스마트보안학부 수강신청 유의사항

○ **사이버국방학과(대외비)**

- 사이버국방학과 수강신청 관련 사항은 행정실(02-3290-4468)로 문의 주시기 바랍니다.

○ **스마트보안학부**

1. 수강신청 기본 안내사항

가. 교육과정은 입학 연도의 교육과정이 적용됩니다.

나. 교육과정 개편에 따라 학번별로 적용되는 교육과정이 상이하므로 교과목 이수에 주의하시기 바랍니다.

다. 수강신청은 반드시 본인이 직접 신청합니다.

2. 수강신청 원칙

가. 수강신청 가능 학점은 최소 1학점 ~ 최대 19학점입니다.

단, 아래의 조건을 하나라도 충족한 경우 추가 3학점 초과 수강 가능합니다.

1) F등급 없이 전체 성적 평점평균이 3.75 이상

2) 직전 학기(정규학기) F등급 없이 18학점 이상 이수하고 평점평균이 3.75 이상

나. 수강신청 기준 학년은 **가진급 학년(2026년 2월 현재 총 취득학점수 기준)**이며 본인의 가진급 학년도에 해당하는 수강신청일에 수강신청을 진행합니다.

다. **유연 수강신청 학점제는 학년도 내에서 최대 3학점까지 선사용하거나 이월하여 활용**할 수 있습니다. 1학기에는 수강 정정 기간에만 선사용이 가능하며, 이월된 학점은 2학기 수강 희망 과목 등록 기간부터 사용할 수 있습니다.

3. 최근 교육과정 개편사항 안내

가. 교과목 폐지 및 변경

1) 4년 미개설 교과목 폐지: 디지털포렌식실무(SMRT424), 스마트보안응용(SMRT435)

2) 캡스톤디자인II(SMRT466) 폐지 및 캡스톤디자인I(SMRT465)의 개설 권장학기 변경(4학년 1학기 → 4학년 2학기)

4. 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 경우의 한에 수강 신청이 가능할 수 있습니다.

나. 강의실 규모와 교과목 특성에 맞추어 수강인원이 제한될 수 있습니다.

다. 수강포기 신청은 1학기 최대 9학점까지 가능합니다. 수강포기 신청은 번복할 수 없으며, 수강포기신청으로 인하여 이수학점이 부족한 경우 졸업요건, 장학금 신청, 성적우수상 선정, 추가수강신청학점 부여 등에 불이익이 있을 수 있으니 유의하시기 바랍니다.

라. 2026-1학기 개설되는 타학과 교과목

학과	학수번호-분반	교과목명	학점인정구분	비고
컴퓨터학과	COSE221-02	논리설계	전공선택	스마트보안학부 교수가 개설한 분반 수강 권고
	COSE341-04	운영체제	전공선택	
	COSE342-03	컴퓨터네트워크	전공필수	
	COSE451-00	소프트웨어보안	전공선택	

마. 학문의 기초(필수)

학번	학수번호	교과목명	학점	시간	강의유형
2026학번	SMRT101	스마트보안개론	3	3	이론중심
	SMRT111	C언어및실습	3	4	이론및실습

바. 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. 졸업 전 게재 확정된 논문을 행정실로 제출해 주시기 바랍니다.

사. 현장실습

현장실습지원센터에서 개설하는 공통교과목에 대한 전공 인정이 가능합니다. 전공인정 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	현장실습	실제근무일 20일
⋮	⋮	⋮	⋮	⋮	⋮	
COOP036	현장실습A6	3	매학기	전공선택	현장실습	
COOP061	현장실습B1	6	매학기	전공선택	현장실습	실제근무일 40일
COOP062	현장실습B2	6	매학기	전공선택	현장실습	
COOP063	현장실습B3	6	매학기	전공선택	현장실습	
COOP091	현장실습C1	9	매학기	전공선택	현장실습	실제근무일 60일
COOP092	현장실습C2	9	매학기	전공선택	현장실습	
COOP121	현장실습D1	12	매학기	전공선택	현장실습	실제근무일 70일(15주)
COOP151	현장실습E1	15	매학기	전공선택	현장실습	

※ 자세한 내용은 현장실습센터 공지사항 확인 부탁드립니다.

※ 같은 이수구분, 같은 학점 수 내에서 교과목 선택은 학수번호 순으로 신청합니다. (다른 학기에 동일한 학점 수로 이수 시 재수강이 아닌 다른 교과목으로 학점을 부여하기 위해 학수번호가 다른 교과목 여러 개로 개설되어 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.

아. 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)

자. 정보보호대학원 학·석사연계과정

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

- 모집학과: 정보보호학과
- 지원 자격: 고려대학교 학부생으로 4학기 이상 등록하고, 총 67학점 이상 취득자로서 성적 평점평균 3.50 이상인 학생
- 접수 기간 : 2026학년도 후기는 2026년 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

2026학년도

구분	내용	학수번호	교과목명	학점(시간)	1차년도		2차년도		3차년도		4차년도	
					Ⅰ	Ⅱ	Ⅰ	Ⅱ	Ⅰ	Ⅱ	Ⅰ	Ⅱ
교양 필수	학문세계의탐구	GELI005	학문세계의탐구Ⅰ	3(3)	•		2024학년도 이후 입학한 외국인 학부생은 GELI007 학문세계의탐구Ⅰ(외국인반), 글쓰기 (외국인반) 이수					
	글쓰기	GEWR002	글쓰기	3(3)	•	•						
	Academic English	IFLS800	Academic English Ⅰ	2(2)	•		신입생 영어능력평가고사 결과 '고급'레벨 취득 학생은 이수 면제					
	1학년세미나	GEKS007 GEKS008	[진로·창업]1학년세미나Ⅰ [진로·창업]1학년세미나Ⅱ	1(1) 1(1)	• 	 •						
	Digital & SW	GECT002 GECT003	[진로·창업]SW프로그래밍의기초 [진로·창업]데이터과학과인공지능	3(3) 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	인공지능보안Ⅰ	3(3)					•			
		SMRT332	시큐어소프트웨어공학Ⅰ	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	인공지능보안I	3(3)
	SMRT222	현대암호학	3(3)	SMRT332	시큐어소프트웨어공학I	3(3)
	SMRT262	사이버윤리	3(3)	COSE342	컴퓨터네트워크*	3(3)
전공 선택	SMRT203	정형기법	3(3)	SMRT433	빅데이터응용보안	3(3)
	SMRT205	인공지능보안수학	3(3)	SMRT461	사이버기술과법	3(3)
	SMRT221	암호수학	3(3) 택1	SMRT463	개인정보보호	3(3)
	MATH223	정수론	3(3)	SMRT465	캡스톤디자인I	3(6)
	SMRT303	디지털포렌식개론	3(4)	SMRT468	스타트업창업방법론	3(3)
	SMRT344	역공학	3(4)	SMRT481	현장실습I	3(0)
	SMRT226	해킹개론	3(4)	SMRT482	현장실습II	6(0)
	SMRT242	시큐어코딩	3(4)	SMRT483	현장실습III	12(0)
	SMRT302	데이터보안	3(3)	COSE221	논리설계*	3(3)
	SMRT321	암호프로토콜	3(3)	COSE222	컴퓨터구조*	3(3)
	SMRT322	현대암호학응용	3(4)	COSE312	컴파일러*	3(3)
	SMRT323	컴퓨터시스템보안	3(4)	CYDF315	과목42 택1	3(3)
	SMRT324	컴퓨터네트워크보안	3(3)	COSE341	운영체제*	3(3)
	SMRT334	위험관리	3(3)	COSE451	소프트웨어보안*	3(3)
	SMRT336	인공지능보안II	3(3)	CYDF211	과목18	3(4)
	SMRT338	개인정보비식별화개론	3(3)			
	SMRT422	하드웨어보안	3(3)			
	SMRT431	시큐어소프트웨어공학II	3(3)			

[붙임 3] 주요 과목 배정시간표

	월	화	수	목	금
1교시 09:00-10:15	C언어및실습 (SMRT111)	스마트보안개론 (SMRT101)	C언어및실습 (SMRT111)		
	암호수학 (SMRT221)		암호수학 (SMRT221)		과목 18 (CYDF211)
	사이버기술과법 (SMRT461)		사이버기술과법 (SMRT461)		
2교시 10:30-11:45	C언어및실습 (SMRT111)	스마트보안개론 (SMRT101)			
		인공지능보안수학(SMRT205)		인공지능보안수학(SMRT205)	과목 18 (CYDF211)
	운영체제 (COSE341)	암호프로토콜 (SMRT321)	운영체제 (COSE341)	암호프로토콜 (SMRT321)	
3교시 12:00-13:15					과목 18 (CYDF211)
			정형기법 (SMRT203)		정형기법 (SMRT203)
4교시 13:30-14:45					
			정형기법 (SMRT203)		정형기법 (SMRT203)
	컴퓨터네트워크 (COSE342)	인공지능보안I (SMRT301)	컴퓨터네트워크 (COSE342)	인공지능보안I (SMRT301)	컴퓨터시스템보안(SMRT323)
		스타트업창업방법론(SMRT468)		스타트업창업방법론(SMRT468)	
5교시 15:00-16:15					
	논리설계 (COSE221)	암호구현및실습 (SMRT201)	논리설계 (COSE221)		
					컴퓨터시스템보안(SMRT323)
	빅데이터응용보안(SMRT433)			빅데이터응용보안(SMRT433)	
6교시 16:30-17:45					
		암호구현및실습 (SMRT201)		암호구현및실습 (SMRT201)	
		디지털포렌식개론(SMRT303)	컴퓨터시스템보안(SMRT323)	디지털포렌식개론(SMRT303)	
7교시 18:00-18:50				디지털포렌식개론(SMRT303)	

Course Registration Notes

Division of Smart Security

Update: January, 2026

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

For inquiries related to course registration in the Department of Cyber Defense, please contact the administrative office at 02-3290-4468.

○ **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

b. A student's year of course registration is determined by the total credit number he/she has earned until winter session, as of February in 2026.

c. The Flexible Credit Course Registration System allows students to pre-use or carry over up to 3 credits within the academic year. For the spring semester, credits can only be pre-used during the course add/drop period, while carried-over credits can be utilized starting from the Pre-Registration of Preferred Courses for the fall semester.

3. What's new

a. Abolition and Modification of Courses

1. Abolition of courses not offered for four years:
Digital Forensics Practice(SMRT424), Smart Security Application(SMRT435)
2. Abolition of Capstone Design II(SMRT466) and change in the recommended offering semester for Capstone Design I(SMRT465)
(from the 1st semester of the 4th year → to the 2nd semester of the 4th year)

4. 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. Please note with care that a course registration drop(waiver) request is final and cannot be reversed, and insufficient credits due to a course registration drop(waiver) request may result in disadvantages in graduation requirements, scholarship applications, selection for academic honors, and granting of additional course credits.

d. Courses Offered by Other Departments in the 2026-1 Semester

Department	Course Number	Course Name	Credit Recognition	Note
Computer Science	COSE221-02	DIGITAL LOGIC DESIGN	Major Elective	Recommended to take the class offered by the Smart Security Faculty
	COSE341-04	OPERATING SYSTEMS	Major Elective	
	COSE342-03	COMPUTER NETWORK	Major Required	
	COSE451-00	SOFTWARE SECURITY	Major Elective	

e. Academic foundations (Mandatory)

Year	Course Number	Course Name	Credit	Hours	Course Type
Students from 2026	SMRT101	INTRODUCTION TO SMART SECURITY	3	3	Theory
	SMRT111	C PROGRAMMING AND PRACTICE	3	4	Theory and Practice

f. Capstone Design course

- Students enrolled in the School of Smart Security must complete at least one of the following courses during their enrollment period: Internship I, II, III, or Capstone Design I, II.
- When taking the Capstone Design course, students are required to write a conference paper based on their research results. Please submit papers that have been confirmed for publication prior to graduation to the administrative office.

g. 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
⋮	⋮	⋮	⋮	⋮	⋮	
COOP036	Field PracticeA6	3	Every semester	Elective Major	Internship	
COOP061	Field PracticeB1	6	Every semester	Elective Major	Internship	Actual work day of 40 days
COOP062	Field PracticeB2	6	Every semester	Elective Major	Internship	
COOP063	Field PracticeB3	6	Every semester	Elective Major	Internship	
COOP091	Field PracticeC1	9	Every semester	Elective Major	Internship	Actual work day of 60 days
COOP092	Field PracticeC2	9	Every semester	Elective Major	Internship	
COOP121	Field PracticeD1	12	Every semester	Elective Major	Internship	Actual work day of 70 days
COOP151	Field PracticeE1	15	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 internship course specifically offered for students in the Division of Smart Security.

h. 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).

i. 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 2026 semester are

expected to be accepted by the end of May 2026.

■ 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 2026

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	GEKS007 GEKS008	[CAREER·ENTREPRENEURSHIP] FRESHMAN SEMINAR I [CAREER·ENTREPRENEURSHIP] FRESHMAN SEMINAR II	1(1) 1(1)	•	•						
	Digital & SW	GECT002	[CAREER·ENTREPRENEURSHIP] PROGRAMMING BASICS	3(3)	•							
		GECT003	[CAREER·ENTREPRENEURSHIP] DATA SCIENCE AND ARTIFICIAL INTELLIGENCE	3(3)		•						
	BT	GEBT001	[CAREER·ENTREPRENEURSHIP] THE WORLD OF BIOSCIENCE.	3(3)	•							
	Subtotal			19								
Elective general				9								
a Total of General course				28								
Academic foundations		SMRT101	INTRODUCTION TO SMART SECURITY	3(3)	•							
		SMRT102	MATHEMATICS FOR SMART SECURITY	3(3)		•						
		SMRT111	C PROGRAMMING AND PRACTICE	3(4)	•							
		SMRT112	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

【Divison 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	CYBER ETHICS	3(3)	COSE342	COMPUTER NETWORK*	3(3)
Major Elective	SMRT203	FORMAL METHODS	3(3)	SMRT433	SECURITY FOR BIGDATA	3(3)
	SMRT205	MATHEMATICS FOR AI SECURITY	3(3)	SMRT461	CYBER TECHNOLOGY AND LAW	3(3)
	SMRT221	CRYPTOGRAPHIC MATH	3(3) Sel 1	SMRT463	PRIVACY PROTECTION	3(3)
	MATH223	NUMBER THEORY	3(3)	SMRT465	CAPSTONE DESIGN I	3(6)
	SMRT303	INTRODUCTION TO DIGITAL FORENSICS	3(4)	SMRT468	WAY TO SET UP A GREAT STARTUP COMPANY	3(3)
	SMRT344	SOFTWARE REVERSE ENGINEERING	3(4)	SMRT481	INTERNSHIP I	3(0)
	SMRT226	INTRODUCTION TO HACKING	3(4)	SMRT482	INTERNSHIP II	6(0)
	SMRT242	SECURE CODING	3(3)	SMRT483	INTERNSHIP III	12(0)
	SMRT302	DATA SECURITY	3(3)	COSE221	DIGITAL LOGIC DESIGN*	3(3)
	SMRT321	CRYPTOGRAPHIC PROTOCOL	3(3)	COSE222	COMPUTER ARCHITECTURE*	3(3)
	SMRT322	CRYPTOGRAPHIC APPLICATIONS	3(4)	COSE312	COMPILER*	3(3) Sel 1
	SMRT323	COMPUTER SYSTEM SECURITY	3(4)	CYDF315	COURSE42	3(3)
	SMRT324	COMPUTER NETWORK SECURITY	3(3)	COSE341	OPERATING SYSTEMS*	3(3)
	SMRT334	RISK MANAGEMENT	3(3)	COSE451	SOFTWARE SECURITY*	3(3)
	SMRT336	AI SECURITY II	3(3)	CYDF211	COURSE18	3(4)
	SMRT338	INTRODUCTION TO DE-IDENTIFICATION	3(3)			
	SMRT422	HARDWARE SECURITY	3(3)			
	SMRT431	SECURE SOFTWARE ENGINEERINGII	3(3)			

[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)		COURSE 18 (CYDF211)
	CYBER TECHNOLOGY AND LAW (SMRT461)		CYBER TECHNOLOGY AND LAW (SMRT461)		
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)	COURSE 18 (CYDF211)
	OPERATING SYSTEMS (COSE341)	CRYPTOGRAPHIC PROTOCOL (SMRT321)	OPERATING SYSTEMS (COSE341)	CRYPTOGRAPHIC PROTOCOL (SMRT321)	
Third class 12:00 -13:15					COURSE 18 (CYDF211)
			FORMAL METHODS (SMRT203)		FORMAL METHODS (SMRT203)
Fourth class 13:30 -14:45					
			FORMAL METHODS (SMRT203)		FORMAL METHODS (SMRT203)
	COMPUTER NETWORK (COSE342)	AI SECURITY I (SMRT301)	COMPUTER NETWORK (COSE342)	AI SECURITY I (SMRT301)	COMPUTER SYSTEM SECURITY (SMRT323)
		WAY TO SET UP A GREAT STARTUP COMPANY (SMRT468)		WAY TO SET UP A GREAT STARTUP COMPANY (SMRT468)	
Fifth class 15:00 -16:15					
	DIGITAL LOGIC DESIGN (COSE221)	ALGORITHM AND PRACTICE FOR CRYPTOGRAPHY (SMRT201)	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)		ALGORITHM AND PRACTICE FOR CRYPTOGRAPHY (SMRT201)	
		INTRODUCTION TO DIGITAL FORENSICS (SMRT303)	COMPUTER SYSTEM SECURITY (SMRT323)	INTRODUCTION TO DIGITAL FORENSICS (SMRT303)	
Seventh class 18:00-18:50				INTRODUCTION TO DIGITAL FORENSICS (SMRT303)	