CSE 4392/5381: Information Security 2
Spring 2015

Details

Instructor:	Matthew Wright	GTA:	Mohsen Imani
email:	mwright@cse.uta.edu	email:	imani.moh@gmail.com
Office:	ERB 528	Office location:	ERB 406
Phone:	(817) 272-0906	Office phone:	(817)-272-3399
Office hours:	M/W 1:00-2:00 PM	Office hours:	Tu/Th 5:00-6:00
Faculty Profile:	https://www.uta.edu/profiles/matthew-wright		

Section Information: CSE 4392, Section 1 and CSE 5381, Section 1
Meeting Times: Tu/Th 3:30 to 4:50 PM Location: WH 308
(*Please check Piazza and Web site for up to date information)*
Web Site: http://isec.uta.edu/mwright/infosec2/
Piazza: https://piazza.com/uta/spring2015/cse5381/home

Description of Course Content

This course will provide both theoretical and practical training in securing networks and communications. We will first cover cryptographic tools and their use, including symmetric and public-key algorithms and hash functions. We then examine cryptographic protocols and study several well-known protocols, such as authentication and confidentiality for Web and email, Kerberos, and wireless access point security. Finally, we discuss some advanced topics.

Course Objectives

By the end of the course, students should be able to:

- Demonstrate how to apply cryptographic primitives to attain the desired security properties.
- Explain the purpose of key design elements in cryptographic algorithms and protocols.
- Implement these algorithms and protocols.
- Identify basic security weaknesses in algorithms and protocols.
- Describe a few cool crypto ideas.

Required Textbooks and Other Course Materials:

Singh, Simon. The Code Book.
ISBN-13: 978-0385495323 ISBN-10: 0385495323
Note: Get the e-book. You need this right away!
Stallings, William. Cryptography and Network Security: Principles and Practices (6th edition).
ISBN-13: 978-0133354690 ISBN-10: 0133354690
Older editions are mostly acceptable (esp. 5th), but use them at your own risk.

Descriptions of major assignments and examinations

- Homework: The written homework assignments are meant to provide exercise with the concepts in the class and are assigned most weeks during the first two-thirds of the class.
- Programming: Implement AES and RSA.
- Independent Project: Work in pairs to explore a security topic that includes an implementation and/or experimentation component, a report, and an in-class presentation.
- Exam 1, in-class, Mon., Feb. 24: Covers Symmetric Ciphers
- Exam 2, in-class, Mon., Apr. 14: Comprehensive; focus on Public Key Cryptography, Protocol Design

Grading: Course grades will be based on the following:

Exams (2)	40%
Homework (10)	30%
Programming Assignments (2)	15%
Independent Project	15%

Grades for Exams will be curved by the instructor and scaled to a standard A = 90-100, B = 80-89, C = 70-79 scale. For example, if the instructor sets the A/B line at 85, then a student who scores 85 will get a scaled score of 90. All other graded elements will not be curved and graded directly on the standard scale. Final grades will simply be the weighted average of the scores, based on the percentages shown above. Small amounts of extra credit may be available, but only on a class-wide basis (no individual requests will be granted). No grade bumps will be offered; 89.99 is a B in this class.

Other Requirements: Pre-requisites for this course: Discrete Structures (including basic number theory) and 5380 or permission of instructor.

Make-ups: Make-ups for graded activities may be arranged if your absence is caused by illness or personal emergency. A written explanation (including supporting documentation) must be submitted to your instructor; if the explanation is acceptable, an alternative to the graded activity will be arranged. *Make-up arrangements must be arranged prior to the scheduled due date.*

Attendance: At The University of Texas at Arlington, taking attendance is not required. Rather, each faculty member is free to develop his or her own methods of evaluating students' academic performance, which includes establishing course-specific policies on attendance. As the instructor of this section, I do not check nor grade attendance. Please note, however, that I will not simply be lecturing to a passive audience. In every class period, you will learn by actively participating in the process of solving problems and working in small groups. Missing class, therefore, means missing out on learning opportunities that cannot be gained from the textbook.

Late Assignments: Homework and programming assignments will be accepted two days (48 hours) after they are due, with a penalty of 10% of the maximum points (e.g. 10 out of 100 points will be deducted).

Schedule (Subject to Change):

Week	Class Dates	Topic	Assignments	Due Dates
1.	Jan. 20/22	Class Intro + Historical Ciphers	HW 1	Jan. 27
2.	Jan. 27/29	Cryptanalysis + Modern Ciphers	HW 2, PR 1	Feb. 3, Feb. 26
3.	Feb. 3/5	AES	HW 3	Feb. 10
4.	Feb. 10/12	Modes + RC4/CRNGs	HW 4	Feb. 17
5.	Feb. 17/19	Hashes	HW 5	Feb. 24
6.	Feb. 24/26	Review + Number Theory 1	Project Idea	Mar. 19
7.	Mar. 3/5	*EXAM 1* + Number Theory 2	HW 6, PR 2	Mar. 17, Apr. 9
8.	Mar. 10/12	**SPRING BREAK**		
9.	Mar. 17/19	RSA	HW 7	Mar. 24
10.	Mar. 24/26	D-H + ECC	HW 8	Mar. 31
11.	Mar. 31/Apr. 2	Protocol Basics + Kerberos	HW 9	Apr. 7
12.	Apr. 7/9	SSL/Email + Wireless	HW 10	Apr. 14
13.	Apr. 14/16	Review + Anonymity		
14.	Apr. 21/23	*EXAM 2* + Zero Knowledge	Project	May 11
15.	Apr. 28/30	Rainbow Tables + Bitcoin		
16.	May 5/7	*Project Presentations*		
17.	May 12	**NO FINAL**		

Note: The instructor reserves the right to adjust this schedule in any way that serves the educational needs of the students enrolled in this course.

Drop Policy: Students may drop or swap (adding and dropping a class concurrently) classes through self-service in MyMav from the beginning of the registration period through the late registration period. After the late registration period, students must see their academic advisor to drop a class or withdraw. Undeclared students must see an advisor in the University Advising Center. Drops can continue through a point two-thirds of the way through the term or session. It is the student's responsibility to officially withdraw if they do not plan to attend after registering. **Students will not be automatically dropped for non-attendance**. Repayment of certain types of financial aid administered through the University may be required as the result of dropping classes or withdrawing. For more information, contact the Office of Financial Aid and Scholarships (http://wweb.uta.edu/aao/fao/).

Americans with Disabilities Act: The University of Texas at Arlington is on record as being committed to both the spirit and letter of all federal equal opportunity legislation, including the *Americans with Disabilities Act (ADA)*. All instructors at UT Arlington are required by law to provide "reasonable accommodations" to students with disabilities, so as not to discriminate on the basis of that disability. Any student requiring an accommodation for this course must provide the instructor with official documentation in the form of a letter certified by the staff in the Office for Students with Disabilities, University Hall 102. Only those students who have officially documented a need for an accommodation will have their request honored. Information regarding diagnostic criteria and policies for obtaining disability-based academic accommodations can be found at www.uta.edu/disability or by calling the Office for Students with Disabilities at (817) 272-3364.

Title IX: The University of Texas at Arlington is committed to upholding U.S. Federal Law "Title IX" such that no member of the UT Arlington community shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity. For more information, visit www.uta.edu/titleIX.

Academic Integrity: Students enrolled all UT Arlington courses are expected to adhere to the UT Arlington Honor Code:

> *I pledge, on my honor, to uphold UT Arlington's tradition of academic integrity, a tradition that values hard work and honest effort in the pursuit of academic excellence.*
>
> *I promise that I will submit only work that I personally create or contribute to group collaborations, and I will appropriately reference any work from other sources. I will follow the highest standards of integrity and uphold the spirit of the Honor Code.*

UT Arlington faculty members may employ the Honor Code as they see fit in their courses, including (but not limited to) having students acknowledge the honor code as part of an examination or requiring students to incorporate the honor code into any work submitted. Per UT System *Regents' Rule* 50101, §2.2, suspected violations of university's standards for academic integrity (including the Honor Code) will be referred to the Office of Student Conduct. Violators will be disciplined in accordance with University policy, which may result in the student's suspension or expulsion from the University.

Electronic Communication: UT Arlington has adopted MavMail as its official means to communicate with students about important deadlines and events, as well as to transact university-related business regarding financial aid, tuition, grades, graduation, etc. All students are assigned a MavMail account and are responsible for checking the inbox regularly. There is no additional charge to students for using this account, which remains active even after graduation. Information about activating and using MavMail is available at http://www.uta.edu/oit/cs/email/mavmail.php.

We will use Piazza for all course communications, including links to readings, assignments, course news, etc. All students are responsible for checking the server regularly for news and assignments. Your MavMail accounts will be set as the default email for interacting with Piazza.

Students will be given accounts for the ASCENT security-teaching lab. All students are expected to be responsible users of the computer systems used for this course. In particular, students are expected to abide by the code of ethics associated with this course.

Student Feedback Survey: At the end of each term, students enrolled in classes categorized as "lecture," "seminar," or "laboratory" shall be directed to complete an online Student Feedback Survey (SFS). Instructions on how to access the SFS for this course will be sent directly to each student through MavMail approximately 10 days before the end of the term. Each student's feedback enters the SFS database anonymously and is aggregated with that of other students enrolled in the course. UT Arlington's effort to solicit, gather, tabulate, and publish student feedback is required by state law; students are strongly urged to participate. For more information, visit http://www.uta.edu/sfs.

Final Review Week: A period of five class days prior to the first day of final examinations in the long sessions shall be designated as Final Review Week. The purpose of this week is to allow students sufficient time to prepare for final examinations. During this week, there shall be no scheduled activities such as required field trips or performances; and no instructor shall assign any themes, research problems or exercises of similar scope that have a completion date during or following this week *unless specified in the class syllabus*. During Final Review Week, an instructor shall not give any examinations constituting 10% or more of the final grade, except makeup tests and laboratory examinations. In addition, no instructor shall give any portion of the final examination during Final Review Week. During this week, classes are held as scheduled. In addition, instructors are not required to limit content to topics that have been previously covered; they may introduce new concepts as appropriate.

Student Support Services: UT Arlington provides a variety of resources and programs designed to help students develop academic skills, deal with personal situations, and better understand concepts and information related to their courses. Resources include tutoring, major-based learning centers, developmental education, advising and mentoring, personal counseling, and federally funded programs. For individualized referrals, students may visit the reception desk at University College (Ransom Hall), call the Maverick Resource Hotline at 817-272-6107, send a message to resources@uta.edu, or view the information at www.uta.edu/resources.

Emergency Exit Procedures: Should we experience an emergency event that requires us to vacate the building, students should exit the room and move toward the nearest exit, which you are required to locate at the end of the first class period. When exiting the building during an emergency, one should never take an elevator but should use the

stairwells. Faculty members and instructional staff will assist students in selecting the safest route for evacuation and will make arrangements to assist individuals with disabilities.

Emergency Phone Numbers: In case of an on-campus emergency, call the UT Arlington Police Department at **817-272-3003** (non-campus phone), **2-3003** (campus phone). You may also dial 911.