강 의 계 획 서

<table>
<tr><td rowspan="2">교 과 목 명</td><td>한 글</td><td colspan="3">현대암호학</td><td rowspan="2">교과목 번호</td><td colspan="6" rowspan="2">109015</td></tr>
<tr><td>영 문</td><td colspan="3">Modern Cryptology</td></tr>
<tr><td>개 설 학 과</td><td colspan="4">컴퓨터공학과</td><td>교과구분</td><td>교양</td><td></td><td>MSC</td><td></td><td>전공</td><td>O</td></tr>
<tr><td>강 좌 번 호</td><td colspan="4">42001</td><td>강의 시간</td><td colspan="6">월 (야) 2,3,4교시</td></tr>
<tr><td>학년 및 학기</td><td colspan="4">4학년 1학기</td><td>선이수 과목</td><td colspan="6">-</td></tr>
<tr><td rowspan="2">이수구분 및
학점(시수)</td><td>교필</td><td>교선</td><td>전필</td><td>전선</td><td>기타</td><td rowspan="2">강의내용 및
학점(시수)</td><td>이론</td><td>설계</td><td>실험</td><td>실습</td><td>기타</td></tr>
<tr><td></td><td></td><td></td><td>3(3)</td><td></td><td>3(3)</td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">담 당 교 수</td><td>성 명</td><td colspan="3">박종혁</td><td>E-mail</td><td colspan="6">jhpark1@snut.ac.kr</td></tr>
<tr><td>TEL</td><td colspan="3">02-970-6702</td><td>Homepage</td><td colspan="6">http://www.parkjonghyuk.net</td></tr>
<tr><td>Room</td><td colspan="3">미래관 325호</td><td>Office Hour</td><td colspan="6">월~금 (10:00-18:00)</td></tr>
<tr><td>교과목 개요</td><td colspan="10">컴퓨팅의 발달과 인터넷의 진화로 현대 사회에서는 많은 정보들이 존재하며 인간 삶을 매우 윤택하게 만들어주었다. 하지만, 해킹 및 바이러스 등 여러 가지 보안 이슈들이 빈번히 발생하고 있다. 이러한 이슈들을 해결하기 위한 기술이 바로 정보보호이며 그 기반이 되는것이 암호학이다.
본 교과목에서는 암호의 개념, 역사 등 기본적인 이론부터 실생활에 사용되는 응용기술까지 현대암호와 관련된 정보보호에 관한 전반적인 이론 및 기초 지식을 학습한다.</td></tr>
<tr><td>교 육 목 표</td><td colspan="10">1) 암호의 개념, 역사를 이해하고, 정보보호 기술의 필요성을 인식한다.
2) 현대 컴퓨터 통신/네트워크 사회에서 사용되고 있는 정보보호 기술을 이해한다.
3) 텀프로젝트 진행을 통해 실무경험을 쌓도록 한다.</td></tr>
<tr><td rowspan="8">학 습 성 과

관 련 도
(L3 = 상)
(L2 = 중)
(L1 = 하)</td><td colspan="8">프로그램 학습성과</td><td>관련도</td></tr>
<tr><td colspan="8">(1) 수학, 기초과학, 공학의 지식과 정보기술을 응용할 수 있는 능력</td><td>L2</td></tr>
<tr><td colspan="8">(2) 자료를 이해하고 분석할 수 있는 능력 및 실험을 계획하고 수행할 수 있는 능력</td><td>L2</td></tr>
<tr><td colspan="8">(4) 공학 문제들을 인식하며, 이를 공식화하고 해결할 수 있는 능력</td><td>L3</td></tr>
<tr><td colspan="8">(6) 복합 학제적 팀의 한 구성원의 역할을 해낼 수 있는 능력</td><td>L1</td></tr>
<tr><td colspan="8"></td><td></td></tr>
<tr><td colspan="8"></td><td></td></tr>
<tr><td>교재 및 참고자료</td><td colspan="10">교재 : 알기쉬운 정보보호 개론, 히로시 유키 지음 (신민철 외 2 공역), 인피니티북스, 2008</td></tr>
<tr><td>활용기자재</td><td colspan="10">칠판(○), 빔프로젝터(○), PC(○), VTR( ), 실습장비( ), 기타( )</td></tr>
<tr><td>학습평가 방법</td><td colspan="10">출석(10%), 과제물 및 팀 프로젝트(40%), 중간고사 (20%), 기말고사 (30%)</td></tr>
<tr><td>기 타 사항</td><td colspan="10">*과제 #1 : 최신 암호응용 / 컴퓨터 보안관련 인터넷 및 자료조사 등을 통해 기술 동향 보고서 작성하여 기한내 제출한다.

* 텀프로젝트 관련
3-4인이 팀을 구성하여 1학기간 프로젝트를 구현하여 학기말에 최종보고서 발표 및 산출물을 시연 한다.</td></tr>
</table>

강 의 진 도 계 획		
주별	강 의 내 용	강 의 방 법, 과제, 평가
1	암호의 세계: 1.암호, 2.암호기술에 의한 보호	강의 개요 수강생 사전설문조사
2	암호의 역사: 1. 시저 암호, 2. 다중 치환암호	이론 강의
3	대칭 암호: 1. 스트림 암호, 2. 블록 암호	이론 강의 * 팀구성
4	블록 암호 모드: 1. ECB 모드, 2. CBC 모드	이론 강의
5	공개키 암호: 1. RSA 공개키 암호, 2. 다른 공개키 암호	이론 강의 *텀 프로젝트 계획서 제출 및 발표
6	하이브리드 암호 시스템: 1. 강한 하이브리드 암호 시스템, 2. 암호 기술의 조합	이론 강의
7	일방향 해시 함수: 1. 일방향 해시 함수 개념, 2. 일방향 해시 함수 예	이론 강의
8	중간고사	중간설문조사 중간고사
9	메시지 인증 코드: 1. 메시지 인증 코드 개념, 2, 메시지 인증 코드 이용하는 예	이론 강의 *과제 #1 : 최신 암호응용 / 컴퓨터 보안관련 기술 동향 보고서 제출
10	디지털 서명: 1. 디지털 서명 방법, 2. 디지털 서명 활용 예	이론 강의
11	인증서: 1. 인증서 만들기, 2. 인증서에 대한 공격	이론 강의
12	키: 1. 키 관리 기법, 2. 키 교환 기법	이론 강의
13	난수: 1. 난수의 성질, 2. 의사난수 생성기	이론 강의
14	정보보호 기술 활용 사례: 1. PGP, 2. SSL/TLS	학습발표 *텀프로젝트 최종보고서 제출 및 산출물 시연
15	기말고사	최종설문조사 기말시험