Course Information

Course Number:	MATH 470
Course Title:	Communications and Cryptography
Section:	502
Time:	11:10am-12:25pm, Tue, Thu
Location:	RICH 114
Credit Hours:	3

Instructor Details

Instructor:	Chun-Hung Liu
Office:	Blocker 631B
E-Mail:	chliu@math.tamu.edu
Office Hours:	Tue 2:00-4:00pm (face-to-face) or by appointments (face-to-face or Zoom)

Course Description

Introduction to coded communications, digital signatures, secret sharing, one-way functions, authentication, error control and data compression.

Course Prerequisites

MATH 304 or MATH 309 or MATH 311 or MATH 323; CSCE 110 or CSCE 111 or CSCE 121 or CSCE 206 or ENGR 112; approval of instructor.

Special Course Designation

This course does not have special course designations.

Course Learning Outcomes

This course builds background in modern cryptography and related mathematical tools. Upon successful completion of this course, students will have abilities to explore advanced or related topics in cryptography.

Textbook and/or Resource Materials

"An Introduction to Mathematical Cryptography", Second Edition, by Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman. Springer, ISBN 978-1-4939-1710-5 (eBook ISBN 978-1-4939-1711-2). (Required material)

To purchase the materials for this class, visit the TAMU bookstore (online or in person). You are not required to purchase the materials from the TAMU bookstore.

Grading Policy

Homework assignments (20%)

- There will be one homework assignment almost every week. Practicing is the best way to absorb the materials covered in lectures. Collaboration and discussion for homework assignments are allowed, but you must write down the solutions on your own and submit your own copy.
- No late assignment will be accepted except for university approved excuses. Deadline and detailed instructions will be included in the problem sheet of each assignment.
- Only the best 10 grades among the assignments will be counted toward the final semester grade.
- Each assignment contains two types of questions: "required submission questions" and "suggested practice". For each assignment, all or some questions of "required submission questions" will be chosen, and only those chosen problems will be graded. The grade of those chosen problems is the grade of this assignment. We will announce which problems are chosen after the grading is complete.
- The solutions of all "required submission questions" will be posted at the course website at Canvas.

All homework must be submitted to Gradescope. No paper submission or email submission will be accepted unless you obtain an extra permission.

2 midterm exams (50%: 25% for each midterm exam).

- Exam time: **Lecture time (11:10am-12:25pm) on October 4 Tuesday**, and **November 17 Thursday**.
- No collaboration or discussion are allowed for exams.
- No make-up exam will be given unless you have university approved excuses and submit related documents in accordance Student Rules and Late Work Policy stated below.
- More details will be given when the date approaches.

Final exam (30%)

- Exam time: **December 9 Friday, 3:00pm-5:00pm** (official final exam schedule).
- No collaboration or discussion are allowed for exams.
- No make-up exam will be given unless you have university approved excuses and submit related documents in accordance Student Rules and Late Work Policy stated below.
- More details will be given when the date approaches.

For the final semester grade, students who get **90%-100% of points will be an A, 80%-90% of points will be a B, 70%-80% of points will be a C, 60%-70% of points will be a D, and an F for otherwise.**

Grades record will be frequently updated at the course website at Canvas. You are required to frequently check the correctness of the grade record posted there. Requests for record correction or regrading for any question in assignments should be made within one week after the grading is complete. The deadline for requesting regrading midterm or final exams will be announced when the grading is complete.

Graded Class Participation – Attending lectures is expected. See *Student Rule 7*.

Late Work Policy

- No submission for assignments or exams will be accepted after the deadline, except for university approved excuses.

- Make-ups for missed exams will be given only if the absence is due to university approved excuses.
- Based on university rules, all absence notifications should be sent to the instructor in writing no later than the end of the next working day after the absence (and prior to the absence if possible).
- The make-up should be done within one week after you return school.

Details about university approved excuses can be found in *Student Rule 7*.

Course Schedule

- The Midterm exams will be on October 4 and November 17 during the lecture time. The Final exam will be at 3:00pm-5:00pm on December 9.
- Topics that will be covered in this course include the following:
  - Week 1: Simple substitution ciphers, divisibility, and greatest common divisor
  - Week 2: Modular arithmetic and prime numbers
  - Week 3: Powers, primitive roots, and symmetric and asymmetric ciphers
  - Week 4: Public keys, discrete logarithm, Diffie-Hellman key exchange, and Elgamal public key cryptosystem
  - Week 5: Hardness and collision algorithms for the DLP, Chinese Remainder Theorem, and Pohlig-Hellman algorithm
  - Week 6: Euler's formula and roots modulo pq
  - Week 7: RSA and primality test
  - Week 8: Pollard's p-1 factorization algorithm and difference of squares
  - Week 9: Smooth numbers, sieves, and index calculus
  - Week 10: Quadratic residues and probabilistic encryption
  - Week 11: Digital signatures
  - Week 12: Counting and probability
  - Week 13: Collision algorithms and Meet-in-the-Middle attacks
  - Week 14: Pollard's rho method
  - Week 15: Elliptic curves
- A more detailed tentative schedule and the deadlines for assignments will be available at the course website.

Optional Course Information Items

COVID statement –To help protect Aggieland and stop the spread of COVID-19, Texas A&M University urges students to be vaccinated and to wear masks in classrooms and all other academic facilities on campus, including labs. Doing so exemplifies the Aggie Core Values of respect, leadership, integrity, and selfless service by putting community concerns above individual preferences. COVID-19 vaccines and masking — regardless of vaccination status — have been shown to be safe and effective at reducing spread to others, infection, hospitalization, and death.

University Policies

Attendance Policy

The university views class attendance and participation as an individual student responsibility. Students are expected to attend class and to complete all assignments.

Please refer to Student Rule 7 in its entirety for information about excused absences, including definitions, and related documentation and timelines.

Makeup Work Policy

Students will be excused from attending class on the day of a graded activity or when attendance contributes to a student's grade, for the reasons stated in Student Rule 7, or other reason deemed appropriate by the instructor.

Please refer to Student Rule 7 in its entirety for information about makeup work, including definitions, and related documentation and timelines.

Absences related to Title IX of the Education Amendments of 1972 may necessitate a period of more than 30 days for make-up work, and the timeframe for make-up work should be agreed upon by the student and instructor" (Student Rule 7, Section 7.4.1).

"The instructor is under no obligation to provide an opportunity for the student to make up work missed because of an unexcused absence" (Student Rule 7, Section 7.4.2).

Students who request an excused absence are expected to uphold the Aggie Honor Code and Student Conduct Code. (See Student Rule 24.)

Academic Integrity Statement and Policy

"An Aggie does not lie, cheat or steal, or tolerate those who do."

"Texas A&M University students are responsible for authenticating all work submitted to an instructor. If asked, students must be able to produce proof that the item submitted is indeed the work of that student. Students must keep appropriate records at all times. The inability to authenticate one's work, should the instructor request it, may be sufficient grounds to initiate an academic misconduct case" (Section 20.1.2.3, Student Rule 20).

Texas A&M at College Station
You can learn more about the Aggie Honor System Office Rules and Procedures, academic integrity, and your rights and responsibilities at aggiehonor.tamu.edu.

Texas A&M at Galveston
You can learn more about the Honor Council Rules and Procedures as well as your rights and responsibilities at tamug.edu/HonorSystem.

Texas A&M at Qatar
You can learn more about academic integrity and your rights and responsibilities at Texas A&M University at Qatar by visiting the Aggie Honor System website.

Americans with Disabilities Act (ADA) Policy

Texas A&M University is committed to providing equitable access to learning opportunities for all students. If you experience barriers to your education due to a disability or think you may have a disability, please contact the Disability Resources office on your campus (resources listed below) Disabilities may include, but are not limited to attentional, learning, mental health, sensory, physical, or chronic health conditions. All students are encouraged to discuss their disability related needs with Disability Resources and their instructors as soon as possible.

Texas A&M at College Station
Disability Resources is located in the Student Services Building or at (979) 845-1637 or visit disability.tamu.edu.

Texas A&M at Galveston
Disability Resources is located in the Student Services Building or at (409) 740-4587 or visit tamug.edu/counsel/Disabilities.

Texas A&M at Qatar
Disability Services is located in the Engineering Building, room 318C or at +974.4423.0316 or visit https://www.qatar.tamu.edu/students/student-affairs/disability-services.

Title IX and Statement on Limits to Confidentiality

Texas A&M University is committed to fostering a learning environment that is safe and productive for all. University policies and federal and state laws prohibit gender-based discrimination and sexual harassment, including sexual assault, sexual exploitation, domestic violence, dating violence, and stalking.

With the exception of some medical and mental health providers, all university employees (including full and part-time faculty, staff, paid graduate assistants, student workers, etc.) are Mandatory Reporters and must report to the Title IX Office if the employee experiences, observes, or becomes aware of an incident that meets the following conditions (see University Rule 08.01.01.M1):

- The incident is reasonably believed to be discrimination or harassment.
- The incident is alleged to have been committed by or against a person who, at the time of the incident, was (1) a student enrolled at the University or (2) an employee of the University.

Mandatory Reporters must file a report regardless of how the information comes to their attention – including but not limited to face-to-face conversations, a written class assignment or paper, class discussion, email, text, or social media post. Although Mandatory Reporters must file a report, in most instances, a person who is subjected to the alleged conduct will be able to control how the report is

handled, including whether or not to pursue a formal investigation. The University's goal is to make sure you are aware of the range of options available to you and to ensure access to the resources you need.

Texas A&M at College Station
Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with Counseling and Psychological Services (CAPS).

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's Title IX webpage.

Texas A&M at Galveston
Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with the Counseling Office in the Seibel Student Center, or call (409)740-4587. For additional information, visit tamug.edu/counsel.

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the Galveston Campus' Title IX webpage.

Texas A&M at Qatar
Texas A&M University at Qatar students wishing to discuss concerns in a confidential setting are encouraged to visit the Health and Wellness website for more information.

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's Title IX webpage.

Statement on Mental Health and Wellness

Texas A&M University recognizes that mental health and wellness are critical factors that influence a student's academic success and overall wellbeing. Students are encouraged to engage in healthy self-care by utilizing available resources and services on your campus

Texas A&M College Station
Students who need someone to talk to can contact Counseling & Psychological Services (CAPS) or call the TAMU Helpline (979-845-2700) from 4:00 p.m. to 8:00 a.m. weekdays and 24 hours on weekends. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

Texas A&M at Galveston
Students who need someone to talk to can call (409) 740-4736 from 8:00 a.m. to 5:00 p.m. weekdays or visit tamug.edu/counsel for more information. For 24-hour emergency assistance during nights and weekends, contact the TAMUG Police Dept at (409) 740-4545. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

Texas A&M at Qatar

Texas A&M University at Qatar students wishing to discuss concerns in a confidential setting are encouraged to visit the Health and Wellness website for more information.

Campus-Specific Policies

Texas A&M at Galveston

Classroom Access and Inclusion Statement

Texas A&M University is committed to engaged student participation in all of its programs and courses and provides an accessible academic environment for all students. This means that our classrooms, our virtual spaces, our practices and our interactions are as inclusive as possible and we work to provide a welcoming instructional climate and equal learning opportunities for everyone. If you have an instructional need, please notify me as soon as possible.

The Aggie Core values of respect, excellence, leadership, loyalty, integrity and selfless service in addition to civility, and the ability to listen and to observe others are the foundation of a welcoming instructional climate. Active, thoughtful and respectful participation in all aspects of the course supports a more inclusive classroom environment as well as our mutual responsibilities to the campus community.

The following statements below are optional. Leave as is to include, or delete if preferred. Either way, delete this note.

Statement on the Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law designed to protect the privacy of educational records by limiting access to these records, to establish the right of students to inspect and review their educational records and to provide guidelines for the correction of inaccurate and misleading data through informal and formal hearings. Currently enrolled students wishing to withhold any or all directory information items may do so by going to howdy.tamu.edu and clicking on the "Directory Hold Information" link in the Student Records channel on the MyRecord tab. The complete FERPA Notice to Students and the student records policy is available on the Office of the Registrar webpage.

Items that can never be identified as public information are a student's social security number, citizenship, gender, grades, GPR or class schedule. All efforts will be made in this class to protect your privacy and to ensure confidential treatment of information associated with or generated by your participation in the class.

Directory items include name, UIN, local address, permanent address, email address, local telephone number, permanent telephone number, dates of attendance, program of study (college, major, campus), classification, previous institutions attended, degrees honors and awards received, participation in officially recognized activities and sports, medical residence location and medical residence specialization.