DEPARTMENT OF ELECTRICAL ENGINEERING
University of Washington
Autumn Quarter 2014

Course: EE 418

Title: Network Security and Cryptography

Credit: 3 Units

Lecture Time: Tuesday, Thursday, 2:30pm - 3:50pm

Lecture Room: EEB 045

Course Instructor: Professor Radha Poovendran
E-mail: RP3@uw.edu
Office: EE 434

Instructor Office Hours: TBD, EE 434

Graduate Teaching Assistant: Mr. Phillip Lee
E-mail: leep3@uw.edu

Teaching Assistant Office Hours: Tentative Monday, 3pm-4pm, Sieg 126

Problem Solving Session: Tentative Thursday, 11am-12pm, Sieg 128

Course Hours:

Schedule	Mon	Tues	Wed	Thurs	Fri
10:00 - 11:00					
11:00 - 12:00				TA OH	
12:00-1:00					
1:00 - 2:00					
2:00-2:30					
2:30-3:00		Lecture		Lecture	
3:00-4:00	TA OH	Lecture		Lecture	

Textbook: D. Stinson, *Cryptography: Theory and Practice*, Third edition, Chapman & Hall/CRC.

Lecture notes will be available on class website.

Homework: There will be weekly homework that **will be due in class** on the date indicated in the assignment.

Course Goal: To develop an understanding of the fundamental principles of cryptography and its application to network and communication security. This course will serve as an introduction to the fundamental tools in cryptography and the protocols that enable its application to network and communication security. In details this course serves an introduction to the basic theory and practice of cryptographic techniques used in computer security. We will cover topics such as encryption (secret-key and public-key), digital signatures, authentication of entities, key management, cryptographic hashing, wireless security. The course projects are used to introduce emerging topics such as RFID security, sensor network security, modeling and mitigation of attacks, privacy in social networks.

Topics/Approximate time table:

1. Chapter 1 from Stinson: Introduction to classical Cryptography and Cryptanalysis (1 week)
2. Chapter 4 from Stinson: Motivation and introduction to hash functions (1.5 weeks)
3. Chapter 5,6 from Stinson: The public key cryptography based on discrete logarithms and factorization (2 weeks)
4. Chapter 7 from Stinson: Digital signature schemes (1 week)
5. Chapter 10 from Stinson: Key distribution (2 weeks)
6. Advanced Topics including trust establishment in social networks, authentication systems and vulnerability analysis in mutual authentication protocols
7. Security metrics and their usage.

Reference Books: **Additional materials that are useful for reading.**

Optional: Network Security: Private Communication in a Public world by C. Kaufman, R. Perlman, and M. Speciner, Prentice Hall, 2002.

Optional: Cryptography and Network Security, 3rd edition, by W. Stallings, Prentice Hall.

Optional: Applied cryptography by B. Schneier.

Optional: Handbook of Applied Cryptography by A. Menezes, P. Van Oorschot, S. Vanstone, available on line.

Exams: There will be two exams. The midterm exam will be held **in class Thursday, November 20**. The final exam will be **in class on the date to be published by the UW.**. All exams are open notes and book.

Projects: There will be two class projects.

Grading: Grading is based as follows:

1. Homework: 20%
2. Exam 1: 20%
3. Exam 2: 20%
4. Project 1: 20%
5. Project 2: 20%

Web Page: The EE418 Web Page is located at

http://www.ee.washington.edu/class/418/2014aut/

or can be accessed from the Classes list on the Electrical Engineering Department homepage. On it are announcements about the class, a list of our office hours, and all handouts from the class.

EPost: There will be a link from the course web page to a message board. **Use this board to post and discuss questions about the homework, projects, and lectures. We will be monitoring it daily.**

Email: Questions about homework and exams be posted on the class discussion board.