

# CS549: Cryptography and Network Security

CS DEPARTMENT, IIT. FALL 2009

## Course Objectives:

We cover in this course principles and practice of cryptography and network security: classical systems, symmetric block ciphers (DES, AES, other contemporary symmetric ciphers), linear and differential cryptanalysis, perfect secrecy, public-key cryptography (RSA, discrete logarithms), algorithms for factoring and discrete logarithms, cryptographic protocols, hash functions, authentication, key management, key exchange, signature schemes, email and web security, viruses, firewalls, digital right management, and other topics.

## General Information:

The class homepage is <http://www.cs.iit.edu/~cs549>. All handouts and important information will be posted there. Please check it regularly for new information.

## Teaching Personnel

	name	office	phone	email	office hour
<b>Instructor</b>	Xiang-Yang Li	SB 237D	567-5207 (O)	xli@cs.iit.edu	Wed. 4:10-6:10 PM
<b>TA</b>	XuFei Mao	SB 019B	567-5869 (O)	xmao3@iit.edu	Tue. 1:00PM-3:00PM

**Time and Location: (Fall Break: Oct 12, 2009; Thanksgiving Break: Nov 25-28, 2009)**

Start Date	End date	Time	ClassRoom	Midterm	Final
Aug-24-09	Dec-07-09	W, 6:25-9:05 PM	SB239	10/14/09, 6:25-9:05PM	Take-home

## Textbook:

The official course textbook is **Cryptography and Network Security: Principles and Practice**; Fourth Edition. By William Stallings, Prentice Hall, Hardcover.

One useful book is **Cryptography: Theory and Practice** by Douglas R. Stinson, CRC press, hardcover, Published March, 1995. ISBN 0-8493-8521-0.

Another useful book, **Network Security Essentials: Applications and Standards** by William Stallings. Prentice Hall, Hardcover, Published November 1999, 366 pages, ISBN 0130160938.

You will also find another book useful later in the course: **Secrets and Lies: Digital Security in a Networked World** by Bruce Schneier John Wiley, Published August 2000, 412 pages, ISBN 0471253111.

There are also some good links from <http://www.cs.iit.edu/~xli/confref.html> and the class webpage.

## Course Theme:

This course provides an introduction to the theory and the practice of cryptography and network security. Particular topics to be covered include (but not limited to):

1. Introduction.
- I. CONVENTIONAL ENCRYPTION.
  2. Conventional Encryption: Classical Techniques.
  3. Conventional Encryption: Modern Techniques.
  4. Conventional Encryption: Algorithms.
  5. Confidentiality Using Conventional Encryption.
- II. PUBLIC-KEY ENCRYPTION AND HASH FUNCTIONS.
  6. Public-Key Cryptography.
  7. Introduction to Number Theory.
  8. Message Authentication and Hash Functions.
  9. Hash and Mac Algorithms.
  10. Digital Signatures and Authentication Protocols.
- III. NETWORK SECURITY PRACTICE and SYSTEM SECURITY (by presentations)
  11. Authentication Applications.
  12. Electronic Mail Security.
  13. IP Security.
  14. Web Security.
  15. Intruders, Viruses, and Worms.
  16. Firewalls.

We will mainly cover the topics listed above, but we can not guarantee that all topics will be fully covered because of the time limit. And we will try to cover some other topics if the time is permitted and there are enough students who are interested in those.

## Grading:

There will be **three** homework, a presentation assignment, a programming assignment, an **on-class** midterm, and a **take-home** final exam most likely. They will count toward the grade as follows:

Homework	30%	MidTerm	25%	Programming	10%	Presentation & Report	10%	Final	25%
----------	-----	---------	-----	-------------	-----	-----------------------	-----	-------	-----

However, the instructor reserves the right to make adjustments to these weights based on his a posteriori evaluation of the relative difficulty of the exams and homework.

Each problem will be graded 80% for correctness and 20% for style and clarity. Good style means giving a sound logical argument and a clear presentation, sufficient to convince someone who knows the material, but not the answer, that your answer is correct. Consider your audience to be a skeptical classmate. Good style also implies that an answer should be reasonably thorough, as well as reasonably concise.

<b>Final Grade:</b>	A:	$85 \leq W$	B:	$70 \leq W < 85$
	C:	$60 \leq W < 70$	D:	$50 \leq W < 60$
	F:	$0 \leq W < 50$		

Here  $W = \frac{W_1 + W_2}{2}$ ,  $W_1$  is the final weighted score and  $W_2 = 100 \times \frac{W_1}{AverageTopFive}$ . Here *AverageTopFive* is the average of  $W_1$  of the best five students in the class. For example, if your  $W_1 = 70$ , and *AverageTopFive* = 90, then your  $W = \frac{70 + 70 \times 100 / 90}{2} \simeq 73.89$ . Then you will get *B* for this course. Notice, undergraduate will get *F* if  $W < 60$ . You have to do well enough in each category: homework, presentation, programming, midterm and final exam to get a good grade. In particular, grade will be reduced by one level for those who skip much homework and classes and rely on stellar exam scores. For example, if you did not submit one homework and you have  $W = 80$ , you will have grade *C* instead of grade *B*. The instructor reserves the right for some small changes of grading.

Regrades: If you feel that a problem was graded incorrectly, please contact the TA first. Contact the instructor if there is still a disagreement. For best results, please attach a short note stating what you want regraded and why.  
**Homework:**

You may take an automatic extension by submitting the solution of an assignment on the specified extended due date and time, but with 10% deduction on this homework's grade.

No late assignments handed in after the extended deadline will be accepted. We will not accept any petition for submitting the solution of the homework and any projects later than the required (or extended) deadlines. Requests for an additional extension will almost always be denied.

In this course you are **NOT** allowed to discuss the problems with your classmates, not to say work together. If you discuss the problems with others, it will be treated as cheating! Keep in mind that you could **NOT** discuss general proof strategies, or general algorithms with other students in the course. You could **NOT** collaborate in the detail development or actual writing of problem sets. Consulting with students outside of the course, or using past notes or solutions, etc., is expressly forbidden. Refer to the Campus Code regarding academic integrity.

You get zero on the cheated assignment if you are caught once in any form of the cheating. You **fail** the course automatically if you are caught in cheating (in total) **TWICE** or more in homeworks and programming, or once during the exams (midterm or final). In addition, the violation and the sanction may be reported to the associate dean of either undergraduate or graduate college, as appropriate.

Please help us by stapling all written pages, labelling them with your name, and clearly labelling each problem. You don't want us to lose part of your assignment or not see your answers, do you?

In addition to the writing homework, you have to do a presentation and/or programming project (depending on whether you are remote-site student). It will be great if the student can come out with his/her own new protocols and then implement it. I hope that some of the students can come out with something that is publishable in a conference after the class.

**Presentation project:** In this project, a group of 2-3 students is required to read some new materials that are not covered in the class, and then present it in the class— each presentation lasts 25 minutes, including questions. You also have to write a formal report (about 15 pages) of your presentation material.

The total number of presentation projects allowed in this course is 9— the topics will be given by instructor, and students choose topics based on First Coming First Service (FCFS).

**Programming project:** In this project, each student is required to program some existing protocols. Your program has to run correctly to be graded. You have to hand in the documentation of your programming in addition to the code itself.

Session 001, 002, 003 students have to do presentation and programming as groups. Students from session 004 has to do programming project individually (no presentation project required).

**Important Notes:** 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 Aggie Niemiec (email [aniemiec@iit.edu](mailto:aniemiec@iit.edu)) as soon as possible. The Center for Disability Resources is located in the Life Sciences Building, room 218, 312-567-5744 or [disabilities@iit.edu](mailto:disabilities@iit.edu).