CSE 4392 Applied Cryptography
Fall 2024

Instructor: Trevor Bakker, CISSP, CISSP-ISSAP, CEH

Email Address: trevor.bakker@uta.edu

Faculty Profile: https://mentis.uta.edu/explore/profile/trevor-bakker

Office Location: ERB 321

Office Hours: Friday 8:00AM - 11:00AM

Office Phone: You may also contact the department at 817-272-3785

Section Information: CSE4392 Section 001

Time and Place of Class Meetings:

Textbooks:

The Joy of Cryptography, Mike Rosulek
`https://joyofcryptography.com`

A Graduate Course in Applied Cryptography, Dan Boneh and Victor Shoup
`https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_4.pdf`

Course Modality Description: This course will be taught in-person. For those who can't attend live, the class recordings of the lectures will be posted to Canvas Echo360.

Technology Requirements: You will need an internet connection for _ this course. A course slack channel will be available for questions and discussions but not required.

Description of Course Content: This course provides an introduction to modern cryptography. Topics include symmetric cryptography, public-key cryptography, digital signatures, key agreement, post-quantum cryptographic algorithms, and zero-knowledge proofs. We will also cover proper usage of cryptographic primitives. Prerequisite: CSE 2315, CSE 3320

Student Learning Outcomes: Upon completion of this course the student will be able to understand and explain:

1. The mathematical background of cryptography.
2. The concepts used in early substitution and translation ciphers.
3. The differences between and implications of random and pseudo-random numbers
4. Block ciphers and some classic block-cipher constructions (DES, 3DES and AES).
5. Stream ciphers such as RC4, ChaCha, and Salsa20
6. Message allocation such as MAC, HMAC, GCM
7. Public-key cryptography including RSA functions and the other based on the Diffie-Hellman protocol.
8. Elliptic curve cryptography such as ECDH, ECDSA and ECMQV
9. Post-quantum cryptography including Kyber and Dillithium.

Upon completion of this course the student will also be able to:

10. Demonstrate the ability to analyze a complex privacy / security problem and design and implement a strong cryptographic solution using symmetric key and public key encryption

Descriptions of major assignments: There will be 6 written assignments over the course of the semester consisting of problems that delve deeper into the material

than the practice problems. Assignments will include reasoning using formal security models, simulating or programming various algorithms, selecting appropriate techniques for providing security in various scenarios, and a significant amount of analysis and writing formal proofs.

There will be two mid-term exams and one final comprehensive exam which will assess students mastery of the learning outcomes 1 through 9 in an exam setting. The final exam date is set by the university and is non-negotiable.

The major programming assignment will assess the master of learning outcome 10.

Honors students completing a contract honors requirement with this class will be provided research papers related to various aspects of cryptography and will select a topic from the research literature, locate appropriate references, and write a thorough research summary and critique.

Important Dates:

Drop Deadline ..... October 25th
Exam 1 ..... Oct. 14th (tentative)
Exam 2 ..... Nov. 11th (tentative)
Final ..... Dec 5th 5:30pm - 8:00pm (fixed)

Grading Policy: Grades are based on the following:

Programming Project	20%
Homework	30%
Exam 1	15%
Exam 2	15%
Final Exam	20%

No make-up exams will be given. If the grade received on your final exam is greater than one of the earlier exams, then I will replace the lowest of the earlier two exam

grades with the grade received on the final exam. In the event of a tie for lowest exam grade among the first two exams, only one will be replaced. The final will only be substituted for an exam grade. A grade of zero due to cheating will not be replaced.

Students are expected to keep track of their performance throughout the semester and seek guidance from available sources (including the instructor) if their performance drops below satisfactory levels; see "Student Support Services," below. I do not negotiate grades or entertain requests for rounding. If you have grade requirements for scholarships or GPA reasons it is your responsibility to track your performance through the semester and pursue any available options such as office hours, email questions and study opportunities. Extra credit work is not provided.

If a student believes an error has been made in the grading of an assignment, the student has **one week** after an assignment is returned to resubmit an assignment for re-grading if they believe there is an error. All requests for re-regrading must be submitted in writing. In case of re-grading, the instructor reserves the right to re-grade the whole assignment or exam which may result in a lower grade. Requests of re-grading the final exam must be done within **one day** of receipt of that grade. Regrading will be conducted on an as-time-available basis and may be prioritized behind other grading activity. All regrading will be complete before the final exam. Final letter grades are based on the standard ranges of:

A	90...100%
B	80...89%
C	70...79%
D	60...69%
F	0...59%

Late Submission Policy: All assignments are due at 5:30 PM on the date specified in the assignment. Submissions later than 5:30 PM will be considered late and get 0 credit. The submission time will be the time shown on the UTA Canvas submission

system.

Exceptions will only be made for documented emergencies, in strict adherence to UTA policy. Computer/network crashes or account problems such as forgotten passwords are not an acceptable excuse for late submissions. To avoid problems with crashes and last-minute problems, students are encouraged to use a personal SCM such as git, subversion, github and submit early and often. You can always revise your submission until the deadline.

Expectations for Out-of-Class Study: Beyond the time required to attend each class meeting, students enrolled in this course should expect to spend at least an additional 10 hours per week of their own time in course-related activities, including reading required materials, completing assignments, preparing for exams, etc.

Attendance Policy: 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 student's academic performance, which includes establishing course-specific policies on attendance. As the instructor of this section, I do not require attendance. However, while UT Arlington does not require instructors to take attendance in their courses, the U.S. Department of Education requires that the University have a mechanism in place to mark when Federal Student Aid recipients begin attendance in a course. UT Arlington instructors will report when students begin attendance in a course as part of the final grading process. Specifically, when assigning a student a grade of F, faculty report the last date a student attended their class based on evidence such as a test, participation in a class project or presentation, or an engagement online via Canvas. This date is reported to the Department of Education for federal financial aid recipients. I do strongly encourage you to attend all classes.

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/).

Disability Accommodations: UT 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), The Americans with Disabilities Amendments Act (ADAAA), and Section 504 of the Rehabilitation Act. 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 disability. Students are responsible for providing the instructor with official notification in the form of **a letter certified** by the Office for Students with Disabilities (OSD). Students experiencing a range of conditions (Physical, Learning, Chronic Health, Mental Health, and Sensory) that may cause diminished academic performance or other barriers to learning may seek services and/or accommodations by contacting:

The Office for Students with Disabilities, (OSD) www.uta.edu/disability or calling 817-272-3364.

Information regarding diagnostic criteria and policies for obtaining disability-based academic accommodations can be found at www.uta.edu/disability.

Counseling and Psychological Services, (CAPS) www.uta.edu/caps/ or calling 817-272-3671 is also available to all students to help increase their understanding of personal issues, address mental and behavioral health problems and make positive changes in their lives.

Non-Discrimination Policy:*The University of Texas at Arlington does not discriminate on the basis of race, color, national origin, religion, age, gender, sexual orientation, disabilities, genetic information, and/or veteran status in its educational programs or activities it operates. For more information, visit uta.edu/eos.*

Title IX:The University of Texas at Arlington (University) is committed to maintaining a learning and working environment that is free from discrimination based on sex in accordance with Title IX of the Higher Education Amendments of 1972 (Title IX), which prohibits discrimination on the basis of sex in educational programs or activities; Title VII of the Civil Rights Act of 1964 (Title VII), which prohibits sex

discrimination in employment; and the Campus Sexual Violence Elimination Act (SaVE Act). Sexual misconduct is a form of sex discrimination and will not be tolerated. For information regarding Title IX, visit www.uta.edu/titleIX or contact Ms. Michelle Willbanks, Title IX Coordinator at (817) 272-4585 or titleix@uta.edu

Electronic Communication Policy: 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.

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 honet 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. Homework assignments, including programming assignments, unless specified, are not group projects; each student is expected to write his or her own programs individually. Code copied from the internet shall be considered a violation of this policy. All acts of academic dishonesty, including programming assignments, will be reported to the Office of Student Conduct. The first act of academic dishonesty on an assignment will result in a grade of 0 for the assignment. The second act will result in a failing grade for the course. Cheating on an exam will result in failure

of the course.

By enrolling in this course, you understand that the consequences for committing any acts of academic dishonesty will include a failing grade for the assignment, and may include failure in the class as a whole, academic sanction, and/or even dismissal from the university.

Use of GitHub Copilot and ChatGPT or any other LLM AI will result in a 0 on the assignment and a referral to the Office of Student Conduct. It is the responsibility of each student to ensure that all work submitted for this class is their own original work, written and completed without the use of AI or other automated writing tools.

Academic Success Center The Academic Success Center (ASC) includes a variety of resources and services to help you maximize your learning and succeed as a student at the University of Texas at Arlington. ASC services include supplemental instruction, peer-led team learning, tutoring, mentoring and TRIO SSS. Academic Success Center services are provided at no additional cost to UTA students. For additional information visit: https://www.uta.edu/student-success/course-assistance

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 students feedback enters the SFS database anonymously and is aggregated with that of other students enrolled in the course. UT Arlingtons 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.

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 http://www.uta.edu/universitycollege/resources/index.ph

Face Covering Policy Face coverings are not mandatory, all students and instructional staff are welcome to wear face coverings while they are on campus or in the classroom.

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. 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. Non-emergency number 817-272-3381

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.

Course Schedule:

Week 1: Overview of Cryptography Introduction to Cryptography One-time pad and perfect secrecy

Mathematic Review

Week 2: Secret key cryptography

Week 3: Stream ciphers

Week 4: Block Ciphers

Week 5: Chosen Plaintext Attack

Week 6: Message Integrity

Week 7: Authenticad Encryption
Week 8: Public Key Cryptography
Week 9: Digital Signatures
Week 10: Elliptic curve cryptography
Week 11: Post-quantum cryptography

Class Schedule

Date	Topic	Assignment
08/19/2024	Introduction to the Course	-
08/21/2024	Overview of the Semester	Read Chapter 1
08/26/2024	Topic 1	Assignment 1 Due
08/28/2024	Topic 2	-
09/02/2024	Topic 3	Read Chapter 2
09/04/2024	Topic 4	Assignment 2 Due
09/09/2024	Topic 5	-
09/11/2024	Topic 6	Read Chapter 3
09/16/2024	Topic 7	Assignment 3 Due
09/18/2024	Topic 8	-
09/23/2024	Topic 9	Read Chapter 4
09/25/2024	Topic 10	Assignment 4 Due
09/30/2024	Topic 11	-
10/02/2024	Topic 12	Read Chapter 5
10/07/2024	Topic 13	Assignment 5 Due
10/09/2024	Topic 14	-
10/14/2024	Mid-Term Exam	-
10/16/2024	Topic 15	Read Chapter 6
10/21/2024	Topic 16	Assignment 6 Due