년도/학기	2015/2	교과목명	보안기초수학	이수구분	1전선	학수번호-분반	EA9212-1	학점	3
교수명	박종환	상담시간	금요일 오후 2시	연구실	I613	전화번호	781-7589		

*교과목개요	The objective of this course is to familiarize students with an undergraduate number theory and its application to modern cryptography. Topics will eventually be oriented toward how to use number theoretic theories to construct several modern cryptographic schemes such as RSA, ElGamal, and DSA crpyto algorithms
*수업운영 방법	The class will be done by 95% of lecture plus 5% of homework checking (assigned to students in the previous class).
*교재 및 참고서적	"Elementary Number Theory" - by Rosen, which is currently 6th edition.
*과제물	Every week homework will be given to students, depending on (appropriate) class schedule. Problems for homework will be extracted from the exercises at the end of each section.

성적평가방법	만점처리기준						
	중간고사	40 %	기말고사	40 %	출결	10	
	기타평가방법	항목명1	과제	비율	10	%	
		항목명2		비율	0	%	
		항목명3		비율	0	%	
		항목명4		비율	0	%	
		항목명5		비율	0	%	

주제별 강의 계획

주	월,일	주제 및 주요내용	수업형태	비고
1주	9/1, 9/2	- Divisibility - Integer Representations	Lecture	
2주	9/8, 9/9	- Prime numbers	Lecture	
3주	9/15, 9/16	- Greatest common divisors and Euclidean algorithm	Lecture	
4주	9/22, 9/23	- Congruences - Chinese remainder theorem	Lecture	
5주	9/30	- Fermat´s little theorem	Lecture	
6주	10/6, 10/7	- Euler´s theorem	Lecture	
7주	10/13, 10/14	- Euler phi-function	Lecture	
8주	10/20, 10/21	Midterm exam.		
9주	10/27, 10/28	- RSA cryptosystem	Lecture	
10주	11/3, 11/4	- Primitive roots	Lecture	
11주	11/10, 11/11	- Index arithmetic	Lecture	
12주	11/17, 11/18	- Primality test	Lecture	
13주	11/24, 11/25	- ElGamal cryptosystem	Lecture	
14주	12/1, 12/2	- Finite fields from polynomials	Lecture	
15주	12/8, 12/9	Final		