

The Counseling Center at A&M-Commerce, located in the Halladay Building, Room 203, offers counseling services, educational programming, and connection to community resources for students. Students have 24/7 access to the Counseling Center's crisis assessment services by calling 903-886-5145. For more information regarding Counseling Center events and confidential services, please visit [www.tamuc.edu/counsel](http://www.tamuc.edu/counsel)



## CSCI 360.61E, Cryptography

COURSE SYLLABUS: Spring 2022

### INSTRUCTOR INFORMATION

|                                  |  |
|----------------------------------|--|
| Instructor:                      | Dr. Srujan Kotikela, Assistant Professor                       |
| Office Location:                 | ACB2 #210  |
| Office Hours:                    | Tuesday & Thursday 9AM – 12PM, Other times by appointment      |
| Office Phone:                    | 979-317-3429   |
| Office Fax:                      | N/A  |
| University Email Address:        | srujan <b>dot</b> kotikela <b>at</b> tamuc <b>dot</b> edu      |
| Preferred Form of Communication: | <b>EMAIL subject must contain</b> Spring 2022 - (CSCI-360-61E) |
| Communication Response Time:     | Email response within 1~2 business days                        |

### COURSE INFORMATION

**Time/Location: Tuesday/Thursday 2:50PM – 4:05 PM at ACB2 #314**

**Required 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**

### **Minimal Technical Skills Needed**

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

### **Instructional Methods and University's Pandemic Response**

Face-to-face lectures and lab will be given every week in the class room. Students are supposed to download assignments online and submit them on time. Students are also encouraged to utilize discussion boards for Q&A.

A&M-Commerce requires the use of face-coverings in all instructional and research classrooms/laboratories. Exceptions may be made by faculty where warranted. Faculty have management over their classrooms. Students not using face-coverings can be required to leave class. Repetitive refusal to comply can be reported to the Office of Students' Rights and Responsibilities as a violation of the student Code of Conduct.

Students should not attend class when ill or after exposure to anyone with a communicable illness. Communicate such instances directly with your instructor. Faculty will work to support the student getting access to missed content or completing missed assignments.

### **Student Responsibilities or Tips for Success in the Course**

Assignments will be announced on myLeoOnline. It is students' responsibility to keep up with the schedule. No makeup exams or assignments.

## **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

*The syllabus/schedule are subject to change.*

## Assessments

### Basis for Evaluation:

|               |     |
|---------------|-----|
| Mini projects | 40% |
| Assignments   | 30% |
| Final Exam    | 20% |
| Participation | 10% |

## TECHNOLOGY REQUIREMENTS

### LMS

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

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

YouSeeU Virtual Classroom Requirements:

<https://support.youseeu.com/hc/en-us/articles/115007031107-Basic-SystemRequirements>

## 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](mailto: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.

*The syllabus/schedule are subject to change.*

## **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 make an effort to answer questions in a timely manner.

## **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 emergency 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).  
<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:

*The syllabus/schedule are subject to change.*

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

### **TAMUC 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>

### **Academic Integrity**

Students at Texas A&M University-Commerce 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**

Texas A&M University-Commerce

Gee Library- Room 162

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

Fax (903) 468-8148

Email: [studentdisabilityservices@tamuc.edu](mailto:studentdisabilityservices@tamuc.edu)

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

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

*The syllabus/schedule are subject to change.*

## **Nondiscrimination Notice**

Texas A&M University-Commerce 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.

## **Campus Concealed Carry Statement**

Texas Senate Bill - 11 (Government Code 411.2031, et al.) authorizes the carrying of a concealed handgun in Texas A&M University-Commerce 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 A&M-Commerce 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 A&MCommerce campuses. Report violations to the University Police Department at 903886-5868 or 9-1-1.

*The syllabus/schedule are subject to change.*

# 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

## 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

*The syllabus/schedule are subject to change.*