



Course Weekly Outline

Course Name: Information Security II

Course Instructor					
E-mail					
Title					
Course Coordinator					
Course Objective	To make students familiar with the basic concepts and applications of public key cryptography and hash functions.				
Course Description	In the second semester, our focus will mainly be directed to public key cryptography. We will cover topics like hash functions, digital signatures, asymmetric encryption, RSA, public-key infrastructure, key distribution, and various applications. Indeed, we will cover topics like viruses, worms, and operating systems security.				
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	20/2/2016	Issues for Symmetric Key Cryptography: Key Distribution		
2	27/2/2016	Random Number Generation		
3	5/3/2016	Prime Numbers Primality Tests		
4	12/3/2016	Public-Key Cryptography I: General Concepts		
5	19/3/2016	RSA System RSA Security		
6	26/3/2016	Public-Key Cryptography II: Exchanging Secret Session Keys		
7	2/4/2016	Diffie-Hellman System		
8	9/4/2016	Public-Key Cryptography III: Constructing Digital Signatures		
9	16/4/2016	El-Gamal System		
10	23/4/2016	Hashing for Message Authentication Cryptographic Hash Functions		
11	30/4/2016	MACs Schemes		
12	7/5/2016	Malware: Viruses		
13	14/5/2016	Worms		
14	21/5/2016	Trusted Systems		
15	28/5/2016	Mounting Targeted Attacks with Trojans and Social Engineering		

Instructor Signature:

Dean Signature: