



Course Weekly Outline

Course Name: Information Security I

Course Instructor					
E-mail					
Title					
Course Coordinator					
Course Objective	To make students familiar with the basic concepts of applied cryptography, including classical cryptography and modern secret key cryptography.				
Course Description	This is an introductory undergraduate course on cryptography and data security. We will focus on classical and symmetric key cryptography, including block ciphers and their modes of operation. The course will emphasize rigorous mathematical formulations of security goals and aim to train students in spotting weaknesses in designs.				
Textbook	William Stallings, <i>Cryptography and Network Security: Principles and Practice</i> , 6/E, Pearson Education, Inc., 2014.				
References	<p>Charles P. Pfleeger and Shari Lawrence Pfleeger, <i>Security in Computing</i>, John Wiley & Sons, Inc., 2007.</p> <p>Mark Stamp, <i>Information Security Principles and Practice</i>, John Wiley & Sons, 2006.</p>				
Course Assessments	Term Tests	Laboratory	Quizzes	Project	Final Exam
	30%		10%	10%	50%
General Notes					



Course Weekly Outline

Week	Date	Topics Covered	Lab. Experiment Assignments	Notes
1		Introduction Historical Notes		
2		Classical Encryption Techniques Substitution Ciphers		
3		Transposition Ciphers Encryption Machines		
4		Block Ciphers		
5		The Data Encryption Standard		
6		DES Cryptanalysis		
7		Groups, Rings, and Fields		
8		Modular Arithmetic		
9		Polynomial Arithmetic		
10		Finite Fields		
11		Finite Fields of the Form $GF(2^n)$		
12		AES: The Advanced Encryption Standard		
13		AES Strength		
14		Using Block and Stream Ciphers		
15		Modes of Operation		

Instructor Signature:

Dean Signature: