CS 505 Modern Cryptography

Summer 2024

Course Credits: 4
Contact Hours: 56 hours
Instructor: TBA
Email:TBA

COURSE OBJECTIVES

This course introduces the fundamental principles and design of cryptosystems, covering essential concepts in cryptography. Students will delve into traditional ciphers, block ciphers, stream ciphers, and public and private key cryptosystems. The course also includes an exploration of hash functions, authentication systems, network security protocols, and the study of malicious logic. Throughout the course, students will gain both theoretical understanding and practical skills in designing and analyzing cryptosystems.

Upon Completion of this Course, students will be able to:

1. Understand the foundational principles of cryptosystems and their role in securing information;
2. Demonstrate a solid understanding of elementary number theory and algebra as they relate to cryptography;
3. Comprehend the structure and functioning of the Data Encryption Standard (DES);
4. Understand the principles and applications of public key cryptosystems;
5. Apply cryptographic concepts to real-world scenarios, including digital signatures and secure key exchange.

PREREQUISITES

MAT 170 Linear Algebra and Matrix Theory

GRADING

Grades will be determined by accumulating points, with 100 points being the maximum, as follows:

ITEM	POINTS
4 Assignments	20 Points
2 Quizzes	20 Points
Midterm Exam	25 Points
Final Exam	35 Points
Total	100 Points

Late submissions will be graded at the end of the course. Grades will be assigned according to the following rule:

A ≥ 90 > B ≥ 80 > C ≥ 70 > D ≥ 60 > F.

We reserve the right to make adjustments to the overall grading policy.

COURSE MATERIALS

Required Texts:

W. Stallings, ***Cryptography and Network Security: Principles and Practice***.

Recommended (Optional) Texts or Other Materials:

None

COURSE TOPICS

MODULE	TASKS
Module 1	**Topics:** Topic 1: Cybersecurity, Information Security, and Network Security Topic 2: Security Services Topic 3: Cryptography Topic 4: Network Security **Assessments:** Assignment #1

Module 2	**Topics:** Topic 5: Introduction to Number Theory Topic 6: Divisibility and the Division Algorithm Topic 7: Prime Numbers Topic 8: Fermat's and Euler's Theorems **Assessments:** Assignment #2 Quiz #1
Module 3	**Topics:** Topic 9: Classical Cryptosystems Topic 10: Substitution Techniques/Transposition Techniques Topic 11: Traditional Block Cipher Structure Topic 12: The Data Encryption Standard **Assessments:** Assignment #3 Midterm Exam
Module 4	**Topics:** Topic 13: The Data Encryption Standard Topic 14: Advanced Encryption Standard Topic 15: Block Cipher Operation Topic 16: Random Bit Generation and Stream Ciphers **Assessments:** Assignment #4 Quiz #2
Module 5	**Topics:** Topic 17: Principles of Public-Key Cryptosystems Topic 18: Cryptographic Hash Functions Topic 19: Digital Signatures Topic 20: User Authentication **Assessments:** Final Exam

ATTENDANCE

1) Class attendance is required. Missing classes without permission will lead to decrease in overall grade.

Missing less than two classes: no penalty.

Missing more than two classes: 7% will be taken off from the overall grade.

If the instructor reports a student's frequent missing of class to the Soochow University Academic Administration Office, the student might get a written warning

and might be prohibited from attending final exam.

2) Participants in this course are expected to arrive in class promptly and adequately prepared. The primary objective of this course is to critically engage with the readings and the subject matter. Therefore, course participants are expected to have completed the reading prior to class and prepare thoughtful reflections/commentaries to share with fellow colleagues.

LEARNING REQUIREMENTS

1) Late assignments are not acceptable and are subjected to grade deductions.
2) Assignments submitted in the wrong format will be counted as not submitted.
3) Failure to submit or fulfill any required course component results in failure of the class.
4) Make-up for midterm and final exams only with valid excuses, as defined by the University.
5) In order to earn a Certificate of Completion, participants must thoughtfully complete all assignments by stated deadlines and earn an average quiz score of 50% or greater.

TECHNOLOGY POLICY

The use of electronic devices in class is distracting, both for the user and for the rest of the class. Only non-programmable calculators can be used in the tests and exam. Any attempts to use cell phones and other electronic communication devices will be seemed as cheating. Laptops are discouraged, unless you use them for activities DIRECTLY related to the course (eg., note taking, reading course documents).

ACEDEMIC INTEGRITY POLICY

Soochow University highly values the academic integrity and aims to promote the academic fairness, honesty and responsibility. Any academic dishonesty behaviors and any attempts to cheats and plagiarism will be reported to the university administration office. A written warning and the relevant penalties will be imposed. The record might be shown on the official university transcript.

DISABILITY ACCOMMODATION

Soochow University is committed to maintaining a barrier-free environment so that students with disabilities can fully access programs, courses, services, and activities at Soochow University. Students with disabilities who require accommodations for access to and/or participation in this course are welcome.

Note:

Please contact the University Administrative Office immediately if you have a learning disability, a medical issue, or any other type of problem that prevents professors from seeing you have learned the course material.