COSC 483/583

Applied Cryptography

Tue/Thurs 2:10 - 3:25, Min Kao 405

Instructor: Dr. Max Schuchard

mschucha@utk.edu
Office Location: Min Kao 345
Office Hours: 3:30 - 4:30 Tue and Thurs

This syllabus is a living document, and subject to change as needed. Any changes made after the first day of class will be announced publicly at the start of the class following the change.

Course Description: This is an introductory cryptography course, with focus on understanding modern cryptographic primitives and how to apply them. These concepts include symmetric ciphers, asymmetric ciphers, secure hash algorithms, public key infrastructure, design of cryptographic protocols, and proofs of security. The course also touches on advanced research topics such as group communication and zero knowledge proofs.

Prerequisite(s): COSC 311, 366, MATH 251.
Credit Hours: 3

Text(s): *Introduction to Modern Cryptography*, 2nd Edition
Author(s): Jonathan Katz and Yehuda Lindell; **ISBN-13:** 9781466570269

Course Objectives:
At the completion of this course, students will be able to:

1. Have an understanding of cryptographic terminology.
2. Have an understanding of basic cryptographic primitives.
3. Apply cryptographic primitives to build complex cryptosystems.
4. Analyze the security properties of cryptosystems.

Grade Distribution:

Exercises (6 in total)	30% (5% per)
Coding Assignments (3 in total)	35% (10%, 10%, 15%)
Quizes (Computed ignoring your worst 25% of quizes.)	10%
Midterm Exam	10%
Final Exam	15%

Letter Grade Distribution:
These are *ceilings* of the grade cut offs.

>= 93.00	A
90.00 - 92.99	A-
87.00 - 89.99	B+
83.00 - 86.99	B
80.00 - 82.99	B-
77.00 - 79.99	C+
73.00 - 76.99	C
70.00 - 72.99	C-
<= 69.99	F

Course Policies:

- **Exams**
  - **Exams** are open book, open notes, and closed devices.
  - **Quizes** are closed everything.
  - **No makeup exams or quizes will be given.**
- **Assignments**
  - Students are allowed to work on exercises in groups of up to TWO students and programming assignments in groups of up to THREE. Only one submission must be handed in for a group. Please ensure that all student's names are on the work, even if done individually.
  - Exercises are expected to be turn in in print at the start of class the day they are due.
  - Programming assignments are turned in via `git` at 23:59:59 the night they are due.
  - No late assignments will be accepted under any circumstances.
  - A wealth of solutions to programming problems can be found on the Internet. While I do not mind you referencing these solutions as examples, it is **not acceptable for you to copy code from the Internet and pass it off as yours**. The first time you are caught doing this you will receive a zero on that assignment, if it happens again you will receive an F in the class. If the copied code is from prior years of the class I will pursue disciplinary action via the university immediately.
- **Attendance and Absences**
  Attendance is encouraged, but you are an adult, and allowed to make decisions about how you spend your time. That being said, no matter what, students are responsible for all missed work, regardless of the reason for absence. It is also the absentee's responsibility to get all missing notes or materials.

Academic Honesty Policy Summary:

Introduction

Academic integrity is defined as not cheating and not plagiarizing; honesty and trust among students and between students and faculty are essential for a strong, functioning academic community. Consequently, students are expected to do their own work on all academic assignments, tests, projects and research/term papers. Academic dishonesty, whether cheating, plagiarism or some other form of dishonest conduct related to academic course work will automatically result in failure for the work involved. But academic dishonesty could also result in failure for the course and, in extremis, suspension from the University.

Here are the common ways to violate the academic integrity code:

Cheating - Intentionally using or attempting to use unauthorized materials, information, or study aids in any academic exercise. The term academic exercise includes all forms of work submitted for credit.

Fabrication - Intentional and unauthorized falsification or invention of any information or citation in an academic exercise.

Facilitating Academic Dishonesty - Intentionally or knowingly helping or attempting to help another to violate a provision of the institutional code of academic integrity.

Plagiarism - The deliberate adoption or reproduction of ideas or words or statements of another person as one's own without acknowledgment. You commit plagiarism whenever you use a source in any way without indicating that you have used it.

Cheating In cases of cheating, the instructor will impose a minimum sanction of failure of work involved. The instructor will inform the student and the program director in writing of:

- The nature of the offense
- The penalty imposed within the course
- The recommendation of the instructor as to whether further disciplinary action by the director is warranted

When academic dishonesty occurs, the following procedures will be followed. The instructor will impose a minimum sanction of failure for the work involved. The instructor will notify the student and the appropriate academic dean/director in writing of the nature of the offense and that the minimum sanction has been imposed. The instructor may recommend to the dean that further penalties should be imposed. If further penalties are imposed, the dean/director will notify the student immediately and the student will have five working days to respond to the intention to impose additional penalties. The student has the right to respond to the charge of academic dishonesty and may request in writing that the dean review the charge of academic dishonesty as fully as possible. If the dean/director determines that no further sanctions will be applied, the instructor's sanction will stand.

Disability Resources:

I want to ensure that the classroom environment is conducive to your learning and ask that you discuss with me any concerns that are interfering with your learning as they arise. Classroom accommodations will be provided for students with documented disabilities. Students must contact the Office of Disability Services about accommodations for this course as early in the semester as possible. Appointments can be made by calling 865-974-6087, or email ods@utk.edu. Further information is available at: http://ods.utk.edu/.

Week	Content
Aug 22	• Introduction, Security Concepts
Aug 27, 29	• Historical Ciphers and One Time Pads
Sep 3, 5	• Proving Security and Block Ciphers
Sep 10, 12	• Non-Determinism and Modes
Sep 17, 19	• Symmetric Key Integrity
Sep 24, 26	• Authenticated Encryption • NO CLASS Sept 26
Oct 1, 3	• Cryptographically Secure Hashing
Oct 8, 10	• Number Theory • MIDTERM Oct 8
Oct 15, 17	• Number Theory • NO CLASS Oct 17 (Fall Break)
Oct 22, 24	• RSA • NO CLASS Oct 24 (Engineering Day)
Oct 29, 31	• Diffie Hellman Based Systems
Nov 5, 7	• Digital Signatures and Certificates
Nov 12, 14	• Cryptographic Protocols and TLS
Nov 19, 21	• WPA, IPSec, and Other Protocols
Nov 26, 28	• Group Communication • NO CLASS Nov 28 (Thanksgiving)
Dec 3	• Zero Knowledge Proofs
Dec 12	• Final Exam: 2:45 - 4:45