



CSCI, 360, 61E, Cryptography

COURSE SYLLABUS: Spring 2025

INSTRUCTOR INFORMATION

Instructor:	Dr. Mohammad Alsmirat
Office Location:	ACB1 #325
Office Hours:	Wednesday 1:30-3:30, Thursday 1:30-2:30.
Office Phone:	TBD
Office Fax:	N/A
University Email Address:	mohammad.alsmirat@tamuc.edu
Preferred Form of Communication:	EMAIL subject must contain <i>Spring 2025 - (CSCI-360-61E)</i>
Communication Response Time:	Email response within 1~2 business days

COURSE INFORMATION

Reference Textbook: *Understanding Cryptography* - Christof Paar, Jan Pelzl.

Published by Springer-Verlag Berlin Heidelberg 2010.

ISBN 978-3-642-04100-6

Course Description

The course includes key concepts and fundamental technology of cryptography, including number-theory related to cybersecurity, such as various encryption/decryption methods. The course will also cover private key / public key approaches. Some advanced methods, such as RSA, DES, and AES will be covered.

Prerequisites: [CSCI 310](#) and [MATH 2305](#).

The syllabus/schedule are subject to change.

Student Learning Outcomes

1. Become familiar with basic paradigms and principles of cryptography
2. Working knowledge of various cryptographic systems & tools
3. Learn how to evaluate the security of cryptographic systems
4. Identify and apply the appropriate cryptographic solutions

COURSE REQUIREMENTS

Minimum Technical Skills Needed

Students should be able to study independently and have strong implementation skills. Students should also be familiar with basic Linux shell commands and system skills. Students are expected to have a strong background in both mathematics and computer systems.

Instructional Methods

Face-to-face lectures and lab will be given every week in the classroom. All material related content will be posted on D2L. Assignments will be posted online on D2L, and student should work on them and submit their solution on time. Students are also encouraged to utilize discussion boards for Q&A.

GRADING

Final grades in this course will be based on the following scale:

A = 90%-100%

B = 80%-89%

C = 70%-79%

D = 60%-69%

F = 59% or Below

Assessments

Basis for Evaluation:

Assignments/projects	40%
Midterm Exam	25%
Final Exam	25%
Quizzes	10%

The syllabus/schedule are subject to change.

Quizzes:

Quizzes are brief assessments conducted during lecture time to gauge your understanding and retention of the material. They may be either spontaneous or pre-announced.

Assignments:

There will be four assignments throughout the semester. Some of these assignments may involve researching a topic and writing a brief report on it, while others may be practical tasks based on the material covered in the course

Exams:

These will be closed-book, closed-note exams designed to measure your understanding of the theoretical material. The midterm exam will cover the material completed before the exam announcement and will take place during the 8th or 9th week. It will be announced at least one week before the exam date, with further details included in the announcement. The final exam will cover the material studied after the midterm and will be held during the final week.

Project:

Project details will be announced during the 7th or 8th week.

Attendance:

Class attendance is mandatory, and students are responsible for all discussions and announcements made during classes. There will be no makeup for quizzes and only in extreme cases for exams.

Use of AI generative tools:

East Texas A&M University acknowledges that there are legitimate uses of Artificial Intelligence, chatbots, or other software that has the capacity to generate code, and textual answers. Any unreferenced and undocumented use of such software is not allowed and constitutes an instance of academic dishonesty (plagiarism).

TECHNOLOGY REQUIREMENTS

LMS

All course sections offered by East Texas A&M University have a corresponding course shell in the myLeo Online Learning Management System (LMS). Below are technical requirements

The syllabus/schedule are subject to change.

LMS Requirements:

<https://community.brightspace.com/s/article/Brightspace-Platform-Requirements>

LMS Browser Support:

https://documentation.brightspace.com/EN/brightspace/requirements/all/browser_support.htm

YouSeeU Virtual Classroom Requirements: <https://support.youseeu.com/hc/en-us/articles/115007031107-BasicSystemRequirements>

ACCESS AND NAVIGATION

You will need your campus-wide ID (CWID) and password to log into the course. If you do not know your CWID or have forgotten your password, contact the Center for IT Excellence (CITE) at 903.468.6000 or helpdesk@tamuc.edu.

Note: Personal computer and internet connection problems do not excuse the requirement to complete all course work in a timely and satisfactory manner. Each student needs to have a backup method to deal with these inevitable problems. These methods might include the availability of a backup PC at home or work, the temporary use of a computer at a friend's home, the local library, office service companies, Starbucks, a TAMUC campus open computer lab, etc.

COMMUNICATION AND SUPPORT

If you have any questions or are having difficulties with the course material, please contact your Instructor.

Technical Support

If you are having technical difficulty with any part of Brightspace, please contact Brightspace Technical Support at 1-877-325-7778. Other support options can be found here:

<https://community.brightspace.com/support/s/contactsupport>

Interaction with Instructor Statement

The instructor will try to answer questions in a timely manner. Please reach-out if you do not get a response within 1-2 business days.

The syllabus/schedule are subject to change.

COURSE AND UNIVERSITY PROCEDURES/POLICIES

Course Specific Procedures/Policies

You should do your own work on exams and for programming assignments. Copying another student's work is not acceptable. Any indication of cheating or plagiarism on an exam/assignment will result in an automatic 0 (zero) for the exam/assignment for all students involved. Yet, based on cheating and plagiarism activity in any section of class, instructor holds the right to give F grade to the identified student(s). Regarding codes in assignments, you may be required to explain the code you submitted. In case of discursive explanation, the instructor holds the right to lower your grade. No makeup exams or assignments unless documents explaining emergencies are provided.

Syllabus Change Policy

The syllabus is a guide. Circumstances and events, such as student progress, may make it necessary for the instructor to modify the syllabus during the semester. Any changes made to the syllabus will be announced in advance.

University Specific Procedures

Student Conduct

All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment. The Code of Student Conduct is described in detail in the [Student Guidebook](#).

<http://www.tamuc.edu/Admissions/oneStopShop/undergraduateAdmissions/studentGuidebook.aspx>

Students should also consult the Rules of Netiquette for more information regarding how to interact with students in an online forum:

<https://www.britannica.com/topic/netiquette>

ETAMU Attendance

For more information about the attendance policy please visit the [Attendance](#) webpage and [Procedure 13.99.99.R0.01](#).

<http://www.tamuc.edu/admissions/registrar/generalInformation/attendance.aspx>

<http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/academic/13.99.99.R0.01.pdf>

The syllabus/schedule are subject to change.

Academic Integrity

Students at East Texas A&M University are expected to maintain high standards of integrity and honesty in all of their scholastic work. For more details and the definition of academic dishonesty see the following procedures:

[Undergraduate Academic Dishonesty 13.99.99.R0.03](#)

<http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/undergraduates/13.99.99.R0.03UndergraduateAcademicDishonesty.pdf>

[Graduate Student Academic Dishonesty 13.99.99.R0.10](#)

<http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/graduate/13.99.99.R0.10GraduateStudentAcademicDishonesty.pdf>

Students with Disabilities-- ADA Statement

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you have a disability requiring an accommodation, please contact:

Office of Student Disability Resources and Services

East Texas A&M University

Gee Library- Room 162

Phone (903) 886-5150 or (903) 886-5835

Fax (903) 468-8148

Email: studentdisabilityservices@tamuc.edu

Website: [Office of Student Disability Resources and Services](#)

<http://www.tamuc.edu/campusLife/campusServices/studentDisabilityResourcesAndServices/>

Nondiscrimination Notice

East Texas A&M University will comply in the classroom, and in online courses, with all federal and state laws prohibiting discrimination and related retaliation on the basis of race, color, religion, sex, national origin, disability, age, genetic information or veteran status. Further, an environment free from discrimination on the basis of sexual orientation, gender identity, or gender expression will be maintained.

The syllabus/schedule are subject to change.

Campus Concealed Carry Statement

Texas Senate Bill - 11 (Government Code 411.2031, et al.) authorizes the carrying of a concealed handgun in East Texas A&M University buildings only by persons who have been issued and are in possession of a Texas License to Carry a Handgun. Qualified law enforcement officers or those who are otherwise authorized to carry a concealed handgun in the State of Texas are also permitted to do so. Pursuant to Penal Code (PC) 46.035 and East Texas A&M University Rule 34.06.02.R1, license holders may not carry a concealed handgun in restricted locations.

For a list of locations, please refer to the [Carrying Concealed Handguns On Campus](#) document and/or consult your event organizer.

Web url:

<http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/34SafetyOfEmployeesAndStudents/34.06.02.R1.pdf>

Pursuant to PC 46.035, the open carrying of handguns is prohibited on all East Texas A&M University campuses. Report violations to the University Police Department at 903886-5868 or 9-1-1.

COURSE OUTLINE

PART I

- Perfect secrecy vs computational secrecy
- Stream ciphers and cryptanalysis
- Modular arithmetic and Random Number Generators

PART II

- Block ciphers (DES, AES)
- Feistel networks and Galois Fields
- Review and mini project

PART III

- Public Key cryptography
- Number theory and RSA
- Diffie-Hellman Key Exchange
- Review and mini project

The syllabus/schedule are subject to change.

PART IV

- Elliptic Curve Cryptosystems
- Digital Signatures and Hash functions
- Review and mini project

PART V

- Message Authentication Codes
- Key establishment and Public-Key Infrastructure
- Review and mini project