Cryptography and Network Security
CS 685

Instructor: Feng Zhu
Office: Technology Hall N346
Email: fzhu@cs.uah.edu
Phone: 824-6255
Class: Technology Hall N324 Monday & Wednesday 5:30-6:50PM
Office Hour: Technology Hall N346 Mon and Tue 4:30-5:30P (or by appointment)

Course Goals

After completing the course, you will be familiar with: (1) the foundation in cryptography and network security; (2) symmetric ciphers, public-key encryption, hash functions, digital signatures and related mathematical theories; (3) network security protocols, applications, and systems; and (4) advanced network security topics including security in wireless networks. You will have a strong enough background to be able to understand and enjoy articles in the computer networks area.

Prerequisites

CS585.

Text Book

Required text book, "Cryptography and Network Security", (4th or 5th edition), by William Stallings.

Other references, optional, “Handbook of Applied Cryptography” by A. Menezes, P. van Oorschot, and S. Vanstone

Tentative Course Outline

Introduction
Symmetric ciphers
Public-key encryption
Hush functions and Digital Signatures
Network security applications
Security in wireless sensor networks

Midterm Exam 1 Sept. 16
Midterm Exam 2 Oct. 21
Final Exam Nov 30, 6:30 – 9:00PM

Grading

A 90-100
B 80-89
C 70-79
D 60-69
F <60

Midterm Exam 1.....20%
Midterm Exam 2.....20%
Final Exam 30%

Quiz.....5%
Presentation…….....10%
Homework & project……15%

Late Policy

Unexcused late work will be accepted with a late penalty of 50%. The students have one week for raising questions on grading after the return of a graded assignment.

UAH COMPUTER SCIENCE DEPARTMENT POLICIES AND PROCEDURES

1. Responsibilities of the teacher

• Provide a detailed syllabus. This syllabus should list office hours, course objectives, textbooks, references, prerequisites, and grading policy/method of assessment.
• Come to class well prepared, on time, and make full use of the class time.
• Provide timely and adequate feedback on grades. Return graded material promptly.
• Conduct final exam at the time designated in the class schedule. Never post grades.
• Not assign **new** work (i.e. not listed on syllabus) that is due in last two weeks of classes.
• Avoid leaving the examination room without a proctor. Provide paper for exams.
• Make reasonable use of the assigned textbook.
• Check students have proper prerequisites. Instructor does not waive assigned prerequisites.
• **Report all incidences of academic misconduct to the Department and VP for Student Affairs**

2. Responsibilities of the student (see also, Student Handbook Article II)

1) Come to class with the proper prerequisites, well prepared, on time, and make full use of the class time.
2) Provide adequate notice of anticipated absences and take full responsibility for finding out about missed work, announcements, and assignments.
3) Submit assessment material on time and submit **only your own work**. (see integrity)
4) Do not allow other students to copy your work.
5) Read and understand the syllabus and follow announced policies.

3. Integrity

We expect CS instructors and students to conduct themselves in a professional manner. Students are subject to all
the provisions in the UAH Code of Student Conduct, which is available free from the Office of Admissions and
Records. Information on plagiarism and other forms of misconduct is presented in the **Student Handbook Article
III**. *Departments are obliged to report all student misconduct to the Office of Student Affairs.*

4. Complaint Procedure

If you have difficulties or complaints related to this course, your first action should be to discuss them with your instructor. If such a discussion would be uncomfortable for you or fails to resolve your difficulties, you should ask for a meeting with the Chair of the Computer Science Department in Technology Hall N-300, info@cs.uah.edu, telephone 824-6088. If you are still unsatisfied, you should discuss the matter with Daniel Rochowiak, Associate Dean of the College of Science. The Associate Dean's office and telephone number are MSB C206 and 824-6605.

5. Students with disabilities

Your instructor would like to hear from anyone who has a disability that may require a modification of seating, testing, or other class procedures. Please see instructor after class or during office hours to discuss appropriate modifications. You should also contact Student Development Services in UC 113 (Ph. 824 6203) for further assistance.

6. Student computer account

Students enrolled in any CS course are entitled to an account on the departmental computer network. Use of such an account is subject to departmental and university policies. To apply for an account, and see the current policies, go to the departmental web site at *http://www.cs.uah.edu/account/*

7. Examination policy
In response to past student complaints about problems during examinations, the Computer Science Department has developed the following guidelines for in-class examinations in all courses.

1. Come to the exam prepared to complete it without a break. If you think you will need a break, please inform the proctor before the exam if possible.
2. Do not communicate with other students. Talk only to the instructor.
3. Whenever you leave the exam room, turn in your exam.
4. Use only the paper provided by the instructor for all writing.
5. If assigned a specific seat, remain in that seat.
6. Unless specifically permitted by the instructor, use no books or other reference materials. Do not bring calculators, computers, pocket-organizers, cell phones, pagers, or other electronic devices to the exam.

UAlert Emergency Notification System:

UAHuntsville has implemented the UAlert emergency notification system. UAlert allows you to receive time-sensitive emergency messages in the form of e-mail, voice mail, and text messages.

Everyone who has a UAHuntsville e-mail address will receive emergency alerts to their campus e-mail address. In order to also receive text and voice message alerts, you are asked to provide up-to-date phone contact information. Participation in UAlert text and voice messaging is optional, but enrollment is strongly encouraged. You can't be reached through UAlert unless you participate. The information you supply is considered confidential and will not be shared or used for purposes other than emergency notification.

To review your UAlert account, add or update phone and alternate e-mail addresses, and set the priority for your contact methods, please visit the UAlert web site: http://ualert.uah.edu.

Official UAH Statement on Plagiarism

"UAH is committed to the fundamental values of preserving academic honesty as defined in the Student Handbook (7.III.A). The instructor reserves the right to utilize electronic means to help prevent plagiarism. Students agree that by taking this course all assignments are subject to submission for textual similarity review to Turnitin.com. Assignments submitted to Turnitin.com will be included as source documents in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. The terms that apply to the University's use of the Turnitin.com service, as well as additional information about the company, are described at www.uah.edu/library/turnitin."

The following information is from http://www.uah.edu/library/turnitin/about.htm: "*Turnitin.com allows the student or educator to upload a paper into the Turnitin.com database, where software will then use algorithms to create "digital fingerprints" that can identify similar patterns in text ("About Turnitin.com"). Then the paper is matched to billions of web pages, paper mill essays, and student papers submitted online. In an hour or less, Turnitin.com creates an "originality report" that highlights any passages from the paper that might not be authentic, and lists web sites and other resources with content that matches that in the paper ("About Turnitin.com").*

Students can use Turnitin.com to:

- *Quickly track down sources used in their essays, minimizing the chance that they will forget to cite sources.*
- *Learn about the concept of plagiarism and its consequences for the student, course, and the academic community as a whole.*
- *Acquire tips on how to avoid both Internet and conventional plagiarism.*
- *Learn guidelines for proper citation.*

• Gain strong research and writing skills.
• Clarify misunderstood concepts like fair use, public domain, and copyright laws."

For more information please visit http://www.uah.edu/library/turnitin/.

The students are urged to use turnitin.com before the submission of their papers. The instructor will use turnitin.com in the evaluation of the papers.