

COMPUTER AND COMMUNICATIONS SECURITY

TCOM 5563/ECE 5563

SPRING 2015

Instructor:

Dr. Pramode Verma, Director T-Com
The University of Oklahoma, Tulsa #4405
(918) 660-3236 (Office)
(918) 576-3648 (cell)
E-mail: pverma@ou.edu
Lecture: Room 4216
Time: Wed. 9:00-11:40a.m.

Text:

Cryptography and Network Security by William Stallings, Prentice Hall, Sixth Edition, (2014) ISBN 10: 0-13-335469-5 ISBN 13: 978-0-13-335469-0

Course Objective:

This course provides an introduction to security problems in information and communications. Each of the basic blocks of network security, including conventional and public-key cryptography, authentication, and digital signatures are covered. The course also discusses aspects of administering security. Essential elements of a Quantum Key Distribution System are also covered.

Pre-Course Assignment:

All students are expected to have reviewed the book by Simon Singh, "The Code Book" published by Anchor Books, 1999. (You may borrow a copy of the book from Ms. Wagenblatt for the duration of the course.)

Office Hours:

Generally speaking, students are welcome to see me in my office anytime. For longer consultations, please feel free to book time on my calendar through my assistant, Renee Wagenblatt. Additionally, you can also see me without an appointment immediately after any class.

**Course Schedule
Spring 2015**

Date	Subject	Notes
Wed 14 Jan	Introduction to Security, Classical Encryption Techniques	Review of Chapters 1 & 2 Please review them prior to the first class.
21 Jan	Block Ciphers & Data Encryption Standard	Chapters 3
28 Feb	Number Theory and Finite Fields	Chapter 4
4 Feb	Advanced Encryption Standard	Chapter 5
11 Feb	Block Cipher Operation and Stream Ciphers	Chapters 6 & 7
18 Feb	Number Theory	Chapter 8
25 Feb	Mid-term quiz no. 1 (closed book) Review of material covered to date	
4 Mar	RSA Cryptography	Chapter 9
11 Mar	Other Public-key Cryptosystems	Chapter 10
18 Mar	Spring break	
25 Mar	Hash Functions and MAC	Chapters 11 & 12
1 Apr	Digital Signatures and User Authentication	Chapters 13, 14, & 15
8 Apr	Quantum Cryptography	Material to be supplied
15 Apr	Quantum Cryptography	Material to be supplied
22 Apr	Mid-term Quiz No. 2 (Closed Book)	
29 Apr	Projects: Student Presentations on Network Level Security	Chapters 16, 17, 18 & 19
6 May	Projects: Student Presentations Final Take-home Exam—due 5/8 5:00pm (Entire subject matter)	

Course Requirements:

Homework			20%
Quiz No. 1	1-hour	Feb 25	20%
Quiz No. 2	1-hour	April 22	20%
Project			20%
Final Examination	Take-home	May 8 5:00 (due)	20%
Total			100%

Semester grades will be determined as follows:

A	90% - 100%
B	80% - 89%
C	70% - 79%
D	60% - 69%
F	59% or below

Any student in this course who has a disability that may prevent him or her from fully demonstrating his/her abilities should contact us as soon as possible so that appropriate accommodations can be made to ensure full participation and fair assessment of performance.