MATH 536 Cryptography

COURSE SYLLABUS: Summer I 2022

INSTRUCTOR INFORMATION

Instructor: Padmapani Seneviratne
Office Location: BIN 316
Office Hours: Virtual office hours. MTWR: 10:00 – 11:00 am virtual.
(The zoom link for office hours will be available on D2L)
Office Phone: 903- 886-5952
Office Fax: 903-886-5945
University Email Address: Padmapani.seneviratne@tamuc.edu

Preferred Form of Communication**: email**
Communication Response Time: within 24 hours during weekdays

COURSE INFORMATION

Textbook: Introduction to cryptography with coding theory, second edition. Wade Trappe and Lawrence C. Washington, Prentice Hall, ISBN 0-13-186239-1.

Additional Reading:

1). Understanding cryptography, Christof Paar and Jan Pelzl, Springer, ISBN 978-3-642-44649-8.

2). Cryptography: Theory and practice, fourth edition, Douglas R. Stinson and Maura B. Paterson. CRC press, ISBN 978-1-138-19701-5

Instructional:

This is a fully online class: All class material will be available through MYLEO online (D2L) website.

Software:

A computer algebra system will be used to illustrate examples and algorithms.

The *syllabus/schedule are subject to change.*

Course Description

Catalogue: The course begins with some classical cryptanalysis (Vigenere ciphers, etc). The remainder of the course deals primarily with number-theoretic and/or algebraic public and private key cryptosystems and authentication, including RSA, DES, AES and other block ciphers. Some cryptographic protocols are described as well. Prerequisites: MATH 437, or MATH 537, or consent of the instructor.

Topics to be covered:

1. Construction and analysis of simple cryptosystems (shift, affine, Vigenere, linear feedback shift registers)

2. The one-time pad and perfect secrecy

3. Public key cryptography (RSA, finding large primes, factoring techniques, ElGamal systems)

4. The Data Encryption Standard and the Advanced Encryption Standard

5. Signature schemes

6. Key distribution

7. Secret sharing schemes

8. Hash functions

9. Zero-knowledge proofs (prove that you have some information without revealing the information)

10. Elliptic curves and ID-based cryptography

Student Learning Outcomes: Upon successful completion of this course students will:

- Construct classical cryptosystems.
- Demonstrate knowledge and understanding of concepts such as public key cryptography, signature schemes, key distribution.
- Analyze cryptographic methods and protocols.
- Understand mathematical theory behind cryptography.
- Implement cryptographic algorithms.

COURSE REQUIREMENTS

Attendance and participation:

Online attendance is required. Your log in, video viewing, homework and participation in our course in D2L determine online participation in this course.

Exams

There will be one midterm exam and a final exam: Both exams will be proctored virtually on Zoom.

Midterm Exam: Thursday June 23rd 2022 from 5:00 – 7:00 pm

Final Exam: Thursday, July 7th 2021 from 5:00 – 7:00 pm

Home Work:

Please submit the home work in pdf format. Write clearly and keep space between lines. Save the file as firstname_lastname_HW#.pdf

At end of each chapter, homework problems will be assigned and will be graded. Submit homework through D2L. The assignment that you submit must be your own work. Plagiarism is prohibited.

Grading policy: The course grade consists of

Home-work and projects:	40%
Midterm Exam	30%
Final Exam:	30%
Total:	100%

Grading Scale:

A: 90 – 100%, B: 80 – 89%, C: 70 – 79%, D:60 – 69%, F: 0 – 59%

The *syllabus/schedule are subject to change.*

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

YouSeeU Virtual Classroom Requirements:
https://support.youseeu.com/hc/en-us/articles/115007031107-Basic-System-Requirements

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

The *syllabus/schedule are subject to change.*

COURSE AND UNIVERSITY PROCEDURES/POLICIES

Course Specific Procedures/Policies

You are expected to attend all classes.

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

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

The *syllabus/schedule are subject to change.*

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
Website: Office of Student Disability Resources and Services
http://www.tamuc.edu/campusLife/campusServices/studentDisabilityResourcesAndServices/

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.

The *syllabus/schedule are subject to change.*

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&M-Commerce campuses. Report violations to the University Police Department at 903-886-5868 or 9-1-1.

A&M-Commerce Supports Students' Mental Health

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

COURSE OUTLINE / CALENDAR

Daily Schedule

Date	Topic/Chapter
June 06	1: Introduction to cryptography/Magma
June 07	1: Number theory essentials
June 08	2: Shift and affine ciphers
June 09	2: Vigenere cipher
June 10	2: block ciphers
June 13	3: RSA cipher
June 14	3: Attacks on RSA
June 15	3: Primality Testing
June 16	4: Discrete log problem and introduction to cyclic groups
June 17	4: Shank's and Pollard-Rho algorithms
June 20	4: ElGamal cryptosystem
June 21	5: The secure hash algorithm
June 22	5: The secure hash algorithm
June 23	**Midterm Exam**
June 24	5: Birthday attacks
June 27	6: Digital signatures: RSA signature
June 28	6: ElGamal signature scheme
June 29	6: The digital signature algorithm
June 30	7: Secret sharing schemes
July 01	7: Secret sharing scehems

The *syllabus/schedule are subject to change.*

July 05	8: Introduction to elliptic curves
July 06	8: Elliptic curve cryptography
July 07	**Final Exam**

The *syllabus/schedule are subject to change.*