우수한 논문을 작성할 수 있게 하여 경쟁력 있는 수학인을 배출하고자 한다.

교육 목표

수학과는 학부과정에서 다진 수학 전반에 대한 기초를 토대로 보다 깊이 있는 수학적 사고를 경험하게 하여 수학에 대한 학문적 연구를 수행할 수 있도록 지도하며, 대수학, 해석학, 기하학, 위상수학, 통계학, 응용수학, 암호학 등 수학의 제 분야를 다루어 수학 전문인으로서의 자질과 학자로서의 손색없는 인격을 갖추도록 하는데 목표를 둔다.

전공 분야

분 야	개 요
수학 전공 (Mathematics Major)	학문적 연구를 위한 이론과 응용 능력을 겸비한 수학전문인의 자질을 갖추도록 함
정보보안 전공 (Information Security Major)	수학 전문 지식을 기반으로 한 암호학 및 정보보안 분야의 이론과 실용적 능력을 겸비한 정보보안 전문 인력을 양성함

학과 운영내규

1. 선수과목

- 1) 타 계열 출신 석사과정과 박사과정 학생의 선수과목은 주임교수 및 지도교수가 필요하다고 인정할 때 지정할 수 있다.

대상	구분	교 과 목 명	학 점
석사 / 박사	학부과목	선형대수학	3
		수리통계학	3
		해석학	3
		조합및그래프이론	3
		기초프로그래밍	2

- 2) 출신 대학에서 이미 이수한 과목이 있는 경우, 학과 주임교수의 승인을 받아 이를 면제받을 수 있다. 출신대학에 따라 과목명이 상이하므로, 동일한 교과내용으로서 과목명이 다른 경우에는 학과 주임교수의 승인을 받아 이를 이미 이수한 것으로 인정받을 수 있다.

2. 외국어시험

- 1) 외국어시험의 응시자격 및 응시절차는 대학원 학칙 및 대학원 학사운영규정에 준한다.
- 2) 박사과정은 제2외국어 시험을 실시하지 않는다.

3. 종합시험

- 1) 종합시험의 응시자격 및 응시절차는 대학원 학칙 및 대학원 학사운영규정에 준한다.
- 2) 종합시험은 석사과정 2과목, 박사과정 3과목으로 한다.

4. 학위청구논문

- 1) 논문계획서는 지도교수의 확인을 받아 석사과정은 3차 학기 개강 1주내, 박사과정은 4차학기 개강 1주내에 주임교수에게 제출하여야 한다.
- 2) 본심사 직전 학기말까지 논문지도 평가를 통과(pass)하여야 한다.
- 3) 석사과정은 논문예비심사를 실시하지 않는다.
- 4) 박사과정에 대한 논문예비심사는 본 심사 학기 초까지 실시하며, 예비심사용 논문원고를 심사일 2주 전에 주임교수에게 제출하여 예비심사위원회에 전달되도록 해야 한다.
- 5) 심사용 학위청구논문의 제출기한은 전기에 졸업하고자 하는 대학원생은 10월 초까지, 후기에 졸업하고자 하는 대학원생은 4월 초까지 제출하여야 한다. 기간 내 제출하지 않은 논문은 심사에서 제외한다.
- 6) 논문심사는 석사과정은 2회, 박사과정은 3회를 실시하며, 논문심사 날짜는 지도교수가 심사위원과 협의하여 정한다. 논문은 각 심사일 2주 전에 심사위원에게 제출하여야 한다.

부 칙

- 이 내규는 2003년 3월 1일부터 시행한다.
 이 변경 내규는 2005년 3월 1일부터 시행한다.
 이 변경 내규는 2019년 3월 1일부터 시행한다.

교과과정표

◦ 전공 공통(Core Courses)

교 과 목		학점	강의	실습	수강대상
현대대수학	(Modern Algebra)	3	3	0	석·박사 공통
실함수론	(Real Function Theory)	3	3	0	
기초위상수학	(Basic Topology)	3	3	0	
기하학기초론	(Foundations of Geometry)	3	3	0	
수리통계학	(Mathematical Statistics)	3	3	0	
응용수학개론	(Introduction to Applied Mathematics)	3	3	0	
정보보호개론	(Introduction to Information Security)	3	3	0	
현대대수학특강	(Topics in Modern Algebra)	3	3	0	
실해석학	(Real Analysis)	3	3	0	
현대미분기하학	(Modern Differential Geometry)	3	3	0	
일반위상수학	(General Topology)	3	3	0	
통계확률특강	(Topics in Statistics and Probability)	3	3	0	
연구윤리및논문연구	(Research Ethics & Thesis Study)	3	3	0	

◦ 수학 전공(Mathematics Major Courses)

교 과 목		학점	강의	실습	수강대상
확률과정론	(Probability Theory)	3	3	0	석·박사 공통
추상대수학특강	(Topics in Abstract Algebra)	3	3	0	
함수해석학	(Functional Analysis)	3	3	0	
위상수학	(Topology)	3	3	0	
보험수리학	(Actuarial Mathematics)	3	3	0	
금융수학특강	(Topics in Financial Mathematics)	3	3	0	
위상기하학	(Topological Geometry)	3	3	0	
위상수학특강	(Topics in Topology)	3	3	0	
미분기하학	(Differential Geometry)	3	3	0	
미분가능다양체	(Differentiable Manifolds)	3	3	0	
기하학특강	(Topics in Geometry)	3	3	0	
다변량해석	(Multivariate Statistical Analysis)	3	3	0	
확률론	(Theory of Probability)	3	3	0	
수치해석특강	(Topics in Numerical Analysis)	3	3	0	
응용미분방정식	(Applied Differential Equations)	3	3	0	
과학계산론특강	(Topics in Scientific Computations)	3	3	0	
체론	(Theory of Field)	3	3	0	
가환대수	(Commutative Algebra)	3	3	0	
대수적정수론	(Algebraic Number Theory)	3	3	0	
군표현론	(Group Representation Theory)	3	3	0	
고급대수학	(Advanced Algebra)	3	3	0	
복소해석학	(Complex Analysis)	3	3	0	
편미분방정식	(Partial Differential Equations)	3	3	0	
위상벡터공간론	(Topological Vector Space)	3	3	0	
작용소이론	(Operator Theory)	3	3	0	
역문제개론	(Introduction to Inverse Problems)	3	3	0	
역문제특강	(Topics in Inverse Problems)	3	3	0	
미분기하학요해	(Elements of Differential Geometry)	3	3	0	
부분다양체론	(Submanifold Theory)	3	3	0	
미분다양체론	(Differential Manifolds)	3	3	0	
리만기하학	(Riemannian Geometry)	3	3	0	
미분기하학특강	(Topics in Differential Geometry)	3	3	0	
미분위상기하학	(Differential Topological Geometry)	3	3	0	

교 과 목		학점	강의	실습	수강대상
대수적위상수학	(Algebraic Topology)	3	3	0	석·박사 공통
호모로지론	(Homology Theory)	3	3	0	
호모토피론	(Homotopy Theory)	3	3	0	
미분위상수학	(Differential Topology)	3	3	0	
퍼지위상수학	(Fuzzy Topology)	3	3	0	
이산분포론	(Theory of Discrete Distribution)	3	3	0	
비모수통계학	(Nonparametric Statistics)	3	3	0	
시계열분석	(Analysis of Time Series)	3	3	0	
회귀분석	(Analysis of Regression)	3	3	0	
통계적결정론	(Statistical Decision Theory)	3	3	0	
자료분석과통계실습	(Data Analysis and Statistics Laboratory)	3	3	0	
미분방정식의수치해법	(Numerical Methods for Differential Equations)	3	3	0	
유한차분법	(Finite Difference Methods)	3	3	0	
영상처리개론	(Introduction to Image Processing)	3	3	0	
전산유체역학	(Computational Fluid Dynamics)	3	3	0	
혼돈과역학계	(Chaos and Dynamical Systems)	3	3	0	
수리모형특강	(Topics in Mathematical Models)	3	3	0	
유한요소법	(Finite Element Methods)	3	3	0	
옵션가격결정론	(Option Pricing)	3	3	0	
수학적계산모델	(Mathematical Models for Computation)	3	3	0	
큐잉이론	(Queueing Theory)	3	3	0	

◦ 정보보안 전공(Information Security Major Courses)

교 과 목		학점	강의	실습	수강대상
암호수학	(Cryptomathematics)	3	3	0	석·박사 공통
암호알고리즘	(Crypto-Algorithms)	3	3	0	
고급암호알고리즘	(Advanced Crypto-Algorithms)	3	3	0	
정보의논리	(Logic of Information Flow)	3	3	0	
정보수학특강	(Mathematics and Information)	3	3	0	
정보보호프로토콜	(Information Security Protocol)	3	3	0	
키관리시스템	(Key Management System)	3	3	0	
전자상거래	(Electronic Commerce Security)	3	3	0	
해쉬함수와데이터인증	(Hash Function and Message Authentication)	3	3	0	
공개키암호분석이론	(Cryptanalysis of Public-key Cryptosystem)	3	3	0	
복잡도와알고리즘	(Complexity and Algorithms)	3	3	0	
증명가능안전성론	(Provable Security)	3	3	0	
스테가노그래피및응용	(Steganography and its Applications)	3	3	0	
네트워크보안	(Networks Security)	3	3	0	
금융보안론	(Financial Information Security)	3	3	0	
대칭키암호분석	(Topics in Symmetric Key Cryptanalysis)	3	3	0	
암호소프트웨어구현	(Implementation of Cryptographic S/W)	3	3	0	
암호하드웨어구현	(Implementation of Cryptographic H/W)	3	3	0	
암호모듈평가및검증	(Evaluation and Validation of Cryptographic Module)	3	3	0	
병렬암호구현	(Implementation of Parallel Cryptography)	3	3	0	
이동통신보안	(Mobile Security)	3	3	0	
무선보안특강	(Wireless Security)	3	3	0	
융합보안특강	(IT Convergence and Security)	3	3	0	
스마트그리드보안	(Smartgrid Security)	3	3	0	
인터넷보안	(Internet Security)	3	3	0	
부채널공격론	(Side Channel Attacks)	3	3	0	
부채널공격대응론	(Countermeasures of Side Channel Attacks)	3	3	0	
다자간계산론	(Secure Multiparty Computation)	3	3	0	
의사난수성론	(Pseudorandomness)	3	3	0	

교과목 개요

수학과는 수학분야의 전문적 학자를 양성하는데 그 목적이 있다. 전공은 크게 대수학, 해석학, 위상수학, 기하학, 확률, 통계, 전산, 응용수학 분야로 나누어져 있으며 순수수학과 응용수학이 유기적 관계를 갖도록 하고 폭넓은 지식을 습득하고 각 분야별 전문학자를 양성할 수 있도록 교과목이 설정되어 있다.

◦ 전공 공통(Core Courses)

- **현대대수학(Modern Algebra)**
군, 환, 체, 가군, 벡터공간 등에 관한 기본적인 대수적 구조와 Category, Functor 기본개념 등을 다룬다.
- **실함수론(Real Function Theory)**
1차원 실수 공간에서의 Lebesgue 측도, 적분과 미분, Riesz Representation 이론, Regular 측도의 존재성, 단일성 등을 다룬다.
- **기초위상수학(Basic Topology)**
위상수학의 기초개념을 통하여 위상공간의 일반적 성질 즉, 연결성, 분리성, Compact 성 및 완비성 등을 연구한다.
- **기하학기초론(Foundations of Geometry)**
유클리드 3차원 기하학의 전반에 걸친 기초지식을 다룬다.
- **수리통계학(Mathematical Statistics)**
확률변수의 함수분포, 추정, 통계학가설, 통계적검정, 비모수통계적 방법 등을 다룬다.
- **응용수학개론(Introduction to Applied Mathematics)**
수학적 방법이 적용되는 다양한 문제의 해결 방법을 구성하고 적용하기 위한 수학적 이론의 응용을 다룬다.
- **정보보호개론(Introduction to Information Security)**
정보보호와 관련된 비밀키 암호, 공개키 암호, 해쉬 함수, 전자 서명, 정보보호 프로토콜, 키 관리 등에 관련된 기본 개념을 학습한다.
- **현대대수학특강(Topics in Modern Algebra)**
군, 환, 체, 가군 등 현대대수학의 기본적이고 중심적인 내용을 다룬다.
- **실해석학(Real Analysis)**
1차원 실수 공간에서의 Lebesgue 측도, 적분과 미분, Banach 공간, 함수공간, 범함수론, 일반추상 공간에서의 적분과 측도 등을 다룬다.
- **현대미분기하학(Modern Differential Geometry)**
텐서해석, 현대미분기하학의 개론과 곡면의 위상적 성질 및 기하학적 성질을 다룬다.
- **일반위상수학(General Topology)**
위상공간의 공리, 곱공간, 연속함수, 분리공간, 연결성, 동일화 위상, 약위상, 콤팩트성, 함수공간 수렴성과 완비성 등의 연구를 통하여 위상의 기본적인 측면에 익숙하여 타 분야의 응용이 될 수 있도록 준비한다.

- 통계확률특강(Topics in Statistics and Probability)
통계 및 확률 전반에 관한 Topic을 중심으로 세미나를 한다.

◦ 수학 전공(Mathematics Major Courses)

- 확률과정론(Probability Theory)
조건부확률, 확률과정의 개념, 극한행위, Markov연쇄, Markov과정 등을 다룬다.
- 추상대수학특강(Topics in Abstract Algebra)
대수학 전반에 걸쳐서 특별한 문제를 중심으로 기본적인 대수적 구조에서부터 특수한 내용까지를 다룬다.
- 함수해석학(Funtional Analysis)
위상선형공간, Banach–Steinhaus의 정리, Open Mapping 정리, Closed Graph 정리, Hahn–Banach 정리, Banach 공간에서의 쌍대성 등을 연구한다.
- 위상수학(Topology)
Homotopy 이론, Homotopy 이론을 복제, CW-복제 등을 통하여 다루고 위상공간의 위상불변량을 연구한다.
- 보험수리학(Actuarial Mathematics)
확률론을 기초로 이자론, 생존확률, 사망법칙, 생명 보험과 연금, 책임준비금, 연속 및 이산보험상품 이론 등을 다룬다.
- 금융수학특강(Topics in Financial Mathematics)
확률 및 확률과정론, 확률미분방정식, Black–Scholes 모델, Hull–White 모델 등 현대 금융상품의 수리적 모델 분석과 수치 해법을 다룬다.
- 위상기하학(Topological Geometry)
다양체, 위상군과 Lie군, 위상변환군 등을 연구한다. 대수적위상수학, 미분 위상수학 등의 기본분야도 다룬다.
- 위상수학특강(Topics in Topology)
논문과 관련된 최근의 위상수학의 연구동향과 그 이론을 소개하고 내용을 토론하고 연구한다.
- 미분기하학(Differential Geometry)
곡선론과 곡면론을 중심으로 연구하고 변환론의 기초를 다룬다.
- 미분가능다양체(Differentiable Manifolds)
다양체상의 Fiber Bundle과 접속기하학, Green정리와 적분공식, 기하학적 변환, Laplace 작용소, 복소다양체 및 접촉다양체 등의 성질 및 미분다양체에 관하여 연구한다.
- 기하학특강(Topics in Geometry)
논문과 관련된 미분기하학의 최근 연구동향을 소개하고 이에 관한 문헌 조사 등을 하며 그에 대한 내용을 토론하고 발표한다.
- 다변량해석(Multivariate Statistical Analysis)
분해이론, 특성함수의 분해이론, 무한분해이론 등을 다룬다.

- **확률론(Theory of Probability)**
확률공간, 확률변수, 기대값, 적률함수, 특성함수 등을 다룬다.
- **수치해석특강(Topics in Numerical Analysis)**
미분·적분방정식 등 수학적, 물리학적 문제의 해를 구하기 위한 방법으로 컴퓨터를 이용한 수치적 해결 방안을 다룬다.
- **응용미분방정식(Applied Differential Equations)**
미분방정식의 응용분야를 다루며 자연과학과 공학 분야의 응용문제와 해법을 다룬다.
- **과학계산론특강(Topics in Scientific Computations)**
수학적 이론을 기초로 컴퓨터를 이용한 수학적 문제의 해결을 위한 이론과 알고리즘의 이용법을 다룬다.
- **체론(Theory of Field)**
유한 차원 확대체, Galois이론, Abel의 확대체, 체의 구조론, 부치론, Artin-Schreier 이론 등 체론 전반적인 내용을 다룬다.
- **가환대수(Commutative Algebra)**
환과 이데알, 가군, 극소화, 준소분해, 정중속, Noether환과 Artin환, 원비화, 차원, Hilbert-Samuel 다항식, 정칙극소환, 자유분해, Gorenstien 등을 다룬다.
- **대수적정수론(Algebraic Number Theory)**
주이데알환, 정수적으로 닫혀있는환, Noether환과 Dedekind환, Ideal Classes and Unit Theorem, 확대체에서 소이데알의 분해, 수체의 Galois 확장 등을 다룬다.
- **군표현론(Group Representation Theory)**
군표현과 지표이론, 가군적표현의 기초, 정수적표현론에 관한 내용을 다룬다.
- **고급대수학(Advanced Algebra)**
공개키 암호 중 고도의 수학 지식을 필요로 하는 타원곡선 암호, Number-Field 상의 암호 등을 위한 각종 대수학적인 이론을 학습한다.
- **복소해석학(Complex Analysis)**
해석함수, 무한급수, 선적분, 등각사상, Dirichlet 문제, 타원함수 등을 다룬다.
- **편미분방정식(Partial Differential Equations)**
2계편미분방정식의 분류와 경계치문제, 초기치문제 및 일반선형편미분방정식의 해의 존재성과 정규성 등을 다룬다.
- **위상벡터공간론(Topological Vector Space)**
Local Convexity, Hahn-Banach 정리, Compactness와 Klein-Milman 정리, Conjugate 공간, Polar 집합 등을 다룬다.
- **작용소이론(Operator Theory)**
Banach Algebras, 작용소 대수에서의 위상과 밀도 정리, Von Neumann Algebras 등을 다룬다.
- **역문제개론(Introduction to Inverse Problems)**
Layer potential, Neumann 및 Dirichlet 함수, Generalized Polarization Tensors의 개념을 익히고

asymptotic formula를 이용하여 물질 내부의 불순물을 탐색하는 알고리즘을 다룬다.

- **역문제특강(Topics in Inverse Problems)**

역문제에서 사용하는 다중신호분류(MULTiple Signal Classification - MUSIC) 알고리즘, 선형 샘플링 방법(Linear sampling method), 위상적 미분(Topological derivative), 프레체(Frechet) 미분을 이용한 뉴턴의 방법(Newton's method)에 대한 개념을 익히고 수치실험방법을 익힌다.

- **미분기하학요해(Elements of Differential Geometry)**

텐서해석, 고전미분기하학, 현대미분기하학의 개론과 곡면의 위상적 성질 및 기하학적 성질을 다룬다.

- **부분다양체론(Submanifold Theory)**

리만다양체, 부분다양체, 복소다양체, 접촉다양체 등을 다룬다.

- **미분다양체론(Differential Manifolds)**

Stokes정리, Frobenius정리, Affine 접속, Lie군, 다양체의 코호모로지, De Rham의 정리, Fiber Bundle, 복소다양체론을 다룬다.

- **리만기하학(Riemannian Geometry)**

구조변환론, 미분형식, 부분공간론 등을 다룬다.

- **미분기하학특강(Topics in Differential Geometry)**

미분기하학에서의 박사과정에 필요한 최근의 관련 토픽을 다룬다.

- **미분위상기하학(Differential Topological Geometry)**

위상적 성질을 이용한 미분기하학적 구조를 다룬다.

- **대수적위상수학(Algebraic Topology)**

단체복체, 기본군, 단체복체 호모로지, 일반호모토피 부동점 정리 등을 다루어서 위상공간을 대수적 도구를 이용하여 분류하고 그의 응용에 주안점을 둔다.

- **호모로지론(Homology Theory)**

특이호모로지이론, 사상에 의하여 부착된 공간, Eilenberg-Steenrod Axiom, 다양체와 Poincare 쌍대성, 부동점정리 등을 다룬다.

- **호모토피론(Homotopy Theory)**

기본적개념, Hopf 준동형과 2차적결합, 장애이론, CW복체, 분류공간, H-공간, 구면의 호모토피군 등을 다루어 본다.

- **미분위상수학(Differential Topology)**

다양체와 매끄러운 사상, Sard 정리 Morse 함수, 유클리드공간에 매립된 다양체, 횡단성과 만남, 다양체상의 적분 등을 다룬다.

- **퍼지위상수학(Fuzzy Topology)**

퍼지집합, 퍼지위상의 공리, 퍼지분리공리, 퍼지연속성, 부동점정리 등 최근 연구되고 있는 주제에 대하여 다룬다.

- **이산분포론(Theory of Discrete Distribution)**

확률생성함수, 포아송분포, 혼합이산분포, 다변수이산분포 등의 이산분포이론을 다룬다.

- **비모수통계학(Nonparametric Statistics)**
위계검정법, 검정력, 부호검정법, 군검정, 쌍비교 등을 다룬다.
- **시계열분석(Analysis of Time Series)**
회귀시계열, Fourier분석, 대표본이론, 평균치추정, 자기상관이론, 주기표분석 등을 다룬다.
- **회귀분석(Analysis of Regression)**
상관성이론, 상관계수의 분포, 최소자승법, 선형·비선형회귀이론, 최적곡선 등을 다룬다.
- **통계적결정론(Statistical Decision Theory)**
Utility 이론, Loss 이론, Bayesian 분석, 최소최대 분석 등을 다룬다.
- **자료분석과통계실습(Data Analysis and Statistics Laboratory)**
선형·비선형회귀분석, 시계열분석 등 여러 분야의 통계자료를 분석하는 방법을 다루고 실제 자료를 분하고 컴퓨터 모의실험을 한다.
- **미분방정식의수치해법(Numerical Methods for Differential Equations)**
 n 차 상미분 방정식 및 초기치-경계치 조건을 갖는 라플라스, 열, 파동방정식 문제에 대한 수치적 해법을 배운다.
- **유한차분법(Finite Difference Methods)**
일치성, 안정성, 수렴성 등 유한차분법의 이론과 초기치·경계치 문제의 유한차분 해법을 다룬다.
- **영상처리개론(Introduction to Image Processing)**
Level set, Calculus of Variations, Euler-Lagrange eQuation, Total Variation minimization problems, regularization, CFL condition 등을 통하여 편미분 방정식의 구조 및 관련된 수치해석 이론을 이해하고 이를 image denoising 및 segmentation과 같은 영상처리에 응용하는 방법을 배운다.
- **전산유체역학(Computational Fluid Dynamics)**
유체역학의 이론과 해석적인 해결이 불가능한 문제의 컴퓨터를 이용한 해법을 다룬다.
- **혼돈과역학계(Chaos and Dynamical Systems)**
반복, 그래픽해석, 혼돈, 안정성 등 혼돈역학계를 다룬다.
- **수리모형특강(Topics in Mathematical Models)**
다양한 수리적 모형을 대상으로 이론적 배경과 수학적 방법의 적용 및 수치적 해법을 다룬다.
- **유한요소법(Finite Element Methods)**
유한요소 공간이 구성과 오차분석 및 응용을 다룬다.
- **옵션가격결정론(Option Pricing)**
주식, 채권, 선물, 옵션 등 파생 상품의 평가, 가격결정 이론, 위험관리 등을 다룬다.
- **수학적계산모델(Mathematical models for Computation)**
Finite Automata, Pushdown Automata, Turing Machine, Recursive Functions 등을 다루며 다양한 수학적 계산 모델을 소개한다.
- **큐잉이론(Queueing Theory)**
통신망이나 컴퓨터 시스템의 모델링과 성능 분석을 위한 기초 이론으로 큐잉 이론의 기초가 되는

확률이론, 랜덤 프로세스를 다루며 큐잉 시스템으로써 M/M/1, M/M/m, M/G/1 등과 큐잉 네트워크의 기초를 다룬다.

◦ 정보보안 전공(Information Security Major Courses)

- 암호수학(Cryptomathematics)
정보보호에 관련된 유한체 이론을 다룬다. 유한체의 구조, 유한체 상의 다항식, 다항식의 인수분해, 특수다항식, 유한체 응용방법, 유한체위에 기반한 타원곡선 암호 등을 학습한다.
- 암호알고리즘(Crypto-Algorithms)
고전 암호, Shannon의 이론에 기초한 스트림 암호와 블록 암호의 안전성 이론, 사용방법에 따른 문제점, 설계방법 등을 학습한다.
- 고급암호알고리즘(Advanced Crypto-Algorithms)
공개키 암호, 알고리즘, 각종 전자 서명 알고리즘, 해쉬 함수의 설계 원리와 응용 방법 등에 대하여 학습한다.
- 정보의논리(Logic of Information Flow)
효율적인 정보의 처리와 관리를 위한 수리적 논리의 성질과 응용을 다룬다.
- 정보수학특강(Mathematics and Information)
통계학과 확률이론을 기초로 하여 정보이론을 구성하는 불확실성, 엔트로피, 부호이론을 다룬다.
- 정보보호프로토콜(Information Security Protocol)
정보보호 프로토콜의 기본 개념과 Key Distribution, Identification Scheme, Message Authentication Code, Secret Sharing, Pseudo-random Number Generation Zero-knowledge Proof, 전자선거 등의 다양한 프로토콜에 대하여 학습한다.
- 키관리시스템(Key Management System)
키의 생성, 관리에 따른 제반 문제 및 키 복구 기법 등을 다룬다. 대칭키 시스템과 공개키 시스템에서 키 생성, 관리에 대한 두 시스템 사이의 차이점과 두 시스템을 결합시키는 방법을 학습한다.
- 전자상거래(Electronic Commerce Security)
전자쇼핑몰을 이용한 전자상거래 시 필요로 하는 각종 보안 기법 및 문제점을 다룬다. 신용 카드나 전자 수표, 전자 화폐를 이용하는 각종 지불 수단에 대해서 다룬다. 전자지불 시스템이 장단점과 보안상의 문제 등을 학습한다.
- 해쉬함수와데이터인증(Hash Function and Message Authentication)
전자서명에 활용되는 충돌 회피 해쉬 함수 및 이를 이용하여 데이터 위변조를 검출할 수 있는 MCA 생성 방법의 설계원리를 학습한다.
- 공개키암호분석이론(Cryptanalysis of Public-key Cryptosystem)
인수분해, 이산로그 등의 수학적 문제에 기반한 공개키 암호에 대한 기본적인 공격법 및 프로토콜의 적용에 따라 발생하는 제반 문제점을 소개한다. 아울러 각종 공개키 암호에 대한 안전성을 학습한다.
- 복잡도와알고리즘(Complexity and Algorithms)
계산 시간분석, 분류, 조합알고리즘 등 복잡도 이론과 다양한 알고리즘들과 함수들이 항상 제한된 알고리즘에 의해 계산가능 여부의 문제를 다룬다.

- **증명가능안전성론(Provable Security)**
Pseudo-randomness, 정보이론 관점의 안전성, 계산 복잡도 측면의 안전성 등 암호 알고리즘 및 프로토콜에 대한 증명가능 안전성 이론을 다룬다.
- **스태가노그래피및응용(Steganography and its Applications)**
스태가노그래피의 원리와 구현기술을 학습하며, 워터마킹, DRM 등 정보은닉기술의 응용을 다룬다.
- **네트워크보안(Networks Security)**
정보통신망을 통한 데이터 보호 기법 개관을 다룬다. 기존 통신망 분석 및 암호 기술의 접목으로서, 가상 사설망(VPN) 등의 네트워크 보안의 기초 이론을 비롯하여 IPsec, SSL, TLS 등을 학습한다.
- **금융보안론(Financial Information Security)**
전자화폐, 전자지불시스템, 인터넷 뱅킹 시스템 등의 금융 관련 정보보안 기술에 대하여 학습한다.
- **대칭키암호분석(Topics in Symmetric Key Cryptanalysis)**
블록암호, 스트림암호에 대한 안전성 분석기술을 다룬다.
- **암호소프트웨어구현(Implementation of Cryptographic S/W)**
국제표준 대칭키 암호 및 공개키 암호의 소프트웨어 구현기술을 습득한다.
- **암호하드웨어구현(Implementation of Cryptographic H/W)**
암호장비의 HW구조 및 최적화 구현을 위한 최신기술을 학습한다.
- **암호모듈평가및검증(Evaluation and Validation of Cryptographic Module)**
암호모듈 검증제도(CMVP)에 대한 이해를 바탕으로 검증기준에 따른 평가를 수행하는데 필요한 지식을 습득한다.
- **병렬암호구현(Implementation of Parallel Cryptography)**
병렬시스템이나 GPU를 이용한 암호알고리즘의 고속구현기술과 그 응용에 대하여 다룬다.
- **이동통신보안(Mobile Security)**
이동통신망의 최신 보안 구조 및 그 응용 기술을 다룬다.
- **무선보안특강(Wireless Security)**
최신의 무선통신 기술과 그 응용에 필요한 보안기술을 학습한다.
- **융합보안특강(IT Convergence and Security)**
IT와 타 산업의 융합기술을 배우고, 그 응용에 필요한 보안기술을 배운다.
- **스마트그리드보안(Smartgrid Security)**
스마트그리드의 구조와 그 응용에 필요한 보안기술을 학습한다.
- **인터넷보안(Internet Security)**
유무선 인터넷의 구조와 관련 보안기술을 다룬다.
- **부채널공격론(Side Channel Attacks)**
스마트디바이스의 물리적 취약성 분석기술을 다룬다.
- **부채널공격대응론(Countermeasures of Side Channel Attacks)**
부채널공격에 안정한 S/W 및 H/W 기반 대응방법의 설계 및 구현에 대하여 다룬다.

- 다자간계산론(Secure Multiparty Computation)

신뢰 서버의 존재성을 가정하지 않는 환경 하에서 참여 개체들의 프라이버시를 보호할 수 있는 기술을 다룬다.

- 의사난수성론(Pseudorandomness)

암호 알고리즘의 기본적인 안전성 요소인 의사난수성 개념과 통계적 난수성 평가 방법에 대하여 학습한다.