교과과정

1. 교과과정 일람표
2. 교수요목

1. 교과과정 일람표

선수과목

<table>
<tr><th>구분</th><th>학수번호</th><th>교과목명</th><th>학점</th><th>시간</th><th>비고</th></tr>
<tr><td rowspan="8">선수과목</td><td>IMS 200</td><td>정보보호개론</td><td>3</td><td>3</td><td rowspan="4">정보보호</td></tr>
<tr><td>IMS 210</td><td>암호수학</td><td>3</td><td>3</td></tr>
<tr><td>IMS 301</td><td>네트워크개론</td><td>3</td><td>3</td></tr>
<tr><td>IMS 310</td><td>컴퓨터알고리즘</td><td>3</td><td>3</td></tr>
<tr><td>IMS 301</td><td>네트워크개론</td><td>3</td><td>3</td><td>금융보안</td></tr>
<tr><td>IMS 301</td><td>네트워크개론</td><td>3</td><td>3</td><td rowspan="3">삼성정보
보호전공</td></tr>
<tr><td>IMS 310</td><td>컴퓨터알고리즘</td><td>3</td><td>3</td></tr>
<tr><td>IMS 320</td><td>OS 개론</td><td>3</td><td>3</td></tr>
</table>

연구지도과목

<table>
<tr><th>구분</th><th>학수번호</th><th>교과목명</th><th>학점</th><th>시간</th><th>비고</th></tr>
<tr><td>연구지도</td><td>IMS 500</td><td>연구지도</td><td>2</td><td>2</td><td rowspan="2"></td></tr>
<tr><td>수료연구지도</td><td>IMS 600</td><td>수료연구지도</td><td>0</td><td>0</td></tr>
</table>

기초공통과목

학과		학수번호	교과목명	학점	비고
정보보호, 금융보안	기술	IMS 520	정보보호이론	3	
		IMS 521	보안공학	3	
		IMS 522	사이버법률	3	
	정책	IMS 522	사이버법률	3	
		IMS 523	정보보호기술개론	3	
		IMS 524	정보보호정책	3	
사이버보안		IMS 1001	사이버보안개론	3	
		IMS 1002	보안공학	3	
		IMS 1003	사이버법률	3	
		IMS 1004	정보보호개론	3	
		IMS 1005	CPS보안	3	
공공보안정책		IMS 1101	사이버보안개론	3	
		IMS 1102	사이버법률	3	
		IMS 1103	침해사고대응관리	3	
디지털포렌식		IMS 1201	정보보호이론	3	
		IMS 1202	침해사고대응관리	3	
		IMS 1203	윈도우포렌식	3	
KB금융보안		IMS 1301	정보보호이론	3	
		IMS 1302	보안공학	3	
		IMS 1303	사이버법률	3	
금융보안정책 전공		IMS 520	정보보호이론	3	
		IMS 521	보안공학	3	
		IMS 522	사이버법률	3	
		IMS 693	전자금융보안론	3	2015학번부터
삼성정보보호 전공		IMS 520	정보보호이론	3	
		IMS 522	사이버법률	3	
		IMS 584	네트워크보안	3	
		IMS 836	시스템보안특론	3	
빅데이터 응용및보안		BAS 520	사이버법률	3	
		BAS 521	빅데이터마이닝	3	
		BAS 522	탐색적통계학	3	
공통		IMS 531	기술영어	3	필수 이수 과목 불포함
		IMS 533	기술글쓰기	3	
		IMS 534	세미나 1	0	

정보보호학과 전공과목

분야	학수번호	교과목명	학점	비고
500	IMS 580	암호알고리즘 1	3	
	IMS 581	정보보호프로토콜 1	3	
	IMS 582	패턴인식	3	
	IMS 584	네트워크보안	3	
	IMS 585	접근제어	3	
	IMS 587	위험관리	3	
	IMS 588	정보보호정책	3	
	IMS 590	보안경제학	3	
600	IMS 659	정보화정책론	3	
	IMS 660	이동통신보안	3	
	IMS 665	정보보호프로토콜	3	
	IMS 666	디지털포렌식개론	3	
	IMS 667	개인정보보호정책	3	
	IMS 668	보안장비개발방법론	3	
	IMS 669	암호프리미티브개발실습 1	3	
	IMS 670	암호알고리즘 2	3	
	IMS 671	정보보호프로토콜 2	3	
	IMS 672	유한체이론	3	
	IMS 673	계산이론	3	
	IMS 674	양자암호 1	3	
	IMS 676	정보은닉이론	3	
	IMS 677	악성코드	3	
	IMS 678	실용암호	3	
	IMS 680	OS보안	3	
	IMS 681	생체인증	3	
	IMS 682	멀티미디어보안	3	
	IMS 684	정보보호시스템	3	
	IMS 685	정보보호컨설팅	3	

분야	학수번호	교과목명	학점	비고
600	IMS 686	디지털포렌식법률	3	
	IMS 689	산업보안총론	3	
	IMS 690	SCADA개론	3	
	IMS 691	프라이버시향상기술	3	
	IMS 692	정보보안법제세미나	3	
	IMS 693	전자금융보안론	3	
	IMS 694	데이터베이스보안	3	
	IMS 697	보안소프트웨어개발방법론 1	3	
	IMS 698	보안소프트웨어개발방법론 2	3	
	IMS 699	디지털포렌식정책	3	
700	IMS 704	암호프리미티브개발실습 2	3	
	IMS 705	온라인게임보안	3	
	IMS 706	악성코드및역공학	3	
	IMS 708	침해사고대응관리	3	
	IMS 709	소프트웨어보안	3	
	IMS 710	확률및랜덤과정	3	
	IMS 757	디지털포렌식실무	3	
	IMS 758	법률과정책개론	3	
	IMS 759	정보보호법제	3	
	IMS 763	사이버전	3	
	IMS 764	사이버심리전	3	
	IMS 765	정보체계론	3	
	IMS 766	보안통계학	3	
	IMS 767	신호정보해독	3	
	IMS 768	디지털신호보안	3	
	IMS 769	스마트그리드보안	3	
	IMS 770	현대암호학 1	3	
	IMS 771	현대암호학 2	3	

분야	학수번호	교과목명	학점	비고
700	IMS 772	키관리	3	
	IMS 773	부채널공격방법론	3	
	IMS 774	블록암호	3	
	IMS 775	스트림암호	3	
	IMS 776	공개키암호	3	
	IMS 777	전자서명	3	
	IMS 778	영지식증명	3	
	IMS 779	양자정보이론 1	3	
	IMS 780	양자정보이론 2	3	
	IMS 781	양자암호 2	3	
	IMS 782	인터넷보안	3	
	IMS 783	역공학기법	3	
	IMS 784	침입탐지시스템	3	
	IMS 786	보안토큰	3	
	IMS 788	고급사이버법률	3	
	IMS 790	정보보호관리	3	
	IMS 791	국가정보학	3	
	IMS 792	국가보안학	3	
	IMS 793	정보보호시스템평가방법론 1	3	
	IMS 794	방송통신법	3	
	IMS 795	정보보호시스템평가방법론 2	3	
	IMS 796	포렌식어카운팅	3	
	IMS 798	IT 융합 보안	3	
	IMS 799	사이버안보정책연구	3	
800	IMS 831	정보보호세미나-1	3	
	IMS 832	정보보호세미나-2	3	
	IMS 833	암호알고리즘특론	3	
	IMS 835	양자암호특론	3	

분야	학수번호	교과목명	학점	비고
800	IMS 836	시스템보안특론	3	
	IMS 838	디지털포렌식특론	3	
	IMS 839	정보보호정책특론	3	
	IMS 840	사이버법률특론	3	
	IMS 842	방송통신융합특론	3	
	IMS 843	디지털사회특론	3	
	IMS 845	무선통신네트워크특론	3	

금융보안학과 금융보안전공 전공과목

분야	학수번호	교과목명	학점	비고
500	IMS 580	암호알고리즘1	3	
	IMS 584	네트워크보안	3	
	IMs 590	보안경제학	3	
	IMS 599	보안기술표준분석및구현	3	
600	IMS 662	IT감사기법	3	
	IMS 663	금융암호기술과보안	3	
	IMS 664	전자금융법규	3	
	IMS 666	디지털포렌식개론	3	
	IMS 667	개인정보보호정책	3	
	IMS 685	정보보호컨설팅	3	
	IMS 693	전자금융보안론	3	
700	IMS 702	정보보호관리	3	
	IMS 703	통계와랜덤	3	
	IMS 706	악성코드및역공학	3	
	IMS 708	침해사고대응관리	3	
	IMS 793	정보보호시스템평가방법론 1	3	

사이버보안학과 전공과목

분야	학수번호	교과목명	학점	비고
2000	IMS 2001	보안관제	3	
	IMS 2002	SCADA시스템보안	3	
	IMS 2003	보안정책과경제	3	
	IMS 2004	스마트그리드보안	3	
	IMS 2005	정보보호평가방법개론	3	
	IMS 2006	개인정보보호정책론	3	
	IMS 2007	침해사고대응관리	3	
	IMS 2008	디지털포렌식개론	3	
	IMS 2009	정보보호컨설팅	3	
	IMS 2010	정보보호특론	3	
	IMS 2011	전력망보안	3	
	IMS 2012	네트워크개론	3	
	IMS 2013	위험관리	3	
	IMS 2014	산업보안정책	3	

공공보안정책학과 전공과목

분야	학수번호	교과목명	학점	비고
3000	IMS 3001	정보보호성과관리론	3	
	IMS 3002	위험관리론	3	
	IMS 3003	개인정보보호정책론	3	
	IMS 3004	스마트그리드보안	3	
	IMS 3005	전자금융보안론	3	
	IMS 3006	디지털포렌식개론	3	

디지털포렌식학과 전공과목

분야	학수번호	교과목명	학점	비고
4000	IMS 4001	디지털포렌식실무	3	
	IMS 4002	법과학개론	3	
	IMS 4003	디지털증거법	3	
	IMS 4004	악성코드및역공학	3	
	IMS 4005	전문가증언	3	
	IMS 4006	사이버법률	3	
	IMS 4007	디지털포렌식개론	3	

KB금융보안학과 전공과목

분야	학수번호	교과목명	학점	비고
5000	IMS 5001	정보보호컨설팅	3	
	IMS 5002	전자금융보안론	3	
	IMS 5003	정보보호시스템평가방법론	3	
	IMS 5004	침해사고대응관리	3	
	IMS 5005	디지털포렌식개론	3	
	IMS 5006	보안개발방법론	3	
	IMS 5007	논문세미나	1	논문세미나

정보보호학과 삼성정보보호전공 전공과목

분야	학수번호	교과목명	학점	비고
500	IMS 534	악성코드및역공학	3	전공 필수
	IMS 535	디지털포렌식실무	3	전공 필수
	IMS 537	침해사고대응관리	3	
	IMS 588	정보보호정책	3	
	IMS 592	위험관리론	3	
600	IMS 665	정보보호프로토콜	3	
	IMS 682	멀티미디어보안	3	
	IMS 689	산업보안총론	3	
	IMS 693	전자금융보안론	3	
	IMS 697	보안소프트웨어개발방법론 1	3	
700	IMS 789	정보보호시스템평가방법론	3	
800	IMS 844	보안특강	3	전공 필수

금융보안학과 금융보안정책전공 전공과목

분야	학수번호	교과목명	학점	비고
600	IMS 685	정보보호컨설팅	3	
	IMS 666	디지털포렌식개론	3	
	IMS 693	전자금융보안론	3	
700	IMS 793	정보보호시스템평가방법론 1	3	
	IMS 708	침해사고대응관리	3	
	IMS 760	보안개발방법론	3	

빅데이터응용및보안학과 전공과목

분야	학수번호	교과목명	학점	비고
500	BAS 580	빅데이터기획분석	3	
	BAS 581	빅데이터텍스트마이닝	3	
	BAS 582	빅데이터마이닝이론및실습	3	
	BAS 583	빅데이터세미나 1	3	
	BAS 585	빅데이터사례분석 1	3	
	BAS 586	빅데이터실습	3	

2. 교수요목

[기초공통과목]

<정보보호학과, 금융보안학과 금융보안전공>

- 기술분야 -

IMS 520 정보보호이론 (Theory of Information Security) [3]

정보보호와 관련된 여러 가지 기초적인 이론을 다룬다. 비밀키 암호, 공개키 암호, 해쉬 함수, 전자 서명, 정보보호 프로토콜, 키 관리 등에 관련된 기본 이론을 다룬다.

IMS 521 보안공학 (Security Engineering) [3]

보안공학은 악의, 실수, 또는 재난을 당해도 믿을만한 수준으로 남아있을 시스템 구축을 목표로 삼는다. 하나의 학문으로서 보안공학은 완벽한 시스템을 설계, 구현, 시험할 수 있게 도구, 과정, 방법과 진화하는 환경에 기존의 시스템을 적응시키는 데 중점을 두고, 보안과 관련된 암호이론과 컴퓨터 보안부터 응용심리학, 조직이론, 법률, 정책 등 다양한 내용을 체계적으로 다룬다.

IMS 522 사이버법률 (Cyber Law) [3]

프라이버시와 개인정보보호, 정보보안와 사이버범죄, 지적재산권, 전자거래와 소비자보호, 표현의 자유와 내용규제, 전자서명 등 인터넷 및 사이버 공간에서의 주요 법적쟁점에 관하여 개괄적으로 학습·연구하는 과목이다.

- 정책분야 -

IMS 522 사이버법률 (Cyber Law) [3]

프라이버시와 개인정보보호, 정보보안와 사이버범죄, 지적재산권, 전자거래와 소비자보호, 표현의 자유와 내용규제, 전자서명 등 인터넷 및 사이버 공간에서의 주요 법적쟁점에 관하여 개괄적으로 학습·연구하는 과목이다.

IMS 523 정보보호기술개론 (Introduction to Information Security Technology) [3]

암호학, 접근통제, 네트워크 보안, 포렌식 등 정보보호 정책 연구에 필수적인 기초•응용 정보보호 기술 관련 이론들을 개괄적으로 학습하는 과목으로, 정보보호 정책 연구자들의 정보보호 기술에 대한 이해도를 높여 효과적이고 현실적인 정보보호 기술정책 분석과 개발을 가능하도록 하는 것을 목적으로 한다.

IMS 524 정보보호정책 (Information Security Policy) [3]

변화하는 IT환경에 따라 정보보호와 관련된 정책적 관심과 수요가 점증하고 있는 상황이다. 정보보호정책 과목은 공공 및 민간영역을 규율하는 주요 정보보호 관련 정책의 현황과 이론 체계를 학습하고, 정보보호 정책의 주요 쟁점을 사회과학적으로 해결할 수 있는 연구방법론에 대해 개괄적으로 학습·연구하는 과목이다.

<사이버보안학과>

IMS 1001 사이버보안개론 (Theory of Cyber Security) [3]

사이버 공간 상에서의 보안과 관련된 여러 가지 이슈를 토대로, 사이버 보안을 위한 기초적인 이론을 다룬다. 네트워크 취약점, 보안 프로토콜, 컴퓨터 해킹 등과 관련된 기본 이론을 학습한다.

IMS 1002 보안공학 (Security Engineering) [3]

보안공학은 악의, 실수, 또는 재난을 당해도 믿을만한 수준으로 남아있을 시스템 구축을 목표로 삼는다. 하나의 학문으로서 보안공학은 완벽한 시스템을 설계, 구현, 시험할 수 있게 도구, 과정, 방법과 진화하는 환경에 기존의 시스템을 적응시키는 데 중점을 두고, 보안과 관련된 암호이론과 컴퓨터 보안부터 응용심리학, 조직이론, 법률, 정책 등 다양한 내용을 체계적으로 다룬다.

IMS 1003 사이버법률 (Cyber Law) [3]

프라이버시와 개인정보보호, 정보보안와 사이버범죄, 지적재산권, 전자거래와 소비자보호, 표현의 자유와 내용규제, 전자서명 등 인터넷 및 사이버 공간에서의 주요 법적쟁점에 관하여 개괄적으로 학습·연구하는 과목이다.

IMS 1004 정보보호개론 (Theory of Information Security) [3]

정보보호와 관련된 여러 가지 기초적인 지식을 습득하는 것을 목적으로, 비밀키 암호, 공개키 암호, 해쉬 함수, 전자 서명, 정보보호 프로토콜, 키 관리 등에 관련된 암호 기반 지식을 다룬다.

IMS 1005 CPS보안 (CPS Security) [3]

사이버 물리 시스템(Cyber Physical System, CPS)의 기본 개념을 이해하고, CPS에서의 국내외 보안 이슈들을 분석하여 에너지 산업 보안의 필수 요소인 safety와 security를 만족하는 CPS를 설계하는 것을 목표로 한다.

<공공보안정책학과>

IMS 1101 사이버보안개론 (Theory of Cyber Security) [3]

사이버 공간 상에서의 보안과 관련된 여러 가지 이슈를 토대로, 사이버 보안을 위한 기초적인 이론을 다룬다. 네트워크 취약점, 보안 프로토콜, 컴퓨터 해킹 등과 관련된 기본 이론을 학습한다.

IMS 1102 사이버법률 (Cyber Law) [3]

프라이버시와 개인정보보호, 정보보안와 사이버범죄, 지적재산권, 전자거래와 소비자보호, 표현의 자유와 내용규제, 전자서명 등 인터넷 및 사이버 공간에서의 주요 법적쟁점에 관하여 개괄적으로 학습·연구하는 과목이다.

IMS 1103 침해사고대응관리 (Security Incident Management) [3]

네트워크 취약점, 보안 프로토콜, 컴퓨터 해킹 등과 관련한 기본적·기술적 이론을 학습하고, 이와 관련된 침해사고 발생 시 신속한 대응을 위한 관리방안을 다룬다.

<디지털포렌식학과>

IMS 1201 정보보호이론 (Theory of Information Security) [3]

정보보호이론의 기초 지식에 대해 소개한다. 대칭키와 공개키 암호 알

고리즘과 키 분배 기법을 소개한다.

IMS 1202 침해사고대응관리 (Security Incident Management) [3]

침해 사고 대응에 대한 개념과 이를 위한 소프트웨어와 하드웨어를 소개한다. 또한 침해 사고 대응을 위한 팀 형성 및 로그 분석 기법을 포함하여 전반적인 침해 사고 대응 절차에 대해 소개한다.

IMS 1203 윈도우포렌식 (Window Forensics) [3]

디지털 포렌식 조사 방법을 심도 있게 소개한다. 윈도우 포렌식 기술에 기반하여 EnCase, 레지스트리 분석기, 이미징 도구, 프리패치 분석기와 같은 각종 도구에 대해 배운다.

<KB금융보안학과>

IMS 1301 정보보호이론 (Theory of Information Security) [3]

정보보호와 관련된 여러 가지 기초적인 이론을 다룬다. 비밀키 암호, 공개키 암호, 해쉬 함수, 전자 서명, 정보보호 프로토콜, 키 관리 등에 관련된 기본 이론을 다룬다.

IMS 1302 보안공학 (Security Engineering) [3]

보안공학은 악의, 실수, 또는 재난을 당해도 믿을만한 수준으로 남아있을 시스템 구축을 목표로 삼는다. 하나의 학문으로서 보안공학은 완벽한 시스템을 설계, 구현, 시험할 수 있게 도구, 과정, 방법과 진화하는 환경에 기존의 시스템을 적응시키는 데 중점을 두고, 보안과 관련된 암호이론과 컴퓨터 보안부터 응용심리학, 조직이론, 법률, 정책 등 다양한 내용을 체계적으로 다룬다.

IMS 1303 사이버법률 (Cyber Law) [3]

프라이버시와 개인정보보호, 정보보안와 사이버범죄, 지적재산권, 전자거래와 소비자보호, 표현의 자유와 내용규제, 전자서명 등 인터넷 및 사이버 공간에서의 주요 법적쟁점에 관하여 개괄적으로 학습·연구하는 과목이다.

<금융보안학과 금융보안정책전공>

IMS 520 정보보호이론 (Theory of Information Security) [3]

정보보호와 관련된 여러 가지 기초적인 이론을 다룬다. 비밀키 암호, 공개키 암호, 해쉬 함수, 전자 서명, 정보보호 프로토콜, 키 관리 등에 관련된 기본 이론을 다룬다.

IMS 521 보안공학 (Security Engineering) [3]

보안공학은 악의, 실수, 또는 재난을 당해도 믿을만한 수준으로 남아있을 시스템 구축을 목표로 삼는다. 하나의 학문으로서 보안공학은 완벽한 시스템을 설계, 구현, 시험할 수 있게 도구, 과정, 방법과 진화하는 환경에 기존의 시스템을 적응시키는 데 중점을 두고, 보안과 관련된 암호이론과 컴퓨터 보안부터 응용심리학, 조직이론, 법률, 정책 등 다양한 내용을 체계적으로 다룬다.

IMS 522 사이버법률 (Cyber Law) [3]

프라이버시와 개인정보보호, 정보보안와 사이버범죄, 지적재산권, 전자거래와 소비자보호, 표현의 자유와 내용규제, 전자서명 등 인터넷 및 사이버 공간에서의 주요 법적쟁점에 관하여 개괄적으로 학습·연구하는 과목이다.

IMS 693 전자금융보안론 (Theory of Electronic Financial Security) [3]

본 과목은 전자금융거래에서 발생할 수 있는 정보 유출에 대한 대응방안에 대해서 연구하는 과목으로, 전자금융거래 기반보호 방법과 Audit 방법, 전자금융관련 정보보호 제도, 전자금융사고 사례 분석 및 유형별 대응 방법 등에 대해 강의한다.

<정보보호학과 삼성정보보호전공>

IMS 520 정보보호이론 (Theory of Information Security) [3]

정보보호와 관련된 여러 가지 기초적인 이론을 다룬다. 비밀키 암호, 공개키 암호, 해쉬 함수, 전자 서명, 정보보호 프로토콜, 키 관리 등에 관련된 기본 이론을 다룬다.

IMS 522 사이버법률 (Cyber Law) [3]

프라이버시와 개인정보보호, 정보보안와 사이버범죄, 지적재산권, 전자거래와 소비자보호, 표현의 자유와 내용규제, 전자서명 등 인터넷 및 사이버 공간에서의 주요 법적쟁점에 관하여 개괄적으로 학습·연구하는 과목이다.

IMS 584 네트워크보안 (Network Security) [3]

네트워크상에서 발생할 수 있는 각종 보안 취약 요소에 대해 알아본다. 데이터를 네트워크상에서 주고받을 경우에 발생할 수 있는 보안 취약 요소를 사전에 예방, 발견하거나, 공격자의 공격을 막을 수 있는 방법에 대해 연구한다.

IMS 836 시스템보안특론 (Research in System Security) [3]

시스템보안에 관한 과제, 특히 박사학위 논문과 관련된 문제를 다룬다.

<빅데이터응용및보안학과>

BAS 520 사이버법률 (Cyber Law) [3]

프라이버시와 개인정보보호, 정보보안와 사이버범죄, 지적재산권, 전자거래와 소비자보호, 표현의 자유와 내용규제, 전자서명 등 인터넷 및 사이버 공간에서의 주요 법적쟁점에 관하여 개괄적으로 학습·연구하는 과목이다.

BAS 521 빅데이터마이닝 (Bigdata Mining) [3]

전통적인 데이터분석에 대한 한계와 실행 관점의 이해를 토대로, 개방형 공공정보, Social Network Service, Twitter 등과 같이 주위에 상시 접할 수 있는 빅데이터를 쉽고 빠르게 분석하여, 분석 요인별 그래프나 워드 클라우드 등 의미 있는 형태로 표현해 내는 것에 대해 다룬다.

BAS 522 탐색적통계학 (Exploratory Statistics) [3]

탐색적 데이터 분석은 관측 자료의 특징과 구조를 탐구하는 작업이다. 이를 위하여 다양하고 적절한 통계 그래프, 변수 변환, 로버스트 성질, 모형과의 일치성 검토 등이 요구된다. 이 교과에서는 탐색적 데이터 분석(exploratory data analysis)과 시각화(visualization) 방법을 학습하고 최

근 관심 주제인 사회 네트워크(social network)를 탐구한다.

[전공과목]

<정보보호학과>

IMS 580 암호알고리즘1 (Crypto-Algorithm1) [3]

비밀키 암호 알고리즘, 해쉬함수, 공개키 암호 알고리즘에 대한 구체적인 알고리즘을 살펴보고, 각각의 분야에 대한 기본적인 안전성의 개념을 다룬다.

IMS 581 정보보호프로토콜1 (Information Security Protocol1) [3]

정보보호프로토콜의 개념과 기본적인 프로토콜인 key distribution, identification scheme, authentication code, Secret sharing scheme, pseudo-random number generation, zero-knowledge proof 등에 대하여 학습한다.

IMS 582 패턴인식 (Pattern Recognition) [3]

패턴인식의 기본 이론과 그 실제 사용 예를 배운다. 예를 들어, kNN, VQ, GMM, Neural Network, HMM, SVM 등 최근에 널리 사용되는 여러 가지 기법을 배운다. 또한 인증을 위하여 사용되는 여러 가지 시스템을 분석하고, 실제 간단한 시스템을 구성해 본다.

IMS 584 네트워크보안 (Network Security) [3]

네트워크상에서 발생할 수 있는 각종 보안 취약 요소에 대해 알아본다. 데이터를 네트워크상에서 주고받을 경우에 발생할 수 있는 보안 취약 요소를 사전에 예방, 발견하거나, 공격자의 공격을 막을 수 있는 방법에 대해 연구한다.

IMS 585 접근제어 (Access Control) [3]

유무선 통신상에서 사용자 인증 및 권한 획득에 대한 기술 및 이론을 습득하고, 실제적인 응용 방법에 대하여 연구한다.

IMS 587 위험관리 (Risk Management) [3]

정보시스템 자산에 대한 정량적 가치 평가 방법과 정보시스템 자산 손실 발생 시 대처할 수 있는 방법론에 대하여 연구한다.

IMS 588 정보보호정책 (Information Security Policy) [3]

변화하는 IT환경에 따라 정보보호와 관련된 정책적 관심과 수요가 점증하고 있는 상황이다. 정보보호정책 과목은 공공 및 민간영역을 규율하는 주요 정보보호 관련 정책의 현황과 이론 체계를 학습하고, 정보보호 정책의 주요 쟁점을 사회과학적으로 해결할 수 있는 연구방법론에 대해 개괄적으로 학습·연구하는 과목이다.

IMS 590 보안경제학 (Security Economics) [3]

정보화시대를 이해할 수 있는 경제변화를 소개함으로써 정보가 갖는 경제적 의미와 가치를 이해하고, 정보경제 시대에 현재 경제적 이슈들을 거시 및 미시경제 관점에서 폭넓게 다룬다. 나아가 정보경제 시대에 거론되고 있는 정보보호시장과 최근 화두가 되고 있는 오픈소스, 소셜미디어 등의 경제적 측면을 다루는데 초점을 맞춘다.

MS 659 정보화정책론 (Information Society Policy) [3]

정보화정책은 정보사회와 사회적 가치의 대응과 관련된 정책체제로서, 정보보호정책의 기반이 되는 정보화정책의 학문적 체계와 실증적인 분석에 관한 지식을 습득하고자, 정책학에 기초하여 정책을 형성하고 만들어가는 이론과 방법에 대한 정책 일반론을 이해하고, 실제적인 사례분석으로 정보화 정책 및 정보보호정책의 방향성을 모색한다.

MS 660 이동통신보안 (Security On Mobile Telecommunication) [3]

각종 표준에서 규정한 무선랜의 구조와 주요 보안구조를 분석한다. 보안 메커니즘에 대한 주요 개념을 소개하고, 이과 관련한 보안 메커니즘에 관한 이론을 소개한다.

IMS 665 정보보호프로토콜 (Information Security Protocols) [3]

기본 암호 tool들을 이용한 정보보호 프로토콜들에 대하여 학습한다. 패스기반 인증 및 키 공유, 전자화폐, 멀티캐스트 보안 등 현재 관심이 높은 응용 프로토콜에 대해 학습한다.

IMS 666 디지털포렌식개론 (Introduction to Digital Forensic) [3]

컴퓨터 범죄의 탐지, 조사, 디지털 증거 수집 방법을 다룬다. 아울러 데이터 복구, 암호 해독에 관한 기술을 다룬다.

IMS 667 개인정보보호정책 (Privacy Policy) [3]

정보화의 진전은 국민생활의 질적인 향상을 가져왔지만, 개인정보의 수집활용, 유통이 극대화되면서 개인정보 침해가 증가되었다. 이에 언론, 의료분야, 사이버 범죄 등 세부 분야별로 개인정보 침해에 대한 논고, 판례들을 통해 개인정보보호에 대한 법률적 지식을 습득하는 것을 목적으로 한다.

IMS 668 보안장비개발방법론 (Encryption Device Development Methods) [3]

국가 정보통신보안장비가 각급기관에서 어떻게 운영되는지 각종 운영 방법에 대해 학습한다. 또한 보안장비 개발 시 본 대학원에서 연구한 암호 알고리즘의 적용범위와 방법에 대해 알아본다.

IMS 669 암호프리미티브개발실습1 (Practice in Cryptographic Primitive Development1) [3]

암호학은 정보 기반 사회에서 매우 중요한 분야 중 하나이다. 상용 정보보호 제품을 개발하는 능력을 배양하기 위한 암호프리미티브 개발에 대한 이론과 같은 기반 이론과 공개키 암호, 전자서명, 해쉬함수와 같은 암호프리미티브 및 알고리즘을 구현한다.

IMS 670 암호알고리즘2 (Crypto-Algorithm2) [3]

비밀키 암호 알고리즘, 해쉬함수, 공개키 암호 알고리즘의 안전성을 평가하고, 암호 분석 방법을 다룬다.

IMS 671 정보보호프로토콜2 (Information Security Protocol2) [3]

정보보호프로토콜을 설계하기 위한 기본적인 tool들을 배우고 이를 전자상거래, 전자투표, 전자경매 등 여러 가지 분야에 적용한다.

IMS 672 유한체이론 (Finite Field Theory) [3]

정보보호에 관련된 유한체 이론을 다룬다. 유한체의 구조, 유한체 상의 다항식, 다항식의 인수분해, 특수다항식, 유한체 응용 방법 등을 다룬다.

IMS 673 계산이론 (Computational Complexity) [3]

알고리즘의 복잡도를 분석하고 문제 자체에 내재한 복잡도를 분석한다. 또한 P, NP-class와 각 class의 completeness, 문제간의 reduction에 대하여 학습한다.

IMS 674 양자암호1 (Quantum Cryptography1) [3]

이 강의에서는 양자 역학적 특성이 도청으로부터 안전한 정보 전달에 어떻게 이용될 수 있는지를 논의한다. 이를 위해 개인키 암호, 양자키 분배, BB84 프로토콜 등의 주제를 다룬다.

IMS 676 정보은닉이론 (Information Hiding) [3]

정상적인 데이터 내부에 정보를 은닉하는 기법에 대해서 설명하고, 응용 분야로 저작권 보호, 불법 사용자 추적 기법 등을 다룬다.

IMS 677 악성코드 (Malicious code) [3]

컴퓨터 바이러스, 웜, 트로이 목마와 같은 악성 코드의 동작 원리를 살펴본다. 또한 이를 이용한 여러 가지 공격 도구들에 대하여 공부를 하고, 새로운 공격이 가능한지에 대한 연구도 동시에 수행한다.

IMS 678 실용암호 (Practical Cryptography) [3]

실생활에서 사용되는 암호기술을 습득하고, 암호기술 응용 시 발생할 수 있는 문제점과 보완점에 대하여 연구한다.

IMS 680 OS보안 (Operating System Security) [3]

컴퓨터 원리에 기반한 컴퓨터의 운영체제를 배우며, 특히 보안과 관련된 운영체제 부분을 공부하며, 특히 Unix, Dos, Linux, Window의 보안 관련 부분을 공부하며, 프로그래밍으로 실습을 한다.

IMS 681 생체인증 (Bio-authentication) [3]

생체인식에 대한 개괄적인 특성을 배운다. 또한, 지문인식, 얼굴인식, 화자인식, 장문인식, 홍채인식, 서명인식에 대하여, 여러 가지 이론을 배운다. 이중 한 가지 이론을 학생들이 선택하여, 실제로 시스템을 제작한다.

IMS 682 멀티미디어보안 (Multimedia Security) [3]

멀티미디어는 대용량의 데이터를 실시간 렌더링해야 하는 요구조건 때문에 일반 데이터 보안과 기술적으로 큰 차이를 보인다. 따라서 통신 프로토콜, 암호기술, 저작권보호 등에서 기존의 보안과 다른 이론을 요구한다. 멀티미디어의 속성, 멀티미디어 통신의 요구조건, 보안기술에 대해 체계적으로 다룬다.

IMS 684 정보보호시스템 (Information Security System) [3]

SSL, VPN, 방화벽, IDS 등과 같은 각종 정보보호시스템을 살펴보며, 시스템 구성 과정에서 발생할 수 있는 정보보호 관련 제반 문제점을 다룬다.

IMS 685 정보보호컨설팅 (Information Security Consulting) [3]

정보시스템 전반에 걸친 표준 정책 및 절차를 수립하고 세부적인 활동 방안을 제시함으로써, 고객의 정보시스템에 대한 전반적인 위험관리 체계 구축을 목표로 한다. 변화하는 IT 환경에 따른 정보보호 요구에 부응하는 경쟁력 있는 기술이 뒷받침되어야 한다. 암호 및 인증분야의 핵심기술로 고객의 정보보안 상태를 종합적으로 진단, 대안을 마련하고 시스템 구축, 컨설팅에 이르는 세부사항을 중심으로 설계한 교육을 실시한다.

IMS 686 디지털포렌식법률 (Digital Forensic Law) [3]

사이버 범죄의 최근 판례를 중심으로 강의하여 기술적 측면이 강조되기 쉬운 디지털 포렌식 분야의 법률적 지식을 습득하게 하는 것을 목적으로 한다. 특히 국경 없는 범죄라는 특성을 반영하여 외국 사례와 동향에 대하여 중점 연구한다.

IMS 689 산업보안총론 (Industrial Security) [3]

산업체가 기업의 비밀을 최대한 보호하기 위한 분야별 보안대책에 대해 학습하고 특히 산업기술의 유출을 방지하기 위하여 취해야 할 각종 수단과 방법에 대해 보안사고 사례를 통해 알아본다. 또한 국가보안체계와의 연계성에 대해서도 관찰한다.

IMS 690 SCADA개론 (Introduction to SCADA) [3]

SCADA의 정의 및 구성요소에 대한 기본적인 이해를 통한 실제 적용과정을 학습한다.

IMS 691 프라이버시향상기술 (Privacy Enhancing Technologies) [3]

사용자 프라이버시를 보장하기 위한 여러 기술들을 다룬다. 암호문에 대한 연산, 프라이버시 보장 계산, 프라이버시 보장 데이터 마이닝 등을 다룬다.

IMS 692 정보보안법제세미나 (Seminars on the Information Security Legislations) [3]

사이버법률과 정보통신법제에 관한 개괄적 학습에 이은 전공 심화과정이다. 정보통신기반보호, 시스템보호 등 물리적 정보보안을 관장하는 법규는 물론, 암호활용 및 정보보호산업과 관련된 법규, 공공과 민간의 정보보안을 관장하는 법규, 판례, 관련 정책들도 함께 연구하며, 이를 통해 정보보호 인력으로서의 전문성을 함양한다.

IMS 693 전자금융보안론 (Theory of Electronic Financial Security) [3]

본 과목은 전자금융거래에서 발생할 수 있는 정보 유출에 대한 대응방안에 대해서 연구하는 과목으로, 전자금융거래 기반보호 방법과 Audit 방법, 전자금융관련 정보보호 제도, 전자금융사고 사례 분석 및 유형별 대응 방법 등에 대해 강의한다.

IMS 694 데이터베이스보안 (Database Security) [3]

데이터베이스에 관한 기본 이론과 데이터베이스 시스템에 대한 공격과 방어기법을 배운다. 또한 여러 환경에서 발생하는 데이터들로부터 정보를 추출하는 기법 등을 다룬다.

IMS 697 보안소프트웨어개발방법론1 (Security Software Development Methodology1) [3]

정보보호 이론적 관점에 근거하여 실무에 적용되는 다양한 응용사례를 살펴봄으로써 문제의식 능력과 능동적 대응능력을 배양하고, 정보보호 개발 도구를 학습하여 효율성과 안전성을 만족하는 소프트웨어를 개발하는 방법에 대해 강의한다. 특히, RFID, Sensor, 휴대단말, 스마트 카드 등의 resource constraint한 device에서 구현위주의 실습을 병행한다.

IMS 698 보안소프트웨어개발방법론2 (Security Software Development Methodology2) [3]

RFID, Sensor, 휴대단말, 스마트카드 등의 resource constraint한 device를 위한 다양한 암호 프로그래밍 도구에 대해 학습하고, 이를 기반으로 하여 안전하고 효율적인 보안소프트웨어를 개발하는 능력을 교육하며 구현위주의 실습을 병행한다.

IMS 699 디지털포렌식정책 (Digital Forensics Policy) [3]

디지털 증거의 법적 허용성 강화와 디지털 포렌식의 성공적인 수행 및 활성화를 위해서는 디지털 포렌식 기술뿐만 아니라 효과적인 디지털 포렌식 정책이 필수적으로 요구된다. 본 과목에서는 국내외의 주요 디지털 증거 및 디지털 포렌식 관련 법률과 제도와 다양한 정책적 이슈들을 다룸으로써 정책적 관점에서의 디지털 포렌식에 대한 이해도를 높이는 것을 목표로 한다.

IMS 704 암호프리미티브개발실습2 (Practice in Cryptographic Primitive Development2) [3]

암호학은 정보 기반 사회에서 매우 중요한 분야 중 하나이다. 상용 정보보호 제품을 개발하는 능력을 배양하기 위하 암포프리미티브 개발에 대한 이론과 같은 기반 이론과 공개키 암호, 전자서명, 해쉬함수와 같은 암호프리미티브 및 알고리즘을 구현한다.

IMS 705 온라인게임보안 (Security Issues In Online Games) [3]

인터넷에서 Web과 더불어 가장 성공적인 서비스 중 하나인 온라인게임 상에 어떠한 보안 문제들이 존재하는지 살펴본다. 클라이언트, 네트워크, 서버 단에 존재할 수 있는 위험 및 취약점에 대해 살펴보고, 이에 대한 보안 방안들을 역공학 방지 관점, 네트워크 트래픽 보호 관점, 데이터마이닝 기반의 이상증후 감지 관점에서 도출하여 본다.

IMS 706 악성코드및역공학 (Malware Forensics) [3]

악성코드에 대한 상세한 분석 기법을 다루며, 악성코드 분석을 위한 어셈블리어 및 역공학 도구의 사용법을 익히고 실제 악성코드 분석을 통해 운영체제 및 소프트웨어 체계를 이해할 수 있도록 한다. 또한 역공학 기법의 습득으로 향후 다양한 시스템 조사 및 분석에 기술적 기반이 되도록 한다.

IMS 708 침해사고대응관리 (Security Incident Management) [3]

네트워크 취약점, 보안 프로토콜, 컴퓨터 해킹 등과 관련한 기본적·기술적 이론을 학습하고, 이와 관련된 침해사고 발생 시 신속한 대응을 위한 관리방안을 다룬다.

IMS 709 소프트웨어보안 (Software Security) [3]

소프트웨어 보안에 관한 최근 기술을 다룬다. 바이러스, 웜, 스파이웨어 등의 악성코드 탐지 및 대응기술, 봇넷 및 DDoS 공격 대응 기술, 침임탐지 기법, 안전한 프로그래밍, 소프트웨어 테스팅 등을 포함한다.

IMS 710 확률및랜덤과정 (Probability and Random Process) [3]

Random 벡터, 수열 및 함수, 선형변환, Second Moment 이론, Spectral Densities, Narrowband Processes, Gaussian Processes, Correlation Detection, Linear Minimum Mean Square Estimation에 대해 학습한다.

IMS 757 디지털포렌식실무 (Practical Affairs in Digital Forensic) [3]

사전 계획, 법적 고려사항, 데이터 수집, 분석, 보고서 작성과 같은 실무에 활용할 수 있는 디지털 포렌식 조사 과정에 대해 교육한다. 휘발성 데이터, 용의자의 하드디스크, 모바일 기기와 같은 데이터를 조사하는 것에 대해 학습한다. 또한 추출된 데이터의 재현, 설명, 보고서 작성을 다룬다.

IMS 758 법률과정책개론 (Introduction to Laws And Policy) [3]

정보보호 제도 및 정책의 내용을 이해하기 위하여 법학 개론 및 정책학 개론에 대한 학습을 통해 기본소양을 습득한다.

IMS 759 정보보호법제 (Information Security Laws) [3]

정보보호에 관한 법이론적 접근과 실제사례를 분석하는 과목으로서 정보보안, 개인정보보호와 통신비밀의 보호 등 관련 법적 이론 및 문제를 고찰한다.

IMS 763 사이버전 (Cyber Warfare) [3]

컴퓨터 해킹, 사이버 테러와 같은 컴퓨터 네트워크 시스템 각종 공격 기술에 관하여 연구하고 이를 방비할 수 있는 제반 대책을 알아본다.

IMS 764 사이버심리전 (Cyber Psychological Warfare) [3]

디지털 사회의 특성과 사이버 공간을 이해하고, 인간이 사이버 공간을 통해 경험하고 행동하는 심리학적 원리와 전쟁에 미치는 영향을 개관·학습하는 것을 목적으로 한다. 사이버 냉전과 사이버 공간에서의 사회심리학을 기반으로, 인간의 사고와 행동이 현실 상황과 사이버 공간에서 보이는 유사성과 차이점에 대한 심리학적 연구들을 살펴본다.

IMS 765 정보체계론 (Information Systems) [3]

사이버전의 목표대상인 조직의 정보체계 유형과 활용, 전략정보시스템, 정보기술과 경영혁신, 정보시스템 개발 및 구축과 관리, 정보시스

템 운영 및 평가, 사이버전 대비 연습체계 등에 대하여 체계적인 지식을 다룬다.

IMS 766 보안통계학 (Security Statistics) [3]

통계학 이론을 보안공학에 응용하기 위해 필요한 통계적 기법, 과학적 상식 등을 다룬다. 확률의 기본원리 이해로 부터 선형회귀(linear regression), hypothesis analysis, ANOVA 등을 통하여 보안공학에서의 응용과 실무 연계가 가능한 기초를 다지도록 한다.

IMS 767 신호정보해독 (Signal and Information Processing for Secure Systems) [3]

보안관련 전자장비들로부터 발생하는 신호정보처리에 대해 논문과 실례를 기반으로 신호정보들에 대한 해석 및 처리를 위한 수학적 이론들과 그 응용을 다룬다. 특히 보안과 관련된 중요 신호정보를 해독하기 위한 기존의 신호처리, 응용통계, 그리고 제어계측에 걸치는 여러 제반 기술들(신호변환, 신호추출, 신호복원, 신호예측 및 분류)을 두루 살펴본다.

IMS 768 디지털신호보안 (Security for Digital Signals) [3]

Maltab을 사용하여 digital image forensics에 대한 이미지 처리 및 통계의 기초에 대해 다룬다.

IMS 769 스마트그리드보안 (Security of Smart Grid) [3]

스마트 그리드는 전력과 IT가 융합된 환경으로 일반적인 보안과 다른 접근이 요구된다. 이 과목에서는 스마트 그리드에서의 보안 이슈를 바탕으로, 스마트 그리드를 추진할 때, 고려하여야 할 보안 관점에 대하여 학습한다. 특히, 스마트 그리드의 보안 강화를 위한 기본적인 기술 이론과 더불어 국가보안체계와 연계되는 정책적 수단에 대한 부분을 다룬다.

IMS 770 현대암호학1 (Theory of Modern Cryptology1) [3]

현대 암호이론의 근간이 되는 형식화에 대하여 학습한다. 기본적인 tool인 일방향 함수, hard-core predicates, pseudorandom generator 등에 대하여 배운다.

IMS 771 현대암호학2 (Theory of Modern Cryptology2) [3]

Interactive proof 중의 하나인 zero-knowledge proof에 대하여 학습한다.

Zero-knowledge proofs for NP, witness indistinguishability and hiding, computational sound proof, 그리고 이를 이용한 암호 방법과 전자서명 등에 대하여 배운다.

IMS 772 키관리 (Key Management) [3]

키의 생성, 관리에 따른 제반 문제 및 키 복구 기법 등을 다룬다. 대칭키 시스템과 공개키 시스템에서 키 생성, 관리에 대해서 알아보며 두 시스템 사이의 차이점들을 다루며, 두 시스템을 결합시키는 방법들을 다룬다.

IMS 773 부채널공격방법론 (Side Channel Attacks and Countermeasures) [3]

스마트카드 또는 보안 토큰 등의 하드웨어 보안 장비에 적용 가능한 부채널 방법인 Fault Attack, Timing Attack, Simple Power Attack, Differential Power Attack 등의 공격 방법론과 이의 대응 방법에 대해 소개한다.

IMS 774 블록암호 (Block Ciphers) [3]

블록 암호에 대한 차분 공격, 선형 공격, 연관키 공격, 보간 다항식 공격 등을 소개하고, 이를 C로 구현하여 여러 알고리즘에 실제적으로 적용하여 본다.

IMS 775 스트림암호 (Stream Ciphers) [3]

난수의 통계 평가 방법, 난수열의 각종 복잡도 개념을 소개하고, 스트림 암호의 각종 공격 방법을 연구한다.

IMS 776 공개키암호 (Public-key Cryptosystem) [3]

인수분해, 이산로그 등의 공개키 암호에 대한 기본적인 공격법 및 프로토콜의 적용에 따라 발생하는 제반 문제점을 소개한다. 아울러 각종 공개키 암호에 대한 안전성을 연구한다.

IMS 777 전자서명 (Digital Signature) [3]

기본적인 전자서명 스킴과 특수한 전자서명 스킴을 살펴보고, 이들에 대한 안전성 및 응용에 대하여 살펴본다.

IMS 778 영지식증명 (Zero Knowledge Interactive Proof) [3]

Interactive proof 중의 하나인 zero-knowledge proof에 대하여 학습한다. Zero-knowledge proofs for NP, witness indistinguishability and hiding, computational sound proof, 그리고 이를 이용한 암호 방법과 전자서명 등에 대하여 배운다.

IMS 779 양자정보이론1 (Quantum Information Theory1) [3]

이 강의는 양자 정보 이론의 기본적 개념과 내용을 다룬다. 양자 상태가 정보의 전달에 어떻게 이용될 수 있는지를 논의한다. 이를 위해 quantum operation 의 구조, 양자 잡음의 성질, 양자 정보의 거리 측정에 대해 배운다.

IMS 780 양자정보이론2 (Quantum Information Theory2) [3]

이 강의에서는 양자 상태가 잡음으로부터 어떻게 보호될 수 있는지를 논의한다. 이를 위해 양자정보 전달 과정의 중요한 도구인 에러 보정, 양자 엔트로피와 그 성질, 잡음이 존재하는 채널을 통한 양자 정보의 전달 등을 논의한다.

IMS 781 양자암호2 (Quantum Cryptography2) [3]

이 강의에서는 양자 역학적 특성이 도청으로부터 안전한 정보 전달에 어떻게 이용될 수 있는지를 논의한다. 이를 위해 EPR 프로토콜, 프라이버시와 coherent 정보, 양자키 분배의 안정성 등의 문제를 다룬다.

IMS 782 인터넷보안 (Internet Security) [3]

World Wide Web을 이용한 인터넷 통신에서 고려하여야 할 여러 가지 보안적 관점을 배우고, 특히, SSL과 SET 그리고, https 프로토콜에 대한 정의를 배운다. 여러 가지 모듈 중, 한 가지 모듈에 대한 실제적인 프로그램을 구현한다.

IMS 783 역공학기법 (Reverse Engineering) [3]

바이너리 코드 분석을 위한 각종 도구의 사용법을 익히고 간단한 암호 소프트웨어에 대한 소스를 복원한다.

IMS 784 침입탐지시스템 (Intrusion Detection System) [3]

컴퓨터 시스템에 비인가자의 침입이 발생하였을 때 이를 효과적으로 탐지할 수 있는 기술과 컴퓨터의 각종 소프트웨어/하드웨어 결함을 이

용한 침입 방법을 다룬다. 네트워크를 통하여, 침입을 탐지하는 방법과 호스트를 사용하여 침입하는 방법에 대해서 공부를 하며, 침입 방지 시스템에 대해서도 공부를 한다.

IMS 786 보안토큰 (Cryptographic Tokens) [3]

스마트카드 또는 USB 토큰 등 환경 제약성이 많은 하드웨어 보안장비에 대한 칩 운영체제인 COS와 보안 토큰에 적용 가능한 전자화폐, 전자지갑 등의 응용 시스템에 대해 학습한다.

IMS 788 고급사이버법률 (Advanced Cyber Law) [3]

기존의 법률과 사이버 공간의 법률 간의 비교, 검토를 통한 사이버법률의 이해를 도모하고, 각국의 사이버법률 이론적 원리를 다룬다.

IMS 790 정보보호관리 (Information Security Management) [3]

각 플랫폼별로 보안의 잠재적 취약성을 체계적으로 점검하여, 비즈니스 요구에 적합한 보안 시스템 운영을 다룬다. 경영정보(MIS)기술, 비즈니스프로세스(Business Process), 보안(Security)기술, 시스템제조업체들이 보유하고 있는 정보기술(IT), 인터넷서비스업체(ISP)들이 가지고 있는 인터넷서비스 기술, 교육 및 훈련(Education & Training), 정책 및 절차 등을 고려한 관리기술 등이 종합적으로 구성되어 조직의 보안상황을 체계적으로 진단 분석함으로써 보안 취약점을 해결하는 방법을 연구한다.

IMS 791 국가정보학 (Theory of National Intelligence) [3]

국가의 정보 수집 체계를 살펴보고 관련된 자료, 첩보, 정보의 개념과 사례를 조사한다. 초등적인 자료 수집부터 외사, 방첩, 나아가서 정보전을 종합적인 관점에서 분석한다.

IMS 792 국가보안학 (Theory of National Security) [3]

국가의 보안체계를 살펴보고 잠재적 적국 또는 경쟁국의 정보수집에 대응한 적극적 방어기법과 보안방책을 연구한다. 또한 전통적 보안과 정보보안의 개념 및 보안사고 사례를 분석하고 정보화시대의 정보전의 기술과 능력에 대해 토론을 통해 학습한다.

IMS 793 정보보호시스템평가방법론1 (Information Security System Verification Methods1) [3]

정보보호시스템이 보안 요구 사항과 보증 요구 사항에 맞게 제대로 구현되었는가를 알아볼 수 있도록 하는 각종 방법에 대해 학습한다.

IMS 794 방송통신법 (Broadcasting and Communication Law) [3]

방송통신법은 영문으로 된 방송법, 전기통신기본법, 전기통신사업법의 주요 내용을 살펴보고, 인터넷 등장에 따른 방송통신융합 환경에 적합한 법적 틀을 고찰하고, 미국의 통신법을 비교 연구한다.

IMS 795 정보보호시스템평가방법론2 (Information Security System Verification Methods2) [3]

정보보호시스템이 보안 요구 사항과 보증 요구 사항에 맞게 제대로 구현되었는가를 알아볼 수 있도록 하는 각종 방법에 대해 학습한다.

IMS 796 포렌식어카운팅 (Forensic Accounting) [3]

최근 이슈화되고 있는 국내외 회계 제도의 개혁안을 학습하고, 회계 제도에 대한 법적 기반에 대하여 고찰한다. 본 수업에서는 회계 부정에 대한 분석 기술을 학습하기 위하여 해외의 법적 요소 및 기술 동향을 살펴보며, 이를 통해 포렌식어카운팅에 대한 정의와 함께 회계 부정의 사례에 대하여 학습한다. 특히 미국 E-Discovery에 대한 설명과 함께, 국내 적용 방안에 대하여 학습한다.

IMS 798 IT융합보안 (IT Convergence Security) [3]

정보기술의 융합 환경에 대한 이해를 기초로 하여, 실무에서 적용되는 다양한 IT 융합 기술과 실 사례를 살펴본다. 이를 토대로 IT 융합 기술을 포함하는 환경에서 발생할 수 있는 다양한 보안 문제를 연구하고 정보보호정책 관점에서의 대응전략을 연구한다.

IMS 799 사이버안보정책연구 (Research On Cyber Security Policy) [3]

진화하는 사이버안보에 대한 위협에 대해 알아보고, 사이버안보의 발전 추세와 대응 능력을 확인하여 사이버안보를 강화하기 위한 대응정책을 모색한다.

IMS 831 정보보호세미나-1 (Seminar in Information Security-1) [3]

정보보호 각 분야에 관한 과제, 특히 박사학위 논문과 관련된 문제를 다룬다.

IMS 832 정보보호세미나-2 (Seminar in Information Security-2) [3]

정보보호 각 분야에 관한 과제, 특히 박사학위 논문과 관련된 문제를 다룬다.

IMS 833 암호알고리즘특론 (Research in Cryptology) [3]

암호알고리즘에 관한 과제, 특히 박사학위 논문과 관련된 문제를 다룬다.

IMS 835 양자암호특론 (Research in Quantum Cryptography) [3]

양자암호에 관한 과제, 특히 박사학위 논문과 관련된 문제를 다룬다.

IMS 836 시스템보안특론 (Research in System Security) [3]

시스템보안에 관한 과제, 특히 박사학위 논문과 관련된 문제를 다룬다.

IMS 838 디지털포렌식특론 (Research in Digital Forensics) [3]

디지털포렌식에 관한 과제, 특히 박사학위 논문과 관련된 문제를 다룬다.

IMS 839 정보보호정책특론 (Research in Information Policy) [3]

정보보호정책에 관한 과제, 특히 박사학위 논문과 관련된 문제를 다룬다.

IMS 840 사이버법률특론 (Research in Cyber Law) [3]

사이버법률에 관한 과제, 특히 박사학위 논문과 관련된 문제를 다룬다.

IMS 842 방송통신융합특론 (Research in Broadcasting and Communication Convergence) [3]

인터넷의 활성화로 인한 방송 통신방식의 변화와 서비스 품질의 향상, 전송방식의 변화 등은 방송과 통신의 융합으로 인한 혜택이다. 본 교과를 통해서는 이러한 다변화 시대에서의 방송과 통신의 융합 정책에 대하여 연구하고, 특히 유비쿼터스시대를 지향하는데 따른 적합한 정책 방향을 모색한다.

IMS 843 디지털사회특론 (Research in Digital Society) [3]

디지털화에 따른 정보격차와 사회적 불평등, 권력이동, 사이버 일탈 및 중독과 같은 사회구조적인 문제들을 진단하고 현실적인 대안을 제시

함으로써 사이버 공간에서의 다양한 사회적 관계와 역동적 작용의 주제에 대한 폭넓은 사유를 시도한다.

IMS 845 무선통신네트워크특론 (Research In Wireless Communication Networks) [3]
무선통신 네트워크 프로토콜 기술의 전반적인 내용에 대해 학습한다.

<금융보안학과 금융보안전공>

IMS 580 암호알고리즘1 (Crypto-Algorithm1) [3]
비밀키 암호 알고리즘, 해쉬함수, 공개키 암호 알고리즘에 대한 구체적인 알고리즘을 살펴보고, 각각의 분야에 대한 기본적인 안전성의 개념을 다룬다.

IMS 584 네트워크보안 (Network Security) [3]
네트워크상에서 발생할 수 있는 각종 보안 취약 요소에 대해 알아본다. 데이터를 네트워크 상에서 주고받을 경우에 발생할 수 있는 보안 취약 요소를 사전에 예방, 발견하거나, 공격자의 공격을 막을 수 있는 방법에 대해 연구한다.

IMS 590 보안경제학 (Security Economics) [3]
정보화시대를 이해할 수 있는 경제변화를 소개함으로써 정보가 갖는 경제적 의미와 가치를 이해하고, 정보경제 시대에 현재 경제적 이슈들을 거시 및 미시경제 관점에 폭넓게 다룬다. 나아가 정보경제 시대에 거론되고 있는 정보보호시장과 최근 화두가 되고 있는 오픈소스, 소셜미디어 등의 경제적 측면을 다루는데 초점을 맞춘다.

IMS 599 보안기술표준분석및구현 (Security Standard Analysis and Implementation) [3]
전자금융거래 서비스에 적용된 보안기술과 관련된 기술표준 및 규격을 분석하고, 구현하여 금융권에 적용된 보안기술의 근간에 대한 전반적인 지식을 습득한다.

IMS 662 IT감사기법 (IT Audit Technology) [3]
IT 감사 기본내용을 설명하고 금융기관의 IT시스템 현황과 금융감독당국에서 실시하고 있는 금융부분 IT 감사내용과 평가방법을 다룬다. 특

히 가상 은행을 대상으로 한 자체검사 및 보고서 작성, 경영면담, 강평 등을 직접 수행하도록 하여 졸업 후 실무에 직접 활용할 수 있는 실전 감각을 갖도록 하고, 금융 IT의 문제점과 대안을 연구하여 금융 IT의 새로운 발전방향을 제시한다.

IMS 663 금융암호기술과보안 (Financial Cryptography and Security) [3]

정보보호 제품의 평가기관에서 수행 중인 다양한 평가과정 및 체계를 사례를 통해 습득하여 금융 보안제품에 대해 테스트 계획부터 결과 도출까지 체계적인 평가 능력을 배양하고자 한다.

IMS 664 전자금융법규 (Act of Electronic Financial) [3]

전자금융과 관련된 법규에 대한 이해를 통하여 금융회사 IT시스템에서 요구하는 사항의 명확한 의미를 파악하도록 한다. 국내 관련 법규는 물론 미국 등 해외 국가와 BASEL 등 국제기구에서 발표한 각종 기준을 동시에 다룬다.

IMS 666 디지털포렌식개론 (Introduction to Digital Forensic) [3]

컴퓨터 범죄의 탐지, 조사, 디지털 증거 수집 방법을 다룬다. 아울러 데이터 복구, 암호 해독에 관한 기술을 다룬다.

IMS 667 개인정보보호정책 (Privacy Policy) [3]

정보화의 진전은 국민생활의 질적인 향상을 가져왔지만, 개인정보의 수집활용, 유통이 극대화되면서 개인정보 침해가 증가되었다. 이에 언론, 의료분야, 사이버 범죄 등 세부 분야별로 개인정보 침해에 대한 논고, 판례들을 통해 개인정보보호에 대한 법률적 지식을 습득하게 하는 것을 목적으로 한다.

IMS 685 정보보호컨설팅 (Information Security Consulting) [3]

정보시스템 전반에 걸친 표준 정책 및 절차를 수립하고 세부적인 활동 방안을 제시함으로써, 고객의 정보시스템에 대한 전반적인 위험관리 체계 구축을 목표로 한다. 변화하는 IT 환경에 따른 정보보호 요구에 부응하는 경쟁력 있는 기술이 뒷받침되어야 한다. 암호 및 인증분야의 핵심기술로 고객의 정보보안 상태를 종합적으로 진단, 대안을 마련하고 시스템 구축, 컨설팅에 이르는 세부사항을 중심으로 설계한 교육을 실시한다.

IMS 693 전자금융보안론 (Theory of Electronic Financial Security) [3]

본 과목은 전자금융거래에서 발생할 수 있는 정보 유출에 대한 대응방안에 대해서 연구하는 과목으로, 전자금융거래 기반보호 방법과 Audit 방법, 전자금융관련정보보호 제도, 전자금융사고 사례 분석 및 유형별 대응 방법 등에 대해 강의한다.

IMS 702 정보보호관리 (Information Security Management) [3]

각 플랫폼별로 보안의 잠재적 취약성을 체계적으로 점검하여, 비즈니스 요구에 적합한 보안 시스템 운영을 다룬다. 경영정보(MIS)기술, 비즈니스프로세스(Business Process), 보안(Security)기술, 시스템제조업체들이 보유하고 있는 정보기술(IT), 인터넷서비스업체(ISP)들이 가지고 있는 인터넷서비스 기술, 교육 및 훈련(Education & Training), 정책 및 절차 등을 고려한 관리기술 등이 종합적으로 구성되어 조직의 보안상황을 체계적으로 진단 분석함으로써 보안 취약점을 해결하는 방법을 연구한다.

IMS 702 통계와랜덤 (Satistics and Random) [3]

통계와 랜덤 프로세스 이론을 습득하고, 공학적 응용을 통해 정보보호 관점의 데이터 분석 방법에 대해 다룬다.

IMS 706 악성코드및역공학 (Malware Forensics) [3]

악성코드에 대한 상세한 분석 기법을 다루며, 악성코드 분석을 위한 어셈블리어 및 역공학 도구의 사용법을 익히고 실제 악성코드 분석을 통해 운영체제 및 소프트웨어 체계를 이해할 수 있도록 한다. 또한 역공학 기법의 습득으로 향후 다양한 시스템 조사 및 분석에 기술적 기반이 되도록 한다.

IMS 708 침해사고대응관리 (Security Incident Management) [3]

네트워크 취약점, 보안 프로토콜, 컴퓨터 해킹 등과 관련한 기본적·기술적 이론을 학습하고, 이와 관련된 침해사고 발생 시 신속한 대응을 위한 관리방안을 다룬다.

IMS 793 정보보호시스템평가방법론1 (Information Security System Verification Methods1) [3]

정보보호시스템이 보안 요구 사항과 보증 요구 사항에 맞게 제대로 구현되었는가를 알아볼 수 있도록 하는 각종 방법에 대해 학습한다.

<사이버보안학과>

IMS 2001 보안관제 (Security Monitoring) [3]

보안관제를 위한 다양한 시스템을 살펴보며, 보안관제 시스템에서 발생하는 보안 사고•사례를 분석한다. 보안관제 시스템의 운영 및 관리를 위한 정책 및 절차와 관련된 모범 사례를 연구하여, 보안관제에 대한 전반적인 보안 지식 습득을 목적으로 한다.

IMS 2002 SCADA시스템보안 (Security of SCADA System) [3]

SCADA 시스템의 구조와 더불어 기본적인 보안의 개념을 다룬다. SCADA 시스 템에서 발생할 수 있는 각종 보안 취약요소를 살펴보고, 이를 해결하기 위한 여러 가지 SCADA 보안 기술에 대하여 연구한다.

IMS 2003 보안정책과경제 (Security Policy and Economics) [3]

보안정책에 의해 구성되는 정보보호 시스템 등은 경제적 측면에서 첨단 정보재로서, 특별하게 고려해야 할 주요 요소 가운데 하나이다. 이 과목에서는 정보보호를 위한 보안정책을 수립할 때 고려해야 할 첨단 정보재 시장의 원리를 다룬다.

IMS 2004 스마트그리드보안 (Security of Smart Grid) [3]

스마트 그리드는 전력과 IT가 융합된 환경으로 일반적인 보안과 다른 접근이 요구된다. 이 과목에서는 스마트 그리드에서의 보안 이슈를 바탕으로, 스마트 그리드를 추진할 때 고려하여야 할 보안 관점에 대하여 학습한다. 특히, 스마트 그리드의 보안 강화를 위한 기본적인 기술 이론과 더불어 국가보안체계와 연계되는 정책적 수단에 대한 부분을 다룬다.

IMS 2005 정보보호평가방법개론 (Introduction to Information Security Evaluation Methods) [3]

정보보증(IA)과 이러한 문제에 대한 해결책에 대한 기본적이고 종합적인 이해를 목적으로 한다. 보안 평가 및 시험 기술뿐만 아니라 관련 정책 및 관리 측면에 초점을 맞춘다.

IMS 2006 개인정보보호정책론 (Privacy Policy) [3]

정보화의 진전은 국민생활의 질적인 향상을 가져왔지만, 개인정보의 수집활용, 유통이 극대화되면서 개인정보 침해가 증가되었다. 이에 언론, 의료분야, 사이버 범죄 등 세부 분야별로 개인정보 침해에 대한 논고, 판례들을 통해 개인정보보호에 대한 법률적 지식을 습득하게 하는

것을 목적으로 한다.

IMS 2007 침해사고대응관리 (Security Incident Management) [3]
네트워크 취약점, 보안 프로토콜, 컴퓨터 해킹 등과 관련한 기본적·기술적 이론을 학습하고, 이와 관련된 침해사고 발생 시 신속한 대응을 위한 관리방안을 다룬다.

IMS 2008 디지털포렌식개론 (Introduction to Digital Forensic) [3]
컴퓨터 범죄의 탐지, 조사, 디지털 증거 수집 방법을 다룬다. 아울러 데이터 복구, 암호 해독에 관한 기술을 다룬다.

IMS 2009 정보보호컨설팅 (Information Security Consulting) [3]
정보시스템 전반에 걸친 표준 정책 및 절차를 수립하고 세부적인 활동 방안을 제시함으로써, 고객의 정보시스템에 대한 전반적인 위험관리 체계 구축을 목표로 한다. 암호 및 인증분야의 핵심기술로 고객의 정보보안 상태를 종합적으로 진단, 대안을 마련하고 시스템 구축, 컨설팅에 이르는 세부사항을 중심으로 설계한 교육을 실시한다.

IMS 2010 정보보호특론 (Research in Information Security) [3]
정보보호 각 분야에 관한 과제, 특히 석사학위 논문과 관련된 문제를 다룬다.

IMS 2011 전력망보안 (Electrical Grid Security) [3]
국내외 전력망 보안 기술의 최신 동향을 파악하고 전력망의 위험, 취약성을 분석하고 전력망의 특성에 맞는 보안대책을 수립하는 것에 대해 다룬다.

IMS 2012 네트워크개론 (Introduction to Network) [3]
비전공자를 대상으로 컴퓨터 네트워크에 대한 이해와 정보보호를 위해서 필요한 필수적인 지식 습득을 목적으로 하며, 물리적 계층에 대한 이해인 Data Transmission부터 시작하여 Packet Transmission, Internetworking 등에 대해서 학습한다.

IMS 2013 위험관리 (Risk Management) [3]
에너지 산업 분야의 정보시스템 자산에 대한 정략적 가치 평가 방법과 자산의 위협, 취약점이 될 수 있는 요인을 분석하고, 정보시스템 자산 손실 발생 시 이에 대해 효과적으로 대처할 수 있는 방법론에 대하여

학습한다.

IMS 2014 산업보안정책(Industrial Security Policy) [3]

산업보안은 기업 활동을 위해 보호할 가치가 있는 인원, 문서, 시설, 기술 등 제반 산업기밀의 침해를 방지하고 관계없는 자에게 누설되지 않도록 보호하는 활동으로, 산업보안정책에서는 기업이 보유하고 있는 산업기술을 각종 위험요소로부터 보호하기 위한 이론과 방법론을 다룬다.

<공공보안정책학과>

IMS 3001 정보보호성과관리론 (Information Security Performance Management) [3]

공공부문 정보보호 전담 조직의 업무수행 목적을 확인하고 이를 달성하기 위해 가용 자산을 효율적으로 활용하기 위한 성과지표의 개발 및 이에 대한 계량적 측정방법에 대해 학습한다.

IMS 3002 위험관리론 (Theory of Risk Management) [3]

정보시스템 자산에 대한 정량적 가치 평가 방법과 정보시스템 자산손실 발생 시 대처할 수 있는 방법론에 대하여 연구한다.

IMS 3003 개인정보보호정책론 (Privacy Policy) [3]

정보화의 진전은 국민생활의 질적인 향상을 가져왔지만, 개인정보의 수집활용, 유통이 극대화되면서 개인정보 침해가 증가되었다. 이에 언론, 의료분야, 사이버 범죄 등 세부 분야별로 개인정보 침해에 대한 논고, 판례들을 통해 개인정보보호에 대한 법률적 지식을 습득하게 하는 것을 목적으로 한다.

IMS 3004 스마트그리드보안 (Security of Smart Grid) [3]

스마트 그리드는 전력과 IT가 융합된 환경으로 일반적인 보안과 다른 접근이 요구된다. 이 과목에서는 스마트 그리드에서의 보안 이슈를 바탕으로, 스마트 그리드를 추진할 때, 고려하여야 할 보안 관점에 대하여 학습한다. 특히, 스마트 그리드의 보안 강화를 위한 기본적인 기술 이론과 더불어 국가보안체계와의 연계되는 정책적 수단에 대한 부분을 다룬다.

IMS 3005 전자금융보안론 (Theory of Electronic Financial Security) [3]

본 과목은 전자금융거래에서 발생할 수 있는 정보 유출에 대한 대응방안에 대해서 연구하는 과목으로, 전자금융거래 기반보호 방법과 Audit 방법, 전자금융관련 정보보호 제도, 전자금융사고 사례 분석 및 유형별 대응 방법 등에 대해 강의한다.

IMS 3006 디지털포렌식개론 (Introduction to Digital Forensic) [3]

컴퓨터 범죄의 탐지, 조사, 디지털 증거 수집 방법을 다룬다. 아울러 데이터 복구, 암호 해독에 관한 기술을 다룬다.

<디지털포렌식학과>

IMS 4001 디지털포렌식실무 (Practical Affairs in Digital Forensic) [3]

사전 계획, 법적 고려사항, 데이터 수집, 분석, 보고서 작성과 같은 실무에 활용할 수 있는 디지털 포렌식 조사 과정에 대해 교육한다. 휘발성 데이터, 용의자의 하드디스크, 모바일 기기와 같은 데이터를 조사하는 것에 대해 학습한다. 또한 추출된 데이터의 재현, 설명, 보고서 작성을 다룬다.

IMS 4002 법과학개론 (Theory of Forensic Science) [3]

디지털 포렌식을 통계적으로 해석하고 분석하는 방법에 대해 학습하며, 법과학 연구방법론을 비롯하여 랩실무, 랩안전, 증거보존, 품질보증 등 법과학의 일반적인 내용에 대해 다룬다.

IMS 4003 디지털증거법 (Digital Evidence Act) [3]

디지털 증거의 압수수색 및 증거능력 등 법정절차의 제약 하에서의 디지털 증거수집과 형소법, 형법 및 특별법 등 실체법과 디지털 포렌식 업무와의 조화 등을 연구한다.

IMS 4004 악성코드및역공학 (Malware Forensics) [3]

악성코드에 대한 상세한 분석 기법을 다루며, 악성코드 분석을 위한 어셈블리어 및 역공학 도구의 사용법을 익히고 실제 악성코드 분석을 통해 운영체제 및 소프트웨어 체계를 이해할 수 있도록 한다. 또한 역공학 기법의 습득으로 향후 다양한 시스템 조사 및 분석에 기술적 기반이

되도록 한다.

IMS 4005 전문가증언 (Expert Witness) [3]

포렌식 전문가로 법정에서 증언하기 위해 알아야 하는 각종 지식과 태도, 윤리, 증언 방법에 대해서 배운다.

IMS 4006 사이버법률 (Cyber Law) [3]

프라이버시와 개인정보보호, 정보보안와 사이버범죄, 지적재산권, 전자거래와 소비자보호, 표현의 자유와 내용규제, 전자서명 등 인터넷 및 사이버 공간에서의 주요 법적쟁점에 관하여 개괄적으로 학습·연구하는 과목이다.

IMS 4007 디지털포렌식개론 (Introduction to Digital Forensic) [3]

컴퓨터 범죄의 탐지, 조사, 디지털 증거 수집 방법을 다룬다. 아울러 데이터 복구, 암호 해독에 관한 기술을 다룬다.

<KB금융보안학과>

IMS 5001 정보보호컨설팅 (Information Security Consulting) [3]

정보시스템 전반에 걸친 표준 정책 및 절차를 수립하고 세부적인 활동 방안을 제시함으로써, 고객의 정보시스템에 대한 전반적인 위험관리 체계 구축을 목표로 한다. 암호 및 인증분야의 핵심기술로 고객의 정보보안 상태를 종합적으로 진단, 대안을 마련하고 시스템 구축, 컨설팅에 이르는 세부사항을 중심으로 설계한 교육을 실시한다.

IMS 5002 전자금융보안론 (Theory of Electronic Financial Security) [3]

본 과목은 전자금융거래에서 발생할 수 있는 정보 유출에 대한 대응방안에 대해서 연구하는 과목으로, 전자금융거래 기반보호 방법과 Audit 방법, 전자금융관련정보보호 제도, 전자금융사고 사례 분석 및 유형별 대응 방법 등에 대해 강의한다.

IMS 5003 정보보호시스템평가방법론 (Information Security System Verification Methods1) [3]

정보보호시스템이 보안 요구 사항과 보증 요구 사항에 맞게 제대로 구현되었는가를 알아볼 수 있도록 하는 각종 방법에 대해 학습한다.

IMS 5004 침해사고대응관리 (Security Incident Management) [3]

네트워크 취약점, 보안 프로토콜, 컴퓨터 해킹 등과 관련한 기본적·기술적 이론을 학습하고, 이와 관련된 침해사고 발생 시 신속한 대응을 위한 관리방안을 다룬다.

IMS 5005 디지털포렌식개론 (Introduction to Digital Forensic) [3]

컴퓨터 범죄의 탐지, 조사, 디지털 증거 수집 방법을 다룬다. 아울러 데이터 복구, 암호 해독에 관한 기술을 다룬다.

IMS 5006 보안개발방법론 (Security Development Methodology) [3]

정보보호 이론적 관점에 근거하여 실무에 적용되는 다양한 응용사례를 살펴봄으로써 문제의식과 능동적 대응능력을 배양하고, 정보보호 개발 도구를 학습하여 효율성과 안전성을 만족하는 도구를 개발하는 방법에 대해 강의한다.

<정보보호학과 삼성정보보호전공>

IMS 534 악성코드및역공학 (Malware Forensics) [3]

악성코드에 대한 상세한 분석 기법을 다루며, 악성코드 분석을 위한 어셈블리어 및 역공학 도구의 사용법을 익히고 실제 악성코드 분석을 통해 운영체제 및 소프트웨어 체계를 이해할 수 있도록 한다. 또한 역공학 기법의 습득으로 향후 다양한 시스템 조사 및 분석에 기술적 기반이 되도록 한다.

IMS 535 디지털포렌식실무 (Practical Affairs in Digital Forensic) [3]

사전 계획, 법적 고려사항, 데이터 수집, 분석, 보고서 작성과 같은 실무에 활용할 수 있는 디지털 포렌식 조사 과정에 대해 교육한다. 휘발성 데이터, 용의자의 하드디스크, 모바일 기기와 같은 데이터를 조사하는 것에 대해 학습한다. 또한 추출된 데이터의 재현, 설명, 보고서 작성을 다룬다.

IMS 537 침해사고대응관리 (Security Incident Management) [3]

네트워크 취약점, 보안 프로토콜, 컴퓨터 해킹 등과 관련한 기본적·기술적 이론을 학습하고, 이와 관련된 침해사고 발생 시 신속한 대응을

위한 관리방안을 다룬다.

IMS 588 정보보호정책 (Information Security Policy) [3]

변화하는 IT환경에 따라 정보보호와 관련된 정책적 관심과 수요가 점증하고 있는 상황이다. 정보보호정책 과목은 공공 및 민간영역을 규율하는 주요 정보보호 관련 정책의 현황과 이론 체계를 학습하고, 정보보호 정책의 주요 쟁점을 사회과학적으로 해결할 수 있는 연구방법론에 대해 개괄적으로 학습·연구하는 과목이다.

IMS 592 위험관리론 (Theory of Risk Management) [3]

정보시스템 자산에 대한 정량적 가치 평가 방법과 정보시스템 자산손실 발생 시 대처할 수 있는 방법론에 대하여 연구한다.

IMS 665 정보보호프로토콜 (Information Security Protocols) [3]

기본 암호 tool들을 이용한 정보보호 프로토콜들에 대하여 학습한다. 패스기반 인증 및 키 공유, 전자화폐, 멀티캐스트 보안 등 현재 관심이 높은 응용 프로토콜에 대해 학습한다.

IMS 682 멀티미디어보안 (Multimedia Security) [3]

멀티미디어는 대용량의 데이터를 실시간 렌더링해야 하는 요구조건 때문에 일반 데이터 보안과 기술적으로 큰 차이를 보인다. 따라서 통신프로토콜, 암호기술, 저작권보호 등에서 기존의 보안과 다른 이론을 요구한다. 멀티미디어의 속성, 멀티미디어 통신의 요구조건, 보안기술에 대해 체계적으로 다룬다.

IMS 689 산업보안총론 (Industrial Security) [3]

산업체가 기업의 비밀을 최대한 보호하기 위한 분야별 보안대책에 대해 학습하고 특히 산업기술의 유출을 방지하기 위하여 취해야 할 각종 수단과 방법에 대해 보안사고 사례를 통해 알아본다. 또한 국가보안체계와의 연계성에 대해서도 관찰한다.

IMS 693 전자금융보안론 (Theory of Electronic Financial Security) [3]

본 과목은 전자금융거래에서 발생할 수 있는 정보 유출에 대한 대응방안에 대해서 연구하는 과목으로, 전자금융거래 기반보호 방법과 Audit 방법, 전자금융관련 정보보호 제도, 전자금융사고 사례 분석 및 유형별 대응 방법 등에 대해 강의한다.

IMS 697 보안소프트웨어개발방법론1 (Security Software Development Methodology1) [3]

정보보호 이론적 관점에 근거하여 실무에 적용되는 다양한 응용사례를 살펴봄으로써 문제의식 능력과 능동적 대응능력을 배양하고, 정보보호 개발 도구를 학습하여 효율성과 안전성을 만족하는 소프트웨어를 개발하는 방법에 대해 강의한다. 특히, RFID, Sensor, 휴대단말, 스마트 카드 등의 resource constraint한 device에서 구현위주의 실습을 병행한다.

IMS 789 정보보호시스템평가방법론 (Information Security System Verification Methods) [3]

정보보호시스템이 보안 요구 사항과 보증 요구 사항에 맞게 제대로 구현되었는가를 알아볼 수 있도록 하는 각종 방법에 대해 학습한다.

IMS 844 보안특강 (Topics In Security) [3]

기업 보안체계를 이해하고, 최신 보안위협에 대응하기 위한 보안기술을 연구한다.

<금융보안학과 금융보안정책전공>

IMS 685 정보보호컨설팅 (Information Security Consulting) [3]

정보시스템 전반에 걸친 표준 정책 및 절차를 수립하고 세부적인 활동방안을 제시함으로써, 고객의 정보시스템에 대한 전반적인 위험관리 체계 구축을 목표로 한다. 암호 및 인증분야의 핵심기술로 고객의 정보보안 상태를 종합적으로 진단, 대안을 마련하고 시스템 구축, 컨설팅에 이르는 세부사항을 중심으로 설계한 교육을 실시한다.

IMS 666 디지털포렌식개론 (Introduction to Digital Forensic) [3]

컴퓨터 범죄의 탐지, 조사, 디지털 증거 수집 방법을 다룬다. 아울러 데이터 복구, 암호 해독에 관한 기술을 다룬다.

IMS 693 전자금융보안론 (Theory of Electronic Financial Security) [3]

본 과목은 전자금융거래에서 발생할 수 있는 정보 유출에 대한 대응방안에 대해서 연구하는 과목으로, 전자금융거래 기반보호 방법과 Audit 방법, 전자금융관련정보보호 제도, 전자금융사고 사례 분석 및 유형별 대응 방법 등에 대해 강의한다.

IMS 793 정보보호시스템평가방법론1 (Information Security System Verification Methods1) [3]
정보보호시스템이 보안 요구 사항과 보증 요구 사항에 맞게 제대로 구현되었는가를 알아볼 수 있도록 하는 각종 방법에 대해 학습한다.

IMS 708 침해사고대응관리 (Security Incident Management) [3]
네트워크 취약점, 보안 프로토콜, 컴퓨터 해킹 등과 관련한 기본적·기술적 이론을 학습하고, 이와 관련된 침해사고 발생 시 신속한 대응을 위한 관리방안을 다룬다.

IMS 760 보안개발방법론 (Security Development Methodology) [3]
정보보호 이론적 관점에 근거하여 실무에 적용되는 다양한 응용사례를 살펴봄으로써 문제의식과 능동적 대응능력을 배양하고, 정보보호 개발도구를 학습하여 효율성과 안전성을 만족하는 도구를 개발하는 방법에 대해 강의한다.

<빅데이터응용및보안학과>

IMS 580 빅데이터기획분석 (Bigdata Planning and Analysis) [3]
빅데이터를 분석하는데 필요한 기초지식을 습득하여, 이를 활용한 간단한 프로젝트를 기획하고 수행한다.

IMS 581 빅데이터텍스트마이닝 (Text Mining for Bigdata) [3]
텍스트 마이닝에 대한 개념을 이해하고, 텍스트 마이닝 분석 기법과 툴을 이용한 빅데이터 분석 활용에 대하여 다룬다.

IMS 582 빅데이터마이닝이론및실습 (Bigdata Mining Theory and Practice) [3]
데이터 마이닝의 이론을 익히기 위해 R, Python, Matlab이나 Excel 등 여러 형태의 코딩 기술을 사용하여 문제 설정, 자료 수집, 목표 달성에 이르는 전 과정을 실습을 통해 익힌다.

IMS 583 빅데이터세미나1 (Bigdata Seminar1) [3]
빅데이터 관련 통계 이론 및 논문을 강독하고, 논문작법 이해를 통한 토론을 실시한다.

IMS 585 빅데이터사례분석1 (Biadata Instance Analysis1) [3]

국내의 실전 빅데이터 분석 사례를 살펴보고, 산업영역에의 구체적인 적용 계획 기획 및 이를 구현하는 시스템 설계 방법에 대해 다룬다.

IMS 586 빅데이터실습 (Bigdata Practice) [3]

객관적이고 합리적인 의사결정을 위한 다양한 빅데이터 분석방법을 알아보고, Hadoop을 통한 빅데이터 저장 및 처리, R 소프트웨어를 통한 분석 방법을 실습한다.