Department of Cyber Security
网络安全系 / 網絡安全系

Department of Cyber Security offers excellent education and interdisciplinary cutting-edge research programs to train future leaders and innovators in cyber security. Faculties from the fields of mathematics, AI, cryptography, and information system provide a broad range of courses and joint research projects in partnership with academia and industry.

❑ **Information Security Major**

Information security major focuses on producing researchers and specialists in privacy protection, protection against hacking, information authentication, and technology evaluation for information security, etc. Our program trains future leaders and innovators in information security by offering an excellent education and cutting-edge research projects.

❑ **Financial Security Major**

Financial security major focuses on producing researcher and specialists in managing and protecting big data, legal and institutional aspects of information security and financial-oriented systems, etc. Our program trains future leaders and innovators working for secure and sustainable environment in defense security areas by offering an excellent education and cutting-edge research projects.

☐ **Courses**

❑ **Core Courses**

· IT Convergence and Security (3)

We study Convergence Technology on IT field and other fields, and the security technology of the applications.

· Research Ethics & Thesis Study (3)

This course provides an overview of methods used to conduct and evaluate research. This course will include discussion on the scientific method, development of research questions, exploration of literature, formulation of research designs, and professional critique of methodologies. Also, ethical issues in research are discussed.

· Cryptographic Algorithms (3)

We study classical cryptography and modern cryptography such as stream ciphers and block ciphers based on Shannon theory.

· **Information Security Protocols (3)**

This is an introductory course for financial information security. After providing brief reviews for cryptographic algorithms, the course covers several topics in protocol including key distribution, secret sharing, authentication, and zero-knowledge protocol.

❑ **Information Security Major**

❑ **Financial Security Major**

· **Introduction to PKI (3)**

The goal of the course is to provide an introduction to PKI (Public Key Infrastructure) and relevant technologies including public key encryption, authentication, and digital signature. As an application. we study how to apply PKI to financial services.

· **Hash Functions and Message Authentication (3)**

This course covers the design principle of collision-free hash functions and message authentication codes which can be used in digital signatures.

· **Cryptanalysis of Public-key Cryptosystems (3)**

This course covers the cryptanalysis of public key cryptosystem based on the mathematical methods such as factorization of numbers, discrete logarithm problems.

· **Topics in Symmetric Key Cryptanalysis (3)**

This course covers the cryptanalysis of symmetric key cryptosystem such as stream ciphers and block ciphers.

· **Parallel Implementation of Cryptographic Algorithms (3)**

This course provides a systematic approach to parallel implementations of cryptographic algorithms. Topics include a brief introduction to computer architecture and operation system. Particularly, parallel computing with GPU will be considered in depth.

· **Evaluation and Validation Techniques for Cryptographic Modules (3)**

This course is an introductory guide for developers who build cryptographic modules. Mandatory standards for cryptographic modules including ISO 19790, 24759, and FIPS 140 will be considered. Students are supposed to understand CMVP(Cryptographic Module Validation Program) in US and Korea and related polices. Also, techniques for security evaluation will be studied.

· **Side Channel Attacks (3)**

This course covers any attack based on side channel information such as timing information, power consumption, electromagnetic leaks or even sound gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis).

· **Countermeasures of Side Channel Attacks (3)**

This course provides secure S/W and H/W cryptographic design and implementations against side channel attacks. The countermeasures fall into two main categories: (1) eliminate or reduce the release of such side channel information; and (2) eliminate the relationship between the leaked information and the secret data.

· **Security Implementation Methodology (3)**

This is a practical guide for implementing security functions. Based on the understanding of cryptographic algorithms, students are required to build an application as a group project and learn how to protect their software from malicious attacks by removing potential vulnerabilities.

· **Mobile Security (3)**

We study the latest mobile networks security architecture and technology.

· **Wireless Security (3)**

We study the latest wireless communications technology and the security technology of the applications.

· **Financial Information Security (3)**

We study the information Security Technology in Financial Field, such as Electronic cash, Secure Electronic Transaction, and Internet Banking Systems, etc.

· **Financial Information Security Policy (3)**

We study the management and the policy of information security. We study the management methodology that can supplement the limit of information security techniques.

· **Information Security Consulting (3)**

This course is a field that focuses on advising IT businesses on how best to use information technology to meet their business objectives. To providing advice, we study how to estimate, manage, implement, deploy, and administer information security products or the IT security related organization about security level, vulnerability, policy, standard, and monitoring process.

· **Information Security System Evaluation Methodology (3)**

This course covers evaluation methodology for information security systems. To understand conformance tests, we refer testing methodology in CC (Common Criteria), CMVP(Cryptographic Module Validation Program), and PIV(Personal Identity Verification).

· **Analysis and Implementation of Security Technical Standards (3)**

This course has two main goals. One is understanding of standardizations of security

techniques and the other is having ability to build systems based on the standard techniques. We refer standard documents by ISO/IEC, IETF (Internet Engineering Task Force), ITU-T. Students are supposed to be familiar with standards and applying them.

· Introduction to Digital Forensics (3)

We study the forensic science encompassing the recovery and investigation of material found in digital devices such as personal computers, notebook computers and cellular phones, often in relation to computer crime.

· Special Research of Digital Forensics (3)

Study and research current cutting-edge technologies and methodologies in digital forensics.

· Defense Device Attacks (3)

The goal of the course is how to seeks and exploits weaknesses in defense devices such as PC, smart phone, smart card, Micro-SD, OTP and so on. And then we study some countermeasures which are secure against these attacks.

· Countermeasures against Defense Device Attacks (3)

Study various H/W- and S/W-based methods and technologies for protecting financial transaction devices from current avaliable security attacks.

· Defense Key Management System (3)

Study key management systems used for providing secure financial services and protecting systems for those services. Students will study the current technologies and theories applied in generating, distributing, and recovering keys used in security systems and mechanisms for financial transactions.

· Defense Networks Security (3)

Students will learn security technologies and theories for protecting important and valuable financial data transmitted through communication systems, e.g., VPN (Virtual Private Networks), IPSec, SSL, TLS, and so forth.

· Electronic Commerce Security (3)

Topics covered include information security schemes to protect the electronic commerce, especially electronic cash, electronic payment, electronic wallet.

· Provable Security (3)

Deals with Computational complexity, Unconditional security, Complexity theoretic security, Provable security under assumptions, Ad hoc security.

· Implementation of Cryptographic S/W (3)

Acquire the software implementation technologies of International standard Symmetric Key Encryption Algorithm and public key Encryption Algorithm.

· **Analysis of Randomness (3)**

Deals with Probabilistic theory of randomness, Design and security analysis of cryptographic random number generators, Statistical test of random sequences.

· **AI and Security (3)**

In this lecture, we will learn about machine learning technique that attempt to fool the AI models by supplying the deceptive input. This class provides the theory and experimental results of the proposed adversarial attack and its defense model of the AI.

· **Advanced Self-supervised AI (3)**

In the field of AI, automatic data augmentation and efficient machine learning algorithms become key elements in future intelligence competitiveness. In this class, we will learn the theory and concept of the self-improving AI techniques to learn meanings, correlations, and time-related associations of complex model knowledge.

· **AI Convergence (3)**

AI convergence seminar provides the new research trends through expert lectures and seminars in various topics related to AI and security technologies.

· **Advanced Internet of Things (3)**

In this class, we learn about Internet of Things (IoT) / Internet of Service (IoS), which are composed of service, platform, network (connectivity) and smart devices. Furthermore, through this class, we will do research on simulation combined with artificial intelligence, Cyber Physical System, and Digital Twin.

· **Wireless Cellular Network (3)**

Through this class, we will learn about wireless mobile communication technology and history from the first generation of wireless mobile cellular communication Advanced Mobile Phone System(AMPS) to 4G Long Term Evolution-Advanced (LTE-A). This class examines 5G and 5G+ mobile communication systems focusing on core technologies such as Network Slicing, Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communication (URLLC), and Massive Machine Type Communication (mMTC). In addition, we will learn about wireless access mobile Internet, Device to Device (D2D), 5G core network technology, and artificial intelligence-based service platform. We also study 6G network requirements and network scalability, which are predicted to start service from 2030.

· **Advanced Information Communication Theory (3)**

It aims to educate about the core /edge network and context awareness and

localization that are the core technologies of computing. It provides information on various application systems including context-awareness / localization, and next generation network architecture, requirements of ubiquitous network, etc.

· Model-based System Design (3)

This course is an introduction to model-based system design with domain specific and domain independent aspects. The metamodeling concepts are introduced for various information systems, and hybrid system such as cyber physical systems. From the fundamental system design with UML up to metamodeling system design will be covered. The object programming language is used to implement the design process.

· Data Mining (3)

Data mining is concerned with the extraction of novel knowledge from large amounts of data. This course introduces and studies the concepts, issues, tasks and techniques of data mining. Topics include data preparation and feature selection, association rules, classification, clustering, evaluation and validation, scalability, spatial and sequence mining, and data mining applications.

· IoT Network (3)

It educates about teristrial IoT(Internet of Things), M2M(Machine to Machine Communication), WoT(Web of Things), UIoT(Underwater IoT) and so on. Furthermore, we will also study about the related international standards.

· Embedded System (3)

This course aims to enhance the understanding of ARM architecture and the ability to design and implement embedded system based on firmware.

· Real-time System (3)

This course aims to enhance the understanding of real-time system and the ability to design and implement embedded system based on RTOS(Real-Time Operating System).

· Information System Development Methodology (3)

It educates about the methodology of developing information system concerning embedded system. Thus, we will study about the data structures and algorithms, the overall process of design and implementation of embedded system and so on.

· Business Data Communication (3)

This course is about the fundamentals of data communications and networking. We will discuss information representation, network topologies, transmission medium, OSI model and TCP/IP networking models, and mainstream LAN and WAN technologies. The OSI model is used as a framework to organize and discuss the network technologies. The technical and managerial aspects of data communications and networking are both emphasized.

· **Cloud Computing (3)**

This course introduces the fundamental technologies and issues in this cloud computing environment. In terms of everything as a Service in cloud computing service, we learn main considerations in SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service), and the related technologies. Students learn concepts and applicable areas of infrastructure system of cloud computing and VM provisioning via cloud environment. Also we will study the trends of enterprise cloud adoption, application integration, and various service provider and application to form the cloud service.

☐ Faculty Members

Yi, Okyeon
Korea Univ., B.S.
Korea Univ., M.S.
University of Kentucky, Ph.D.
Mobile security and cryptographic module
oyyi@kookmin.ac.kr

Kang, Ju-Sung
Korea Univ., B.S.
Korea Univ., M.S.
Korea Univ., Ph.D.
Design and security analysis of cryptographic algorithms
jskang@kookmin.ac.kr

Han, Dong-Guk
Korea Univ., B.S.
Korea Univ., M.S.
Korea Univ., Ph.D.
Cryptographic engineering - Cryptographic implementations, Attacks against implementations and countermeasures against these attacks
christa@kookmin.ac.kr

Yeom, Yongjin
Seoul National Univ., B.S.
Seoul National Univ., M.S..
Seoul National Univ., Ph.D.
Implementation and evaluation of cryptographic techniques
salt@kookmin.ac.kr

Kim, Jongsung
Korea Univ., B.S.
Korea Univ., M.S.
Katholieke Universiteit Leuven, Ph.D.
Design and Cryptanalysis of Cryptographic Algorithms
jskim@kookmin.ac.kr

Park, Soo Hyun
Korea Univ., B.S.
Korea Univ., M.S.
Korea Univ., Ph.D.
Computer Network, IoT / IoS
shpark21@kookmin.ac.kr

Choi, Eunmi
Korea Univ., B.S.
Michigan State University, M.S.
Michigan State University, Ph.D.
Distributed System and Cloud Computing
emchoi@kookmin.ac.kr

Dong-Chan Kim
Sogang Univ., B.S.
Sogang Univ., M.S.
Sogang Univ., Ph.D.
Cryptography, Coding theory
dckim@kookmin.ac.kr

Seo, SeogChung
Ajou Univ., B.S.
GIST, M.S.
Korea Univ., Ph.D.
Information Security
scseo@kookmin.ac.kr

Yoon, SangMin
Korea Univ., B.E.
Korea Univ., M.E.
TU Darmstadt, Ph.D.
Computer Vision, AI
smyoon@kookmin.ac.kr

You, IlSun
Dankook Univ., B.S.
Dankook Univ., M.S.
Dankook Univ., Ph.D.
Kyushu Univ., Ph.D.
Information Security
isyou@kookmin.ac.kr

Kim, HwanKook
Korea Univ., B.E.
Korea Univ., M.E.
TU Darmstadt, Ph.D.
Computer Vision, AI
smyoon@kookmin.ac.kr