The University of Texas at Tyler
Soules College of Business
Computer Science Department

COSC 4367.001 – Cryptography
Fall Term 2023

Course Syllabus

Instructor Contact Information:

Name: Dr. Tim Nix
Office: COB 315.12
E-mail: tnix@uttyler.edu
Office Hours: Send me an email to make an appointment

Lecture Schedule: MonWedFri 10:10AM – 11:05AM COB 211

***Course Description*:** This course provides an overview to cryptography, which includes classical encryption, block ciphers and DES, public key cryptography, hashing, message authentication, key management, digital signatures, user authentication, transport layer security, wireless security, and e-mail security.

Prerequisite: COSC 4325 or COSC 4360.

Required Textbook:

- *Serious Cryptography: A Practical Introduction to Modern Encryption; Author: Jean-Philippe Aumasson; Publisher: No Starch Press; ISBN: 978-1593278267.*

Grading Policy:

Reading Quizzes	25%
Programming Assignments	25%
Midterm Exam	25%
Final Exam	25%
Total:	**100%**

Grading Rubric:

Letter Grade	Assigned Score (s)	Definition
A	$90\ \% \leq s$	Mastery
B	$80\ \% \leq s < 90\ \%$	Good Understanding
C	$70\ \% \leq s < 80\ \%$	Adequate
D	$65\ \% \leq s < 70\ \%$	Probably Failed to Demonstrate
F	$s < 65\ \%$	Definitely Failed to Demonstrate

Academic Dishonesty: Representation of other's work as your own will not be tolerated and this includes AI-generated content. Cheating on examinations, quizzes, and homework and the false representation of work

will be interpreted as academic dishonesty. Academic dishonesty will be subject to disciplinary action as outlined by the UT Tyler Student Guide on Conduct and Discipline.

Evidence of academic dishonesty will result in automatic failure of the course.

Tentative Topic Schedule:

Week	Topic
Aug 21 – Aug 25	Introduction to Encryption
Aug 28 – Sep 01	Randomness in Cryptography
Sep 04 – Sep 08	Cryptographic Security
Sep 11 – Sep 15	Block Ciphers
Sep 18 – Sep 22	Stream Ciphers
Sep 25 – Sep 29	Hash Functions
Oct 02 – Oct 06	Keyed Hashing
Oct 09 – Oct 13	Authenticated Encryption and Midterm Exam
Oct 16 – Oct 20	Hard Computational Problems
Oct 23 – Oct 27	The Rivest-Shamir-Aldleman (RSA) Cryptosystem
Oct 30 – Nov 03	The Diffee-Hellman Protocol
Nov 06 – Nov 10	Elliptic Curve Cryptography (ECC)
Nov 13 – Nov 17	The Transport Layer Security (TLS) Protocol
Nov 20 – Nov 24	Thanksgiving Break
Nov 27 – Dec 01	Quantum and Post-Quantum Cryptography
Dec 04 – Dec 08	Final Exams

Reading Quizzes: For each assigned chapter of the textbook, a corresponding reading quiz will also be assigned. You may take the reading quiz at any time between it becoming available and its due date/time. However, once you begin the reading quiz, you will only have 90 minutes to complete it. There is a reading quiz for each assigned chapter of the textbook, and they constitute 25% of the overall course grade.

Programming Assignments: Programming assignments will focus on practical skills and applications. These assignments will require students to upload the source code containing their solution. There will be 7-10 programming assignments and are worth 25% of the overall course grade.

Exams: There will be one midterm exam during the semester and a final exam. All exams are comprehensive. The midterm exam will be given during the scheduled lecture period and is worth 25% of the final grade. The midterm exam must be taken during the specified time period on the date scheduled. No makeup exams will be given. The final exam will be taken in accordance with the final exam schedule and is worth 25% of the final grade. Check the final exam time. If the final exam time is a problem, you need to drop this course.

Tentative Exam Dates:

Date	Day	Description
10/13/2023	Friday	Midterm Exam
12/06/2023	Wednesday	Final Exam

Late Policies: All homework assignments are due on the date/time specified in the assignment. Assignments will not be accepted after that time. Any assignment submitted late will receive a grade of zero.

Any assignment submitted late will receive a grade of zero.

EXPECTATIONS OF STUDENTS:

- **Be prepared for lectures and take notes.** I expect you to have read the assigned readings. Class time is primarily for extending and applying what you learn from the readings. If you come unprepared, you will get significantly less out of class and quickly fall behind. Be an active note-taker.

- **Attend the lectures and be on time.** There will be times when you will want to skip class. Make your education a priority. During the lectures, I will reinforce material from the textbook and cover things that are not in the textbook. You will still be responsible for this material. Missing a lecture should be a rare occurrence. If you do miss the lecture, get the notes from another student. See me during my office hours for clarification of any missed material.

- **Take ownership of your learning.** You are solely responsible for how much you get out of this course. It is not my responsibility to spoon-feed you knowledge, but rather to guide you along your developmental path. I hope that this course will challenge you. Deep learning happens when you struggle and succeed. During lectures, your participation and undivided attention are critical. On the assignments, leaning too much on looking at someone else's code robs you of learning and tricks you into thinking you understand more that you do.

- **Seek my help early if you feel lost.** If you are doing the readings, attending the lectures and taking copious notes, and yet you still feel lost, do not convince yourself that things will get better on their own or that you will catch up this weekend. This course, like most others, builds on itself throughout the semester. Come see me before the feelings of confusion compound.

UNIVERSITY POLICIES

UT Tyler Honor Code – Every member of the UT Tyler community joins together to embrace: Honor and integrity that will not allow me to lie, cheat, or steal, nor to accept the actions of those who do.

Student Standards of Academic Conduct – Disciplinary proceedings may be initiated against any student who engages in scholastic dishonesty, including, but not limited to, cheating, plagiarism, collusion, the submission for credit of any work or materials that are attributable in whole or in part to another person, taking an examination for another person, any act designed to give unfair advantage to a student or the attempt to commit such acts.

"Cheating" includes, but is not limited to:

- copying from another student's test paper or homework assignment;
- using, during a test, materials not authorized by the person giving the test;
- failure to comply with instructions given by the person administering the test;
- possession during a test of materials which are not authorized by the person giving the test, such as class notes or specifically designed "crib notes". The presence of textbooks constitutes a violation if they have been specifically prohibited by the person administering the test;
- using, buying, stealing, transporting, or soliciting in whole or part the contents of an unadministered test, test key, homework solution, or computer program;
- collaborating with or seeking aid from another student during a test or other assignment without authority;
- discussing the contents of an examination with another student who will take the examination;

- divulging the contents of an examination, for the purpose of preserving questions for use by another, when the instructors has designated that the examination is not to be removed from the examination room or not to be returned or to be kept by the student;
- substituting for another person, or permitting another person to substitute for oneself to take a course, a test, or any course-related assignment;
- paying or offering money or other valuable thing to, or coercing another person to obtain an unadministered test, test key, homework solution, or computer program or information about an unadministered test, test key, home solution or computer program;
- falsifying any academic work offered for credit;
- taking, keeping, misplacing, or damaging the property of The University of Texas at Tyler, or of another person, if the student knows or reasonably should know that an unfair academic advantage would be gained by such conduct; and
- misrepresenting facts, including providing false grades or resumes, for the purpose of obtaining an academic or financial benefit or injuring another student academically or financially.
- use of any AI-generated content.

Unless otherwise specified, all work submitted for a grade must be completed by yourself. You are not to submit another person's work and claim it as your own. Plagiarism and/or collusion will result in disciplinary actions. To spare yourself accusations of plagiarism:

1. Do not show another student a copy of your work before it has been graded. The penalties for permitting your work to be copied are the same as the penalties for copying someone else's work.
2. Do not leave printouts of your work where other students may pick them up.

Students Rights and Responsibilities – To know and understand the policies that affect your rights and responsibilities as a student at UT Tyler, please follow this link: http://www.uttyler.edu/wellness/rightsresponsibilities.php

Campus Carry – We respect the right and privacy of students 21 and over who are duly licensed to carry concealed weapons in this class. License holders are expected to behave responsibly and keep a handgun secure and concealed. More information is available at http://www.uttyler.edu/about/campus-carry/index.php

UT Tyler a Tobacco-Free University – All forms of tobacco will not be permitted on the UT Tyler main campus, branch campuses, and any property owned by UT Tyler. This applies to all members of the University community, including students, faculty, staff, University affiliates, contractors, and visitors. Forms of tobacco not permitted include cigarettes, cigars, pipes, water pipes (hookah), bidis, kreteks, electronic cigarettes, smokeless tobacco, snuff, chewing tobacco, and all other tobacco products. There are several cessation programs available to students looking to quit smoking, including counseling, quitlines, and group support. For more information on cessation programs please visit www.uttyler.edu/tobacco-free.

Grade Replacement/Forgiveness and Census Date Policies – Students repeating a course for grade forgiveness (grade replacement) must file a Grade Replacement Contract with the Enrollment Services Center (ADM 230) on or before the Census Date of the semester in which the course will be repeated. (For Fall, the Census Date is Sept. 12.) Grade Replacement Contracts are available in the Enrollment Services Center or at http://www.uttyler.edu/registrar. Each semester's Census Date can be found on the Contract itself, on the Academic Calendar, or in the information pamphlets published each semester by the Office of the Registrar. Failure to file a Grade Replacement Contract will result in both the original and repeated grade being used to calculate your overall grade point average. Undergraduates are eligible to exercise grade replacement for only three course repeats during their career at UT Tyler; graduates are eligible for two grade replacements. Full

policy details are printed on each Grade Replacement Contract. The Census Date (Sept. 12th) is the deadline for many forms and enrollment actions of which students need to be aware. These include:

- Submitting Grade Replacement Contracts, Transient Forms, requests to withhold directory information, approvals for taking courses as Audit, Pass/Fail or Credit/No Credit.
- Receiving 100% refunds for partial withdrawals. (There is no refund for these after the Census Date)
- Schedule adjustments (section changes, adding a new class, dropping without a "W" grade)
- Being reinstated or re-enrolled in classes after being dropped for non-payment
- Completing the process for tuition exemptions or waivers through Financial Aid

State-Mandated Course Drop Policy – Texas law prohibits a student who began college for the first time in Fall 2007 or thereafter from dropping more than six courses during their entire undergraduate career. This includes courses dropped at another 2-year or 4-year Texas public college or university. For purposes of this rule, a dropped course is any course that is dropped after the census date (See Academic Calendar for the specific date). Exceptions to the 6-drop rule may be found in the catalog. Petitions for exemptions must be submitted to the Enrollment Services Center and must be accompanied by documentation of the extenuating circumstance. Please contact the Enrollment Services Center if you have any questions.

Student Accessibility and Resources – In accordance with Section 504 of the Rehabilitation Act, Americans with Disabilities Act (ADA) and the ADA Amendments Act (ADAAA) the University offers accommodations to students with learning, physical and/or psychiatric disabilities. If you have a disability, including non-visible disabilities such as chronic diseases, learning disabilities, head injury, PTSD or ADHD, or you have a history of modifications or accommodations in a previous educational environment you are encouraged to contact the Student Accessibility and Resources (SAR) office and schedule an interview with the Accessibility Case Manager/ADA Coordinator, Cynthia Lowery Staples. If you are unsure if the above criteria applies to you, but have questions or concerns please contact the SAR office. For more information or to set up an appointment please visit the SAR office located in the University Center, Room 3150 or call 903.566.7079. You may also send an email to cstaples@uttyler.edu.

Student Absence due to Religious Observance – Students who anticipate being absent from class due to a religious observance are requested to inform the instructor of such absences by the second class meeting of the semester.

Student Absence for University-Sponsored Events and Activities – If you intend to be absent for a university-sponsored event or activity, you (or the event sponsor) must notify the instructor at least two weeks prior to the date of the planned absence. At that time, the instructor will set a date and time when make-up assignments will be completed.

The following pages may be revised without notice. These policies can be found on UT Tyler's website: http://www.uttyler.edu/academicaffairs/files/syllabuspolicy.pdf