**University of Texas at Tyler**
**Soules College of Business**
**Department of Computer Science**
**COSC 4367- COSC 5367 Cryptography**

***Subject to Change***

## Course Information

**COSC 4367- COSC 5367** Summer I 2024
Online Asynchronous Mode (5-week schedule)

## Instructor Contact

Instructor: Sara Memarian Esfahani
Office location: COB 315.16
Zoom Meeting ID: https://uttyler.zoom.us/j/8432799050
Office hours: Mondays and Wednesdays 9:30 to 11:00 on Zoom by appointment
Email: Use the Inbox in Canvas (MUST include COSC 4367 Cryptography in the Subject Line)
Normally, I will reply to an email within 24 to 48 hours.
To ensure a quick response over the weekends, please email me no later than Friday mornings.
Occasionally I will be unable to respond within that time frame but will inform the class in advance.

## Communication Expectations

The most convenient way to communicate with the instructor is through the Inbox in Canvas. Download the mobile app for your convenience.

**Discussion Board Communication**
Please post general course or assignment questions to the General Course Questions & Answers Discussion Topic. Students are encouraged to respond to their fellow classmates' questions. I will read all discussion postings and add comments/suggestions/questions as necessary to keep the discussion on topic. Specific topic instructions on discussions are provided in the forums when needed.

**Canvas Notifications:**
Receive instant notifications about course events, such as submissions, discussion messages, and announcements through canvas. Assignments and all deliverables will be graded and returned no later than one week after the due date.

## About the Professor/Instructor

Welcome to **COSC 4367- COSC 5367 Cryptography**. I am Sara Memarian Esfahani, the instructor for this course. I am excited to have you in this course and look forward to learning more about you and your academic career goals while at UT Tyler. Together we will explore a variety of topics within Cryptography, including the types of encryption (symmetric and asymmetric), decryption mechanisms, and the use of cryptographic algorithms and we will journey through this course together to do great things.

## Course Description

This course on cryptography provides an introduction to the fundamentals of securing communication and information. Students will explore key concepts such as encryption and decryption, exploring the symmetric and asymmetric encryption methods, major cryptographic algorithms, and their practical applications. The curriculum covers encryption standards, public key infrastructures, and the use of cryptography in cybersecurity and privacy. Through lectures and hands-on exercises, students will learn to design and analyze cryptographic systems, gaining both theoretical knowledge and practical skills for real-world applications.

## Course Structure

This course is an Online Asynchronous Mode delivered through 5-week schedule. See the course schedule table at the end of this file and on Canvas.

**Course Objectives**

By the end of this course, students will be equipped to:

- Grasp Cryptographic Fundamentals: Learn key concepts including encryption types, decryption processes, and cryptographic algorithms.
- Evaluate Cryptographic Algorithms: Analyze the security and efficiency of major algorithms like DES, AES, RSA, and ECC.
- Implement Cryptographic Techniques: Develop skills to apply cryptography in securing digital communications and data storage.
- Explore Cryptography's Role in Security: Understand how cryptography fits into broader cybersecurity strategies and modern security challenges.

**Course Topics**

1. Information and Network Security
2. Introduction to Number Theory
3. Classical Encryption Technique
4. Block Cipher and Encryption Technique
5. Advanced Encryption Standards
6. Block Cipher Operation
7. Random Bit Generation and Stream Cipher
8. Public Key and RSA
9. Hash Function
10. Digital Signature

## Required Materials

Cryptography and Network Security: Principles and Practice, 8th edition, William Stallings, Published by Pearson (September 14, 2020) © 2020

## COURSE REQUIREMENTS AND GRADING:

Your grade will be determined based on your performance on the activities identified below. No make-up for exams, simulations, or homework will be given. It is highly likely that "extra-credit work" will be assigned to individuals as a replacement for, or in addition to, these components. All points will show up in Canvas. Be sure to review the grading schema below to determine your letter grade.

**Individual Assignments**: Weekly reading of the assigned chapter for each week. Also you are expected to complete and deliver 4 assignment during the following 5 weeks of the class. All the students are expected to submit their original work. – Individual, untimed, open-book, open-notes assignments will contain objective questions, programming exercises, and/or short-answer questions to help students review and practice course concepts and skills. Late submission (within 1 days after due date) will incur a 20% deduction in score. Submission is closed after the grace period.

**EXAMS and Quizzes**: There will be 4 quizzes and a comprehensive final exam during the semester. You will be tested on all material assigned or taught in this course which includes class slides, quizzes, videos, etc. Respondus Lockdown Browser & Monitor is required to take all exams which require a webcam feature. Instructions are posted on canvas.

If you find that there is no grade recorded for submitted work, or if you want to dispute a grade, you must send your instructor an email about the problem NO LATER THAN 2 DAYS after the submission date.

**GRADE CRITERIA:** All course work is always due at 11:59 p.m., unless otherwise noted. If you have not finished your projects, submit whatever you have completed. You will earn credit for what you complete.

| **Assignments (Subject to change)** | **Points Possible (Approx.)** |
|---|---|
| Class Quizzes (4 Q, each 50) | 200 |
| Assignments (4 Assignment, each 50) | 300 |
| Final Exam | 600 |
| **Total Points Possible with no extra credit** | **1000** |

| **Total Points (%)** | **Letter Grade** |
|---|---|
| 900 & above | A |
| 800 - 899 | B |
| 700 - 799 | C |
| 600 - 699 | D |
| 599 & below | F |

*Schedule (subject to change)*
*Due by Saturday 11:59 p.m. unless otherwise noted.*

| Week | Date | Topic / Reading | Note |
|---|---|---|---|
| Week 1 | 6/3 | Chapter 1: Information and Network Security<br>Chapter 2: Introduction to Number Theory | • Quiz 1<br>• Assignment 1 |
| Week 2 | 6/10 | Chapter 3: Classical Encryption Technique<br>Chapter 4: Block Cipher and Encryption Technique | • Quiz 2<br>• Assignment 2 |
| Week 3 | 6/17 | Chapter 6: Advanced Encryption Standards<br>Chapter 7: Block Cipher Operation | • Quiz 3<br>• Assignment 3 |
| Week 4 | 6/24 | Chapter 8: Random Bit Generation and Stream Cipher<br>Chapter 9: Public Key and RSA | • Quiz 4<br>• Assignment 4 |
| Week 5 | 7/1 | Chapter 11: Hash Function<br>Chapter 13: Digital Signature | • Review |
| Final Week | 7/5 | Final Exam | • Comprehensive |

## Code of Conduct and Ethics

Academic integrity must be exhibited in your academic work, methods and conduct. Course work for which you receive an individual grade must be your original, individual effort. If any evidence exists of copying, cheating, or any other forms of academic dishonesty on all, or part, of your graded course work, you (and any others involved) will be awarded a ZERO for that work. Sharing files also counts as academic dishonesty. A second incident will result in a grade of an "F" in this course and a recommendation for further action by the office of the Vice President for Student Development.

A few key points to remember:

I would like to point out some of the activities we have sanctioned (awarded "F" grade and sometimes even more, removed from dean's list, merit list etc.). I want to share this so that you know that we careintegrity of the degree you receive from UT Tyler.

1. In one of the semesters, some exams were conducted using Respondus lockdown browser and video monitoring. However, some students took advantage of a loophole and had help from resources outside the screen and camera. Our instructors viewed 120 hours of video recording and found a group of students involved in a coordinated plagiarism. All were sanctioned, with some losing even scholarships!
2. In one instance, a student outsourced all his assignments to a person outside this country. The assignments were flagged for abnormal activities and with the help of some technology providers we were able to trace the IP address. The student was sanctioned (awarded a "F" grade in the course))
3. In multiple instances, students have had to borrow a laptop from another student in the course and posted something as them because they had not logged out of Canvas. This is considered misconduct on the part of both students. DO NOT give another student access to your UTTyler accounts.

Almost exams and quizzes have multiple versions, and the numbers and options are different. So, if you use your peer – the chance of choosing the wrong answer is extremely high. In worst cases (it has happened in some instances), the student would have used the numbers and details.

The instructor will post both UNOFFICIAL grade reports using Canvas.

**THREE BEFORE ME RULE**: If you have any issues or questions about assignments, class policies and schedules, etc. and want to speak with me (the Professor), please remember the three before me rule as stated in the next sentence. You must have attempted at least three options before you come to me. For example: TA, tutor, grader, etc. You must tell me what you tried and the results, including screen prints of errors or printed error messages.

Name:----------

Signature:----------

Date: ----------