

스마트보안학부 수강신청 유의사항

최종업데이트: 2025년 1월

○ 사이버국방학과(대외비)

- 사이버국방학과 수강신청 관련 사항은 행정실(02-3290-4253)로 문의 주시기 바랍니다.

○ 스마트보안학부

1. 수강신청 기본 안내사항

- 가. 교육과정은 입학 연도의 교육과정이 적용됩니다.
- 나. 교육과정 개편에 따라 학년별로 적용되는 교육과정이 상이하므로 교과목 이수에 주의하시기 바랍니다.
- 다. 수강신청은 반드시 본인이 직접 신청합니다.

2. 수강신청 원칙

- 가. 수강신청 가능 학점
 최소 1학점 ~ 최대 19학점
 단, 아래의 조건을 하나라도 충족한 경우 추가 3학점 초과 수강 가능
 - 1) F등급 없이 전체 성적 평균평점이 3.75 이상
 - 2) 직전 학기(정규학기) F등급 없이 18학점 이상 이수하고 평균평점이 3.75 이상인 경우

3. 수강신청 신규 제도: 유연 수강신청 학점제

- 가. 제도 정의: 학년도 내에서 최대 3학점을 선사용 또는 이월하는 제도
- 나. 유형구분

유형	사용 범위
1학기 수강(희망) 학점 = 수강 가능학점	-
1학기 수강(희망) 학점 < 수강 가능학점	최대 3학점까지 2학기 이월
1학기 수강(희망) 학점 > 수강 가능학점	최대 3학점까지 2학기 수강 가능학점 선사용

※ 수강포기로 인해 수강 신청 학점이 축소된 사항은 반영하지 않음

다. 유의사항

- 1) 당해 학기 최종 수강학점이 17학점 미만이 되는 경우 학기우수생이나 성적우수

상 대상이 될 수 없음

- 2) 직전학기 F등급 없이 17(18)학점 미만을 이수할 경우 초과 수강신청 부여 불가
- 3) 기존과 동일하게 수강신청 시스템에서 수강신청 진행 (수강신청학점은 자동 계산)
- 4) 1학기 수강신청이 끝난 후(수강 정정기간 포함) 2학기 선사용 학점 및 이월 학점 전산 반영
- 5) 1학기 학적변동자(휴학, 해외 교환학생 및 국내 학점교류), 2학기 신·편입생 및 재입학생은 신청 불가

라. 시행 시기

- 1) 학점 선사용(1학기) : 학기 초 수강정정기간(학년별 ~ 전체 정정)
- 2) 학점 이월(2학기) : 수강희망과목등록 시기부터

4. 최근 교육과정 개편사항 안내

가. 교과목 폐지 및 신설

: 권장이수학기 및 강의유형 변경에 따른 교과목 폐지 및 신설

교과목명(학수번호)	권장이수학기 및 강의유형	
	기존	개편 후
디지털포렌식개론 (SMRT303)	2학년 1학기 / 이론 중심	3학년 1학기 / 이론 및 실습
역공학 (SMRT224)	2학년 2학기 / 이론 중심	3학년 2학기 / 이론 및 실습

나. 강의 유형 변경

교과목명(학수번호)	강의 유형
시큐어코딩(SMRT242)	이론 및 실습 → 이론 중심 (이론 3시간)
디지털포렌식실무 (SMRT424)	이론 중심 → 이론 및 실습 (이론 2시간, 실습 2시간)
인공지능보안II (SMRT336)	

다. 권장이수학기 변경

교과목명(학수번호)	권장이수학기
시큐어소프트웨어공학I (SMRT332)	3학년 1학기 → 3학년 2학기
시큐어소프트웨어공학II (SMRT431)	4학년 2학기 → 4학년 1학기

라. 타 학과 교과목 신설

-사이버국방학과 교과목 과목18 (CYDF211) 전공선택으로 추가

5. 기타 유의사항
가. 수강학과 제한

스마트보안학부 학생(이중전공, 융합전공, 복수전공) 이 아닌 학생들의 경우 수강신청 기간에는 수강 신청 자격이 제한됩니다. 타학과 학생은 전체 정정기간 중 여석이 있는 경우에 한해 수강 신청이 가능할 수 있습니다.

나. 스마트보안학부 교과목의 경우, 강의실 규모와 교과목 특성에 맞추어 수강인원이 제한될 수 있습니다.

다. 2023학년도 2학기부터 수강포기제도 시행에 따라 1학기 최대 9학점까지 수강포기가 허용됩니다. 1학년 필수 과목 등 일부 수강 포기 제한이 필요한 과목의 경우 수강 포기가 제한 됩니다.

라. 2025-1학기 개설되는 타학과 교과목

학과	학수번호	교과목명	학점인정구분	비고
컴퓨터학과	COSE221	논리설계	전공선택	스마트보안학부 교수가 개설한 분반 수강 권고
	COSE341	운영체제	전공선택	
	COSE342	컴퓨터네트워크	전공필수	
	COSE451	소프트웨어보안	전공선택	

마. 타 단과대학 교과목에 대한 전공 학점 인정

학과	학수번호	교과목명	인정구분	학점	시간	비고
컴퓨터학과	COSE221	논리설계	전공선택	3	3	2023학번부터 스마트보안학부 학점 인정
	COSE222*	컴퓨터구조	전공선택	3	3	2022학번부터 스마트보안학부 학점인정
	COSE312*	컴파일러	전공선택	3	3	
	COSE341*	운영체제	전공선택	3	3	
	COSE342*	컴퓨터네트워크	전공필수	3	3	
	COSE451*	소프트웨어보안	전공선택	3	3	

※ "*" 교과목을 기 이수 한 경우 스마트보안학부 전공학점으로 소급 적용하여 인정가능.

바. 학문의 기초(필수)

학번	학수번호	교과목명	학점	시간	강의유형
2025학번	SMRT101	스마트보안개론	3	3	이론중심
	SMRT111	C언어및실습	3	4	이론및실습

사. 캡스톤디자인

- 1) 캡스톤디자인 과목의 경우, 수강생이 학부연구원으로 연구할 연구실의 지도교수가 과목을 담당하게 되므로 사전에 연구실 지도교수의 승인을 받고 신청하시기를 바랍니다.
- 2) 캡스톤디자인 수강 시 연구 결과를 토대로 학술대회 논문 한편을 작성해야 합니다.

아. 현장실습

현장실습지원센터에서 개설하는 공통교과목에 대한 전공 인정이 가능합니다. 전공 인정 학점의 상한선은 18학점이며, 수강 신청 전 학과에서 전공 연관성 검토 후 진행이 가능합니다.

- 신청자격 : 4학기 이상 등록 (단, 계절학기(여름, 겨울) 현장실습학기제에 한해 2학기 이상 등록 가능)

학수번호	교과목명	학점	개설 시기	이수구분	강의 종류	최소인정조건
COOP031	현장실습A1	3	매학기	전공선택	인턴십	실 근무일 20일, 실 근무시간 160시간
⋮	⋮	⋮	⋮	⋮	⋮	
COOP036	현장실습A6	3	매학기	전공선택	인턴십	실 근무일 40일, 실 근무시간 320시간
COOP061	현장실습B1	6	매학기	전공선택	인턴십	
COOP062	현장실습B2	6	매학기	전공선택	인턴십	
COOP063	현장실습B3	6	매학기	전공선택	인턴십	실 근무일 75일, 실 근무시간 640시간
COOP121	현장실습D1	12	매학기	전공선택	인턴십	

※ 자세한 내용은 현장실습센터 공지사항 확인부탁드립니다.

※ 같은 이수 구분, 같은 학점 수 내에서 교과목 선택은 학수번호순으로 신청합니다. (다른 학기에 동일한 학점 수 이수 시 재수강이 아닌 다른 교과목으로 학점부여하기 위해 학수번호가 다른 교과목 여러개로 개설 되어 있음)

※스마트보안학부 학생을 대상으로 개설된 현장실습 교과목이 아닌 경우 해당 현장실습 교과목을 전공학점으로 인정받기 위해 사전에 학과에 문의하여 학(과)부장에게 해당 현장실습 교과목을 승인 받으시기를 바랍니다.

자. 정보보호대학원 교과목 학점 인정(선수강)

학과	학수번호	교과목명	학점	시간	스마트보안학부 전공 인정 구분
정보보호학과	SCS552	IoT포렌식	3	3	전공선택
	SCS554	클라우드보안	3	3	전공선택
	SCS558	빅데이터분석방법론	3	3	전공선택
	SCS605	IoT보안	3	3	전공선택
	SCS606	블록체인	3	3	전공선택
	SCS701	데이터법	3	3	전공선택

- 선수강 대상자: 스마트보안학부 4학년 학생으로 직전학기까지 전체 성적 평균평점 3.50이상
- 정보보호대학원 선수강 학점인정 범위: 정보보호대학원 석사 또는 석박사통합과정으로 입학한 경우, 학부 졸업요구학점을 초과한 범위에서 6학점까지 인정 (근거: 대학원 학칙 일반대학원 시행세칙 제 25조 3항 2호)

차. 정보보호대학원 학·석사연계과정

고려대학교의 학사과정과 정보보호대학원의 석사과정을 연계하여 운영하는 과정으로 학부과정에서 대학원 교과목을 선이수하여 석사과정을 단축을 할 수 있는 제도입니다.

- 모집학과: 정보보호학과
- 지원 자격: 고려대학교 학부생으로 4학기 이상 등록하고, 총 67학점 이상 취득자로서 성적 평점평균 3.50 이상인 학생
- 접수 기간 : 2025학년도 후기는 2025년 5월 말 접수 예정
- 학·석사연계과정생 특전
 - 가. 수업연한 단축
 - 1) 석사과정 진입 후에 평점평균 4.0 이상으로 석사과정 수료 자격을 모두 갖춘 경우 1학기 내에서 단축할 수 있음 (대학원 석사과정 4학기 → 3학기로 단축)
 - 2) 학부 조기 졸업은 학부 졸업 요건을 따름. 학부 조기 졸업하는 경우 학부 1학기 추가 단축 가능
 - 나. 석사과정 진입 시, 진입한 학기에 입학금에 해당하는 장학금 지급 (개강 후 본인 계좌로 지급, 1학기 : 4월경, 2학기 : 10월경)
- 정보보호대학원 교과목 이수

가. 정보보호대학원 교과목 이수

- 1) 학·석사연계과정 합격 다음 학기부터 학부 졸업 시까지 학부 졸업요구학점을 초과하여 정보보호대학원 정보보호학과 교과목(선수과목, 연구지도 제외)을 총 6학점 이상 추가 이수하여야 함
- 2) 학·석사연계과정으로 석사과정에 진입할 경우, 학부 졸업요구 학점을 초과하는 정보보호학과 이수학점에 대해 9학점까지 인정할 수 있음

※ 자세한 내용은 정보보호대학원 공지사항 확인부탁드립니다.

이 밖의 자세한 사항은 스마트보안학부 행정실 담당자(02-3290-4250)에게 문의하시기 바랍니다.

[붙임 1] 교과과정표

스마트보안학부

2025학년도

구분	내용	학수번호	교 과 목 명	학점(시간)	1차년도		2차년도		3차년도		4차년도	
					I	II	I	II	I	II	I	II
교양 필수	학문세계의탐구	GELI005	학문세계의탐구 I	3(3)	•		2024학년도 이후 입학한 외국인 학부생은 GELI007					
	글쓰기	GEWR002	글쓰기	3(3)	•	•	학문세계의탐구 I (외국인반), 글쓰기 (외국인반) 이수					
	Academic English	IFLS800	Academic English I	2(2)	•		신입생 영어능력평가고사 결과 '고급'레벨 취득 학생은 이수 면제					
	1학년세미나	GEKS007	[진로·창업]1학년세미나 I	1(1)	•							
		GEKS008	[진로·창업]1학년세미나 II	1(1)		•						
	Digital & SW	GECT002	[진로·창업]SW프로그래밍의기초	3(3)	•							
		GECT003	[진로·창업]데이터과학과인공지능	3(3)		•						
BT	GEBT001	[진로·창업]생명과학의세계	3(3)	•								
소 계				19								
교양선택				9								
교양 총 계				28								
학문의기초	SMRT101	스마트보안개론	3(3)	•								
	SMRT102	스마트보안수학	3(3)		•							
	SMRT111	C언어및실습	3(4)	•								
	SMRT112	계산논리	3(3)		•							
기본 전공	필수	SMRT201	암호구현및실습	3(4)		•						
		SMRT222	현대암호학	3(3)			•					
		SMRT262	사이버윤리	3(3)			•					
		SMRT301	인공지능보안 I	3(3)				•				
		SMRT332	시큐어소프트웨어공학 I	3(3)					•			
		COSE342	컴퓨터네트워크	3(3)				•				
	선택			24								
계				42								
심화 전공	필수											
	선택											
	계			36								
졸업요구 총 이수학점*				130								
비 고		* 현장실습교과목은 최대 18학점까지 전공으로 인정하며, 현장실습지원센터 개설과목(학수번호 COOP로 시작)도 18학점까지 전공으로 인정함 수강신청 전 학과에서 전공 연관성 검토 후 진행										

[붙임 2] 개설과목목록
【스마트보안학부】

이수 구분	학수번호	교과목명	학점 (시간)	학수번호	교과목명	학점 (시간)
전공 필수	SMRT201	암호구현및실습	3(4)	SMRT301	인공지능보안	3(3)
	SMRT222	현대암호학	3(3)	SMRT332	시큐어소프트웨어공학I	3(3)
	SMRT262	사이버윤리	3(3)	COSE342	컴퓨터네트워크*	3(3)
전공 선택	SMRT203	정형기법	3(3)	SMRT431	시큐어소프트웨어공학II	3(3)
	SMRT205	인공지능보안수학	3(3)	SMRT433	빅데이터응용보안	3(3)
	SMRT221	암호수학	3(3)	SMRT435	스마트보안응용	3(3)
	SMRT303	디지털포렌식개론	3(4)	SMRT461	사이버기술과법	3(3)
	SMRT344	역공학	3(4)	SMRT463	개인정보보호	3(3)
	SMRT226	해킹개론	3(4)	SMRT465	캡스톤디자인	3(6)
	SMRT242	시큐어코딩	3(3)	SMRT466	캡스톤디자인II	3(6)
	SMRT302	데이터보안	3(3)	SMRT468	스타트업창업방법론	3(3)
	SMRT321	암호프로토콜	3(3)	SMRT481	현장실습I	3(0)
	SMRT322	현대암호학응용	3(4)	SMRT482	현장실습II	6(0)
	SMRT323	컴퓨터시스템보안	3(4)	SMRT483	현장실습III	12(0)
	SMRT324	컴퓨터네트워크보안	3(3)	COSE221	논리설계*	3(3)
	SMRT334	위험관리	3(3)	COSE222	컴퓨터구조*	3(3)
	SMRT336	인공지능보안II	3(4)	COSE312	컴파일러*	3(3)
	SMRT338	개인정보비식별화개론	3(3)	COSE341	운영체제*	3(3)
	SMRT422	하드웨어보안	3(3)	COSE451	소프트웨어보안*	3(3)
	SMRT424	디지털포렌식실무	3(4)	CYDF211	과목18	3(4)

[붙임 3] 주요 과목 배정시간표

	월	화	수	목	금
1 교시 09:00-10:15	C언어및실습 (SMRT111)	스마트보안개론 (SMRT101)	C언어및실습 (SMRT111)		
	암호수학 (SMRT221)		암호수학 (SMRT221)		
	사이버기술과법 (SMRT461)	스타트업창업방법론(SMRT468)	사이버기술과법 (SMRT461)	스타트업창업방법론(SMRT468)	
2 교시 10:30-11:45	C언어및실습 (SMRT111)	스마트보안개론 (SMRT101)			
		인공지능보안수학 (SMRT205)		인공지능보안수학 (SMRT205)	
	운영체제 (COSE341)		운영체제 (COSE341)		
			시큐어소프트웨어공학II(SMRT431)		
3 교시 12:00-13:15				암호구현및실습 (SMRT201)	
		암호프로토콜 (SMRT321)			암호프로토콜 (SMRT321)
	시큐어소프트웨어공학II(SMRT431)				
4 교시 13:30-14:45					
	컴퓨터네트워크 (COSE342)	인공지능보안 (SMRT301)	컴퓨터네트워크 (COSE342)	인공지능보안 (SMRT301)	컴퓨터시스템보안 (SMRT323)
5 교시 15:00-16:15	논리설계 (COSE221)		논리설계 (COSE221)		
					컴퓨터시스템보안 (SMRT323)
	빅데이터응용보안 (SMRT433)		빅데이터응용보안 (SMRT433)		
6 교시 16:30-17:45	암호구현및실습 (SMRT201)	정형기법 (SMRT203)		정형기법 (SMRT203)	
		디지털포렌식개론 (SMRT303)	컴퓨터시스템보안 (SMRT323)	디지털포렌식개론 (SMRT303)	
7 교시 18:00-18:50	암호구현및실습 (SMRT201)			디지털포렌식개론 (SMRT303)	

Course Registration Notes

Division of Smart Security

Update: January, 2025

○ **Department of Cyber Defense (Confidential)**

For inquiries related to course registration in the Department of Cyber Defense, please contact the administrative office at 02-3290-4253.

○ **Division of Smart Security**

1. Course registration basics

- a. The curriculum applied is based on the year of admission.
- b. Due to curriculum revisions, the curriculum applied varies by year, so please pay attention to the course requirements.
- c. Course registration must be completed by the student themselves.

2. Principles of Course registration

- a. Credit limits for registration:
 - Minimum: 1 credit, Maximum: 19 credits
 - Exception: Students may exceed by 3 additional credits if they meet one of the following conditions:
 1. A cumulative GPA of 3.75 or higher without any F grades.
 2. A GPA of 3.75 or higher in the previous regular semester, having completed at least 18 credits without any F grades

3. New Course Registration System: Flexible Credit Course Registration System

- a. Definition: This system allows students to pre-use or carry over up to 3 credits within an academic year
- b. Type Classification

Type	Scope of Use
Spring Semester Desired Credits = Permitted Credits	-
Spring Semester Desired Credits < Permitted Credits	Carry-over up to 3 credits to Fall Semester
Spring Semester Desired Credits > Permitted Credits	Pre-use up to 3 credits from Fall Semester's allowance

※ Reductions in registered credits due to Course Registration Drops(Withdraws) are not reflected

c. Important Notes and Miscellaneous

1. If the total registered credits for the semester fall below 17 credits, students will be ineligible for academic honors or excellence awards
2. Students who completed fewer than 17 (or 18) credits in the previous semester without any F grades will not be allowed additional credit registration
3. Please proceed with course registration through the existing system as previously (credit adjustments will be automatically calculated)
4. After the completion of the spring semester course registration (including the course revision period), credits for pre-use in the fall semester and carry-over credits will be applied to the system
5. The system cannot be applied to students who have changes in their academic status during the Spring Semester (pre-using Fall Semester credits or carrying over credits to the Fall Semester is not allowed). Freshmen, transfer students, re-admitted students in the Fall Semester are also ineligible.

d. Implementation Timeline

- A. [pre-use] Spring Semester: During the Course Add/Drop period (from school year-specific to all-student adjustments)
 - B. [carry-over] Fall Semester : Starting from the Pre-Registration of Preferred Courses period
- ※ Note: The spring semester of this system is based on the start of the academic year in March. (the fall semester starts in September)

4. What's new

a. Course Discontinuation and Introduction

: Discontinuation and introduction of courses due to changes in recommended enrollment semesters and course types

Course Name	Recommended semesters and types of lectures	
	Before	After
INTRODUCTION TO DIGITAL FORENSICS (SMRT303)	1st semester of the 2nd year / Theory	1st semester of the 3rd year / Theory and practice
SOFTWARE REVERSE ENGINEERING (SMRT224)	2nd semester of the 2nd year / Theory	2nd semester of the 3rd year / Theory and practice

b. Changes in types of lectures

Course Name	Types of lectures
SECURE CODING (SMRT242)	Theory and practice → Theory
DIGITAL FORENSIC PRACTICE (SMRT424)	Theory → Theory and practice
AI SECURITY II (SMRT336)	

c. Changes of Recommended Semester Enrollment

Course Name	Recommended Semester Enrollment
SECURE SOFTWARE ENGINEERING I (SMRT332)	1st semester of the 3rd year → 2nd semester of the 3rd year
SECURE SOFTWARE ENGINEERING II (SMRT431)	2nd semester of the 4th year → 1st semester of the 4th year

d. Introduction of courses from other department.

- Cyber Defense Department course, CYDF211, added as a major elective.

5. Miscellaneous

a. Restrictions on Enrollment by Department:

Students who are not in the Department of Smart Security (including double majors, interdisciplinary majors, and multiple majors) are restricted from registering during the registration period. Students from other departments may register only if there are available seats during the overall adjustment period.

b. For courses in the Department of Smart Security, enrollment may be limited according to classroom capacity and the nature of the course.

c. Starting from the second semester of the 2023 academic year, a course withdrawal system is implemented, allowing withdrawal of up to 9 credits per semester. Some courses, such as required freshman courses, may have restrictions on withdrawals.

d. Courses Offered by Other Departments in the 2025-1 Semester

Department	Course Number	Course Name	Credit Recognition	Note
Computer Science	COSE221	DIGITAL LOGIC DESIGN	Major Elective	Recommended to take the class offered by the Smart Security Faculty
	COSE341	OPERATING SYSTEMS	Major Elective	
	COSE342	COMPUTER NETWORK	Major Required	
	COSE451	SOFTWARE SECURITY	Major Elective	

e. Recognition of Major Credits for Courses from Other Colleges

Department	Course Number	Course Name	Credit Recognition	Credit	Hours	Note
Computer Science	COSE221	DIGITAL LOGIC DESIGN	Major Elective	3	3	Recognized for Division of Smart Security for students from 2023
	COSE222*	COMPUTER ARCHITECTURE	Major Elective	3	3	Recognized for Division of Smart Security for students from 2022
	COSE312*	Compiler	Major Elective	3	3	
	COSE341*	OPERATING SYSTEMS	Major Elective	3	3	
	COSE342*	COMPUTER NETWORK	Major required	3	3	
	COSE451*	SOFTWARE SECURITY	Major Elective	3	3	

※Note: Courses marked with "*" can be retroactively recognized as major credits for Division of Smart Security if already completed.

f. Academic foundations (Mandatory)

Year	Course Number	Course Name	Credit	Hours	Course Type
Students from 2025	SMRT101	INTRODUCTION TO SMART SECURITY	3	3	Theory
	SMRT111	C PROGRAMMING AND PRACTICE	3	4	Theory and Practice

g. Capstone Design course

■ For Capstone Design course, the supervising professor of the laboratory where the student will conduct research as an undergraduate researcher will be in charge of the course. Therefore, please obtain prior approval from the supervising professor of the laboratory before applying.

- When taking the Capstone Design course, students are required to write a conference paper based on their research results.

h. Internship course

Credits for common courses offered by the Internship Support Center can be recognized as major credits. The maximum limit for recognized major credits is 18 credits, and the course should be taken after the department reviews its relevance to the major.

- Qualification : Students who are registered for at least 4 semesters (However, for the students who takes seasonal semesters (summer, winter) field practice system, 2 semesters are required)

Course Number	Course Name	Credit	Available Semester	Course Type	Lecture Type	Minimum Requirement
COOP031	Field PracticeA1	3	Every semester	Elective Major	Internship	Actual work day of 20 days, Actual work time of 160 hours
⋮	⋮	⋮	⋮	⋮	⋮	
COOP036	Field PracticeA6	3	Every semester	Elective Major	Internship	Minimum of 40 days, 320 hours
COOP061	Field PracticeB1	6	Every semester	Elective Major	Internship	
COOP062	Field PracticeB2	6	Every semester	Elective Major	Internship	
COOP063	Field PracticeB3	6	Every semester	Elective Major	Internship	Minimum of 75 days, 640 hours
COOP121	Field PracticeD1	12	Every semester	Elective Major	Internship	

※ Note: For detailed information, please check the announcements from the Field Practice Center

※ Course selection within the same course type and credit will be made in order of course number. (If the same credit are completed in a different semester, the credit is awarded for a different course, not for a retaken course. Therefore, multiple courses with different course numbers are offered for the same credit.)

※ Please consult with your department and obtain approval from the department head in advance to have the field practice course recognized as a major credit if it is not a intership course specifically offered for students in the Division of Smart Security.

i. Credit Recognition for School of Cybersecurity Courses(Prerequisites)

Department	Course Number	Course Name	Credit	Hours	Division of Smart Security Major Classification
Cybersecurity	SCS552	IoT Forensics	3	3	Elective Major
	SCS554	Cloud Security	3	3	Elective Major
	SCS558	Research on Bigdata Analysis	3	3	Elective Major
	SCS605	IoT Security	3	3	Elective Major
	SCS606	Blockchain and Cryptocurrency	3	3	Elective Major
	SCS701	Data Law	3	3	Elective Major

- Eligible Students: 4th-year students of Division of Smart Security with an overall GPA of 3.50 or above in the previous semester.

- Credit Recognition for School of Cybersecurity Pre-Enrollment: If enrolled in the Master's or Integrated Master's and Doctoral program of School of Cybersecurity, up to 6 credits can be recognized beyond the required graduation credits of the undergraduate program (based on the Graduate School Regulations, General Graduate School Implementation Rules, Article 25, Paragraph 3, Subparagraph 2).

j. Combined Bachelor's and Master's Program in School of Cybersecurity

This program combines the undergraduate curriculum at Korea University with the master's curriculum at School of Cybersecurity, allowing students to pre-complete graduate courses during their undergraduate studies and shorten the duration of their master's program.

- Department: Department of Information Security
- Qualification: Korea University undergraduate students who have completed at least 4 semesters, earned at least 67 credits, and have a GPA of 3.50 or higher.
- Application Period: Applications for the Fall 2025 semester are expected to be accepted by the end of May 2025.
- Benefits for Combined Bachelor's and Master's Program Students

a. Shortened Course Duration

- a) If a student enters the master's program and meets all the requirements with a GPA of 4.0 or higher, the master's program can be shortened by one semester (from 4 semesters to 3 semesters).
- b) Early graduation from the undergraduate program is subject to the undergraduate graduation requirements. If early graduation is achieved, an additional semester can be shortened from the undergraduate

program.

b. Scholarship upon Entering the Master's Program

Students will receive a scholarship equivalent to the admission fee in their first semester of the master's program (paid to their account after the start of the semester; April for the first semester, October for the second semester).

■ Course Completion at School of Cybersecurity

a. Course Completion

a) Starting from the semester following acceptance into the combined program and until undergraduate graduation, students must complete at least 6 additional credits in Cybersecurity courses (excluding prerequisites and research guidance) at School of Cybersecurity, beyond the required credits for undergraduate graduation.

b) If entering the master's program through the combined program, up to 9 credits of Cybersecurity courses completed beyond the undergraduate graduation requirements can be recognized towards the master's program.

※ For detailed information, please refer to the announcements from School of Cybersecurity.

For further details, please contact the administrative office of Division of Smart Security (02-3290-4250).

[Attachment 1] Course Catalog
Division of Smart Security

The Academic Year 2025

Category	Content	Course Number	Course Name	Credit (Hour)	First year		Second year		Third year		Fourth year	
					I	II	I	II	I	II	I	II
General required	Exploration of The Academic World	GELI005	EXPLORATION OF THE ACADEMIC WORLD I	3(3)	•		International undergraduate students admitted after the 2024 academic year must complete GELI007 Exploration of the Academic World I (for international students) and College Writing (for international students)					
	College Writing	GEWR002	COLLEGE WRITING	3(3)	•	•						
	Academic English	IFLS800	ACADEMIC ENGLISH I	2(2)	•		Freshmen who achieve an 'Advanced' level on the English proficiency test are exempt from the course requirement					
	Freshman Seminar	CEKS007 CEKS008	[CAREER-ENTREPRENEURSHIP] FRESHMAN SEMINAR I	1(1)	•							
			[CAREER-ENTREPRENEURSHIP] FRESHMAN SEMINAR II	1(1)		•						
	Digital & SW	GECT002 GECT003	[CAREER-ENTREPRENEURSHIP] PROGRAMMING BASICS	3(3)	•							
			[CAREER-ENTREPRENEURSHIP] DATA SCIENCE AND ARTIFICIAL INTELLIGENCE	3(3)		•						
BT	CEBT001	[CAREER-ENTREPRENEURSHIP] THE WORLD OF BIOSCIENCE.	3(3)	•								
Subtotal				19								
Elective general				9								
a Total of General course				28								
Academic foundations		SMRTI01	INTRODUCTION TO SMART SECURITY	3(3)	•							
		SMRTI02	MATHEMATICS FOR SMART SECURITY	3(3)		•						
		SMRTI11	C PROGRAMMING AND PRACTICE	3(4)	•							
		SMRTI12	COMPUTATIONAL LOGIC	3(3)		•						
Major	Required	SMRT201	ALGORITHM AND PRACTICE FOR CRYPTOGRAPHY	3(4)			•					
		SMRT222	MODERN CRYPTOGRAPHY	3(3)				•				
		SMRT262	CYBER ETHICS	3(3)					•			
		SMRT301	AI SECURITY I	3(3)						•		
		SMRT332	SECURE SOFTWARE ENGINEERING I	3(3)							•	
	COSE342	COMPUTER NETWORK	3(3)						•			
Elective				24								
Subtotal				42								
Intensive major	Required											
	Elective											
	Subtotal				36							
Total credits required for graduation*				130								
Note		※ Internship courses can be recognized for up to 18 credits towards the major, including courses offered by the Internship Support Center (courses number starting with COOP). Before course registration, the department will assess their relevance to the major										

[Attachment 2] Undergraduate Courses
【Division of Smart Security】

Category	Course Number	Course Name	Credit (Hour)	Course Number	Course Name	Credit (Hour)
Major Required	SMRT201	ALGORITHM AND PRACTICE FOR CRYPTOGRAPHY	3(4)	SMRT301	AI SECURITY I	3(3)
	SMRT222	MODERN CRYPTOGRAPHY	3(3)	SMRT332	SECURE SOFTWARE ENGINEERING I	3(3)
	SMRT262	CYVER ETHICS	3(3)	COSE342	COMPUTER NETWORK*	3(3)
Major Elective	SMRT203	FORMAL METHODS	3(3)	SMRT431	SECURE SOFTWARE ENGINEERINGII	3(3)
	SMRT205	MATHEMATICS FOR AI SECURITY	3(3)	SMRT433	SECURITY FOR BIGDATA	3(3)
	SMRT221	CRYPTOGRAPHIC MATH	3(3)	SMRT435	SMART SECURITY APPLICATION	3(3)
	SMRT303	INTRODUCTION TO DIGITAL FORENSICS	3(4)	SMRT461	CYBER TECHNOLOGY AND LAW	3(3)
	SMRT344	SOFTWARE REVERSE ENGINEERING	3(4)	SMRT463	PRIVACY PROTECTION	3(3)
	SMRT226	INTRODUCTION TO HACKING	3(4)	SMRT465	CAPSTONE DESIGN I	3(6)
	SMRT242	SECURE CODING	3(3)	SMRT466	CAPSTONE DESIGN II	3(6)
	SMRT302	DATA SECURITY	3(3)	SMRT468	WAY TO SET UP A GREAT STARTUP COMPANY	3(3)
	SMRT321	CRYPTOGRAPHIC PROTOCOL	3(3)	SMRT481	INTERNSHIP I	3(0)
	SMRT322	CRYPTOGRAPHIC APPLICATIONS	3(4)	SMRT482	INTERNSHIP II	6(0)
	SMRT323	COMPUTER SYSTEM SECURITY	3(4)	SMRT483	INTERNSHIP III	12(0)
	SMRT324	COMPUTER NETWORK SECURITY	3(3)	COSE221	DIGITAL LOGIC DESIGN*	3(3)
	SMRT334	RISK MANAGEMENT	3(3)	COSE222	COMPUTER ARCHITECTURE*	3(3)
	SMRT336	AI SECURITY II	3(4)	COSE312	COMPILER*	3(3)
	SMRT338	INTRODUCTION TO DE-IDENTIFICATION	3(3)	COSE341	OPERATING SYSTEMS*	3(3)
	SMRT422	HARDWARE SECURITY	3(3)	COSE451	SOFTWARE SECURITY*	3(3)
	SMRT424	DIGITAL FORENSIC PRACTICE	3(4)	CYDF211	Course 18	3(4)

[Attachment 3] Major Course Schedule

	Mon	Tue	Wed	Thu	Fri
First class 09:00 -10:15	C PROGRAMMING AND PRACTICE (SMRT111)	INTRODUCTION TO SMART SECURITY (SMRT101)	C PROGRAMMING AND PRACTICE (SMRT111)		
	CRYPTOGRAPHIC MATH (SMRT221)		CRYPTOGRAPHIC MATH (SMRT221)		
	CYBER TECHNOLOGY AND LAW (SMRT461)	WAY TO SET UP A GREAT STARTUP COMPANY (SMRT468)	CYBER TECHNOLOGY AND LAW (SMRT461)	WAY TO SET UP A GREAT STARTUP COMPANY (SMRT468)	
Second class 10:30 -11:45	C PROGRAMMING AND PRACTICE (SMRT111)	INTRODUCTION TO SMART SECURITY (SMRT101)			
		MATHEMATICS FOR AI SECURITY (SMRT205)		MATHEMATICS FOR AI SECURITY (SMRT205)	
	OPERATING SYSTEMS (COSE341)		OPERATING SYSTEMS (COSE341)		
Third class 12:00 -13:15				ALGORITHM AND PRACTICE FOR CRYPTOGRAPHY (SMRT201)	
		CRYPTOGRAPHIC PROTOCOL (SMRT321)			CRYPTOGRAPHIC PROTOCOL (SMRT321)
	SECURE SOFTWARE ENGINEERINGII (SMRT431)				
Fourth class 13:30 -14:45					
	COMPUTER NETWORK (COSE342)	AI SECURITY I (SMRT301)	COMPUTER NETWORK (COSE342)	AI SECURITY I (SMRT301)	COMPUTER SYSTEM SECURITY (SMRT323)
Fifth class 15:00 -16:15	DIGITAL LOGIC DESIGN (COSE221)		DIGITAL LOGIC DESIGN (COSE221)		
					COMPUTER SYSTEM SECURITY (SMRT323)
	SECURITY FOR BIGDATA (SMRT433)		SECURITY FOR BIGDATA (SMRT433)		
Sixth class 16:30 -17:45					
	ALGORITHM AND PRACTICE FOR CRYPTOGRAPHY (SMRT201)	FORMAL METHODS (SMRT203)		FORMAL METHODS (SMRT203)	
		INTRODUCTION TO DIGITAL FORENSICS (SMRT303)	COMPUTER SYSTEM SECURITY (SMRT323)	INTRODUCTION TO DIGITAL FORENSICS (SMRT303)	



Seven th class 18:00-1 8:50	ALGORITHM AND PRACTICE FOR CRYPTOGRAPHY (SMRT201)			INTRODUCTION TO DIGITAL FORENSICS (SMRT303)	
---	--	--	--	--	--