

ECE802: Cryptography and Network Security

Course Information

Instructor: Dr. Jian Ren
Office: 2215 EB
Phone: 353-4379
Email: renjian@egr.msu.edu
Website: <http://www.egr.msu.edu/~renjian/teaching/ece802.htm>
Class Hours: MWF: 11:30am-12:20am
Classroom: Wells Hall, C304
Office Hours: MW: 1:30-3:00pm or by appointment

Text

- Cryptography and Network Security - Principles and Practice, Third Edition, by William Stallings, ISBN: 0-13-091429-0. Prentice-Hall, Inc., 2003

Major References

- Cryptography and Data Security, by Dorothy Denning, Addison-Wesley, ISBN: 0-201-10150-5
- Wireless Communications and Networks, by William Stallings, Prentice-Hall, Inc.
- Computer Networks, Fourth Edition, by Andrew S. Tanenbaum, Prentice-Hall, 2003

Course Description

This course gives a broad introduction to classical and modern cryptography theory. The students will learn about network security principles and practices. Wireless security for the two most popular wireless communication standards CDMA and GSM will be discussed from both the physical layer and network layer perspectives. Upon completion of this course, students should be able to build security related protocols and applications, solve network security problems using cryptographic techniques, analyze the security of existing network systems and provide suitable security countermeasures to the variety of security threats across the spectrum of computing.

Course Outline

1. Symmetric ciphers
 - (a) Classic encryption techniques
 - (b) Block ciphers and data encryption standard (DES)
 - (c) Advanced encryption standard (AES)
 - (d) Confidentiality using symmetric encryption
2. Public-key encryption
 - (a) Public-key cryptography: RSA and ElGamal

- (b) Key management
 - (c) Message authentication and hash functions
 - (d) Digital signature and non-repudiation
3. Computer Networks and Internet
- (a) What is Internet?
 - (b) Reference models: OSI vs. TCP/IP
 - (c) Hybrid Model
 - (d) Seven-layer Introduction
4. Network security practices
- (a) Authentication applications
 - (b) Electronic mail security
 - (c) IP security
 - (d) Web security
5. System security
- (a) Intrusion detection
 - (b) Firewalls
6. Wireless Security
- (a) Why is wireless communication different from wireline communication?
 - (b) CDMA security
 - (c) GSM security

Grading Policy

Homework	20%
Exam 1	20%
Exam 2	20%
Project 1	20%
Final Project	20%

Final Project is due on Monday December 8 10:00am

Homework

Assignments will be given in class. The due dates are one week after the assignments unless announced otherwise. **Late homework and project will not be graded.**

Email policy

When sending emails to me regarding this course, make sure you always start the subject with “ECE802”.