

# CS549: Cryptography and Network Security (Spring 2012)

## Description and Goals

The course will start with a review of necessary background topics such as number theory, basic conventional encryption methods, basic public key cryptosystems, basic digital signature systems, and zero knowledge proof systems. We will then discuss applications of cryptography in different fields, such as wireless sensor networking, RFID, mesh networks, cloud computing and mobile social networks. New and emerging topics in both theoretical research and applications will be presented as well.

The goal of the course is to provide students with the necessary foundations to apply cryptography techniques in new and emerging fields. The focus of this class is to discuss and understand the security challenges in emerging systems, and wireless networks.

## Administrivia

- 1) Classroom: Stuart Building 238
- 2) Date/Time: W 6:25pm-9:05pm (see [IIT calendars](#) for holidays, such as Spring Break starting on Mon, March 19, 2012),
- 3) Class Dates: Jan 9<sup>th</sup> to April 28, 2012.
- 4) Instructor: [XiangYang Li](#); Electronic contact: xli at cs dot iit dot edu; Office: SB 229C; Office hours: M, W: 2-3pm
- 5) Teaching Assistant: ShaoJie Tang; Email: stang7@hawk.iit.edu, Office: SB 019B, Office Hours: Friday 1PM to 3PM.
- 6) Course Lectures: See the following [links](#) for the course schedule and lectures (most are from old lectures <http://www.cs.iit.edu/~cs549/cs549s07/lectures.htm>)
- 7) Paper Presentation: See [this link](#) for the list of papers to be presented, and the [term project group](#) information.

## Prerequisites

Undergraduate/graduate courses in number theory, algorithms, networking, and programming are preferred but not required. However, the course will provide a short review on the necessary background material. Finally, it is assumed that the students are familiar with some programming language, such as C.

## Books and Suggested Readings

There is no mandated textbook. Recommended books are:

### Cryptography and essentials

1. *Modern Cryptography: Theory and Practice*, by Wenbo Mao, [Prentice Hall PTR, 2003](#)
2. *Cryptography: Theory and Practice*, by Douglas R. Stinson, CRC press, hardcover.

3. *Handbook of Applied Cryptography*, by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. CRC Press, 1996.
4. *Foundations of Cryptography*, vol. I (2001) and vol. II (2004), by Oded Goldreich. Cambridge Press.

## Network Security

1. *Cryptography and Network Security: Principles and Practice*, by William Stallings, Prentice Hall, Hardcover. Fifth Edition is out also. See <http://williamstallings.com/Crypto3e/Crypto3e-student.html> for student online help.
2. *Network Security Essentials: Applications and Standards*, by William Stallings. Prentice Hall, Hardcover, Published November 1999, 366 pages, ISBN 0130160938
3. *Secrets and Lies: Digital Security in a Networked World* by Bruce Schneier John Wiley, Published August 2000, 412 pages, ISBN 0471253111.

## Introduction to number theory

1. D. Angluin: *Lecture Notes on the Complexity of Some Problems in Number Theory*. Available for download from Tal Malkin's website at Columbia. This is a short review of number theory and its computational aspects. It is sufficient for the needs of our class.
2. V. Shoup: *A Computational Introduction to Number Theory and Algebra*. This is a very comprehensive introduction to algorithmic number theory, with all the necessary mathematical background self-contained. This is a BETA version, but in good shape.
3. *A Course in Number Theory and Cryptography* (Graduate Texts in Mathematics), (Hardcover) by Neal Koblitz
4. *Number theory with computer applications*, by Ramanujachary Kumandari and Christina Romero (1998)
5. *Fundamental Number Theory with Applications*, 1998 edition, by Richard Mollin;

## Excellent Online Lecture Notes

1. S. Goldwasser and M. Bellare: [Lecture Notes on Cryptography](#). These are notes from a summer cryptography class given by Profs. Shafi Goldwasser and Mihir Bellare at MIT. The treatment here is focused on the theoretical foundations of cryptography.
2. M. Bellare and P. Rogaway: [Lecture Notes](#) for a *graduate cryptography course at UCSD*. The approach here is still aimed towards precise definitions and provable security, although more emphasis is given to practical considerations.
3. J. Katz' lecture Notes for the [Intro to Crypto](#) class taught at University of Maryland.

There are also some good links from my homepage:  
<http://www.cs.iit.edu/~xli/confref.html>

## Tasks and Grading Policy

This is **tentative** grading policy for non-India session, and the instructor reserved the right to do small changes.

- a) **Class attendance and paper presentation (15%)** (Students are expected for form study group. Each group is expected to read several papers from a chosen topic and be able to lead the discussion about the papers in this topic.)
  - 1) The technical paper presentation is a group project. The group is SAME as the group for term project. However, EACH student in the group needs to read the papers, and be present at the presentation. Each student should be ready to answer any questions by the students or instructor during the presentation.
  - 2) We will do attendance monitoring. You can miss one class at most among all monitored class attendances.
  - 3) The attendance accounts for 5%. Paper presentation counts for 10%.
  - 4) Each group needs to first select a topic from the list of topics listed in our class webpage. Each group then needs to present a comprehensive summary of papers from the chosen topic. The selection of the topic from the list is first-come-first-service. No TWO groups of students are allowed to select the SAME topic.
  - 5) The paper is selected from the list of papers provided by me (you can also suggest some really good papers to present, but this needs to be approved by the instructor before you can present this paper).
  - 6) Send the group information (list of the names and student IDS) to TA, and the selection of the technical topics to be presented no later than 4<sup>th</sup> week of the semester.
  - 7) Each presentation will last 25 minutes (20 minutes for presentation and there are additional 5 minutes for Q&A). Thus, each class can host at most 6 presentations. For presentation, each group will present the papers at the order of the topics (thus, do NOT need to reserve a timeslot for presentation at specific days). The timeslots will be assigned by the instructor.
  
- b) **One term paper report (15%)** (a research paper or survey paper that successfully addressed some challenging questions).

- 1) The term paper is an individual project. The technical ideas about your term paper could come from the papers presented in the class or some other conferences. If the ideas are from the term project, the team members should NOT collaborate in writing the term paper. You cannot COPY any material from any segment of results written by others (online material or published books, papers, reports), unless you need to cite some results or statements and clearly indicate in your report.
  - 2) You need to write a final research paper. The paper should be of **8-15 pages and in IEEE conference format**. The paper is due on **April 27<sup>th</sup>, 2012**. Upload your paper in PDF format to blackboard and naming the file using your name and additional info so that your file name will be unique.
- c) **One term project (20%)** (term project is formed by a team of students, but the team size should have TWO students. We will NOT allow group with 3 or more than 3 members). This project is about programming and implementation.
- 1) The term project is proposed by students, i.e., yourself (or you can choose from the list of programming assignments given by me). You need to carefully think about this project. You have to really implement the project and show that it works. See programming assignments for details.
  - 2) Each group needs to discuss the term project with the instructor before **Feb 1<sup>st</sup>, 2012**. Each group needs to submit a **2 page project proposal** by the end of the **4th week (Feb 4<sup>th</sup>, 2012)**. Upload this to blackboard for your group.
  - 3) Each student in the group will be graded equally unless it was reported to me and confirmed that some student did not do sufficient work for the project.
  - 4) Each group needs to do a **10 min presentation** at the end of the semester to demo the final results of your project (**April 25<sup>th</sup>, 2012**). Thus, each class can host at most 10 presentations. For presentation, each group will need to reserve a timeslot (numbered 1 to 10) for presentation at specific days.
    - a. **Presentation Final:** covers the following material:  
Explain your design. Discuss design alternatives, cryptography and network security aspects of your project, such as algorithms, data to show the performance of your systems, system architecture. The challenges faced by your group in implementing the project and how you address these challenges; Lessons learned from the project, and future plan for

the project. Management aspects such as your project plan, critical paths, means of team communication (e-mail, chat room, meetings, version control system).

- b. Bring your own laptop to present slides and to demo your application. The presentation should demo your implementations of some real systems. Your group needs to run your application or demo your system. Demonstrate what it does for its users. Show that your system functions properly. You also need to submit the programming codes that work properly.
- c. You can arrange special timeslot for project demo if you receive permission from the instructor before **April 21<sup>st</sup>, 2012**.
- d) **One final exam for this course (30%)**. The exam will be held before the final exam week. It will cover all materials covered in the lectures.
- e) **Two homework problem-sets (each 10%, total 20%)**.
  - 1) Homework problem sets will also be posted at the blackboard. Download the PDF files of the homeworks from the class webpage or from the blackboard. You need to upload your written solution to blackboard.
  - 2) Homework 1, PDF file, homework 2 PDF file.

#### **The tentative grading policy for India session:**

**Homework 20%, final exam 40%, individual term programming project 25%, individual term paper 15%**. Notice that, all programming projects and paper writing projects are individual effort (not group project). You have to propose your own programming project (by sending email to TA). You also need to send TA an email about the topics you will work on and write a technical paper (it could be a well thought survey paper on a given topic, or a research paper on an open question, or some nice protocol design and analysis on some interesting topics).

#### **Other policies:**

- a. You may take an automatic extension by handing in the homework assignment on the specified extended due date (one week) and time but with **10% deduction** on this homework grade.
- b. No late assignments handed in after the extended deadline will be accepted. Requests for an additional extension will almost always be denied.
- c. In this course you are allowed to discuss the problems with your classmates, and to work together. If you choose to do so, please indicate the name(s) of the people with whom you have worked. Otherwise, it will be treated as cheating! Keep in mind that you may discuss *assignment problems, general proof strategies, or general algorithms* with other students in the course, but you may not collaborate in *the detail development or actual writing* of problem sets. You

need to upload your solution to the blackboard. For convenience, you can also submit additional hard-copy to TA. Please help us by stapling all written pages, labeling them with your name, and clearly labeling each problem. You don't want us to lose part of your assignment or not see your answers, do you?

- d. The term **project** and paper **presentation** is a **team** project; each team will have 2 team members from the class. **All** students are required to do team project (exceptions will only be made for remote students who cannot form a team). All members in each team will be graded equally for the team project unless it has been verified that some students contribute significantly less.
- e. The term **paper** must be an **individual** effort, and thus written and submitted **individually**. Notice that it should be the result of individual effort. Examples of individual term paper include, but are not limited to, 1) survey on some research topics, 2) successful addressing of some challenging research questions. It is encouraged that you discuss with your classmates on the research topics. The term paper should be written in conference format.
- f. If you are remote students who cannot form a team with other students, term project and term paper will be individual effort. Note that you still need to term project and term paper. If you are remote student and cannot do your presentation in the classroom, you can prepare PPT, video-tape your presentation, and send me your files. We can then play your presentation of the paper in classroom.

### **Tentative Grading Policy**

To get A, you need perform well in all aspects of the class. Generally, (this is tentative, so the instructor reserves the right to change the scale here.),

- 1) For all students, you get grade A, if your score is at least 87 (out of maximum 100). You get B, if your score is [75, 86], and C if your score is [60,74].
- 2) For undergraduate students, you will get D if your score is [50,59] and you will get E if your score is [0,49].
- 3) For graduate students, you will get E if your score is [0,59].

### **Term Paper Ideas:**

- 1) Reading papers on some related topics, and then writing a comprehensive survey on some topics. Examples of topics: trustworthy computing, security issues in cloud computing, security issues in wireless sensor networking, security issues in CPS.
- 2) Comprehensive and well organized literature review on some interesting topics and papers from ACM CCS conferences or other related conferences.
- 3) Work on some specific challenging research topics and write a paper about your research results. This could be a theoretical

problem which could lead to publication in some research oriented conferences or journals.

The term paper must be formed like a conference paper that summarizes the results from term project, including, technical challenging questions that are successfully addressed, and NEW algorithms or protocols that are presented and implemented, and new experiment results collected from the project.

**Term Project ideas** (you are encouraged to propose your own team projects, and discuss with me the feasibility of your projects.):

- 1) Modeling/Simulation/Verification/Synthesis/Implementation of some network security systems
- 2) Something related to your own research. You implement the protocols you designed and then evaluate the performances of your protocols in real systems or testbeds.
- 3) Real network security systems, such as security protocols for CPS

**Term Project grading:** In particular, the following four aspects of a term project were considered in project grading:

- 1) Project has a clear goal
- 2) Goal has a clear value if achieved
- 3) There are novel ideas involved in achieving the goal
- 4) These ideas and your implementation work

In summary, the project grade is based on answers to these questions: Clear goal? Has value? New ideas? Ideas work?

If you would like to get detailed written feedback on your project report please let me know and I will give you a marked hard copy. If you disagree with my assessment of any of the above regarding your project, please see me. I would be happy to discuss the final project grade with you and fix it if appropriate.

### **How to do a good presentation:**

Wear professional attire; Clear and concise manner of speaking; Professional-looking audio/visual material such as slides; Split the presentation time about evenly among the members of your team and rehearse the hand-off when the presentation is done by a team. Rehearse your presentation and demo, and time the duration of each part.

One or more group members may deliver the presentation, but all group members are expected to be present and available to answer questions about the project. During the presentation all group members should join together

with the presenter at the front of the room. Please put any electronic materials on a memory stick or post to the web in a readily available location.

## **Tentative Course Topics to be covered**

This course provides an introduction to the theory and the practice of cryptography and network security. Particular topics to be covered include:

### Introduction

Basic concepts, number theory

### I. CONVENTIONAL ENCRYPTION.

Conventional Encryption: Classical Techniques.

Conventional Encryption: Modern Techniques.

Conventional Encryption: Algorithms.

Confidentiality Using Conventional Encryption.

### II. PUBLIC-KEY ENCRYPTION AND HASH FUNCTIONS.

Public key crypto-systems

Message Authentication and Hash Functions.

Hash and MAC Algorithms.

Digital Signatures and Authentication Protocols.

Key Management

Secret Sharing

Interactive proof

### III. NETWORK and SYSTEM SECURITY PRACTICE.

Electronic Mail Security.

IP Security, and/or Web Security.

Intruders, Viruses, Worms, and Firewalls.

## **Other Course Policies**

I expect students to arrive on-time for the class. Classroom participation **constitutes 5%** of the grade in this class. You will be expected to have previously read the reading assignment before the class, and to be able to participate in classroom discussions.

The students are also required to abide the University's Honor Code. Basically, do not represent other persons' work as your own, properly cite sources, and do not intentionally seek to undermine the efforts of your classmates.

Requests for extensions and for making up exams required a documented reason. An example of adequate documentation of a medical reason for missing an exam is a discharge notice from the Student Health Center.

All students registered in this course (and all courses throughout the University) are bound by the Academic Honor Code. Plagiarism (use of somebody else's work without proper acknowledgment) will not be tolerated.

A copy of the full University Academic Honor Code (code of academic honesty) can be found in the current Student Handbook.

Code of Academic Honesty: [academichonesty@iit.edu](mailto:academichonesty@iit.edu), page 243 of UG Bulletin  
[http://retention.iit.edu/resources/bulletin\\_2008\\_2010.pdf](http://retention.iit.edu/resources/bulletin_2008_2010.pdf)

Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me [the instructor] as soon as possible. The Center for Disability Resources (CDR) is located in Life Sciences Room 218, telephone 312-567-5744 or [disabilities@iit.edu](mailto:disabilities@iit.edu).