# Communications and Cryptography

### Math 470-504

### Fall Semester 2023

**Instructor:** Peter F. Stiller

**Office:** Blocker Bldg. 623D

**Office Phone:** Due to financial constraints office phones were removed some time ago.

**E-mail:** p-stiller@tamu.edu
DO NOT send email to any other email address as it is virtually certain to be overlooked or deleted. With the reorganization of the university certain email addresses are no longer be valid. If you are replying to one of my emails, MAKE SURE that the above address is where the reply is going. In all emails please put "your name, Math 470, and the subject of the message" in the subject line.

**Office Hours:** Fall 2023 Schedule
Office hours will be a mix of online and in person sessions (see the link to my Fall 2023 Schedule above). Links for the online sessions will be emailed to you the first week of class. In person sessions will be at my office (623D Blocker). Because I teach two large sections of Math 470, it may be necessary to break the classes into two groups for office hours. If that happens, please attend only those times assigned to your section (504 in this case). You are always welcome to listen in at the other times, but questions will only be taken from students in the appointed section. Also, you may make an individual appointment to speak with me on Zoom at a mutually agreeable time. Just email me with some time options suitable for you. Hopefully one of those will work for me.

## Course Organization and Requirements

**Time:** MWF 3:00pm to 3:50pm
Our class meets Monday, Wednesday and Friday at 3:00pm from Monday August 21st through Monday December 4th. The instructor will deliver in person lectures unless he is ill (e.g. quarantined for COVID) or traveling on University business, in which case lectures will be given by a substitute instructor or via **Zoom** during the scheduled class time. Recorded versions of the lectures WILL NOT be available. Posted times are local time on the main campus of Texas A&M.

**Place:** BLOC 117

**Course Format:** This course is a 16-week course taught in a face-to-face format, with a few weeks of instruction consisting of just a single class day or just two class days. Throughout the course this document will be your primary source for course information and material. It will be your guide to course events, especially quizzes and exams, suggested homework, and course notes. All tests, quizzes, or other work will be taken or submitted in class on the day it is scheduled or due. Additional instructions will be provided for each of these items.

**Pay special attention to the dates and times for scheduled quizzes and exams!! DO NOT schedule other**

**activities for these times.** Should you miss an exam, you will need a valid University authorized excuse to schedule a make-up - see the policy on absences below.

**Text:** *An Introduction to Mathematical Cryptography* by Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, **2nd Edition**, Undergraduate Texts in Mathematics, Springer, New York, 2014. You **will** need to purchase a copy of this book for the course.

**Note: The required text is the second edition published in 2014, NOT the original first edition. There are differences between the two editions. While the material covered is generally the same, the arrangement of the chapters, exercises, etc. is different. You will be responsible for doing readings and exercises from the second edition.**

**Supplementary Texts:** (These are not required, but are useful references.)
*An Introduction to Number Theory with Cryptography* by J. S. Kraft and L. C. Washington, CRC Press, 2014.
*Introduction to Cryptography with Coding Theory* by W. Trappe and L. C. Washington, Prentice Hall, 2006.

**Computer Hardware Requirements:**
A laptop,smart phone, or tablet that can access the internet in BLOC will be very useful. Several highly efficient online calculators for the specialized mathematics used in our cryptographic algorithms are available online and may be allowed during an exam. While the exam/quiz problems can be done without these, you will save considerable time if you can use them during the exam. I am not sure how they will work on a particular smart phone, so a laptop or tablet is best.

**Texas A&M Student ID:** For each quiz or exam you should be prepared to show your TAMU student ID to the proctor in order to be admitted to the exam, and you should be prepared to show it at any time when requested during the exam.

**Pre-Class Form:** You will receive a form via email prior to the start of class. It must be completed and returned per the instructions on the form. It will certify on your part that you have read and understood everything on this syllabus and will abide by the Honor Code. Submission of this form will also serve to verify your attendance in the class. It is a Federal requirement that instructors certify students as attending for financial aid purposes. Failure to submit the form could result in your not being certified present and may result in loss of financial aid.
**Pre-Class Form**

**Communication Strategy:** Email is the best way to contact me on an individual basis. I can be reached **only, repeat, only** at p-stiller@tamu.edu. I will do my best to respond to you within 24 hours, excluding weekends. Hopefully I can respond quicker than 24 hours, but I can't guarantee a quick response all of the time, especially on the weekends. When emailing please BE SURE to put "Your Name, Math 470" in the subject line.

**Zoom Appointment**: I am available for Zoom appointments. Please contact me via email to schedule a mutually agreeable time to speak.

**Netiquette**: Be sure to participate in online office hours and if necessary online lectures or exams in a responsible and respectful way that is consistent with good academic practice. To learn about polite online behavior, or "netiquette", check the following link: http://albion.com/netiquette/corerules.html . Violation of netiquette will result in your withdrawal from the class.

---

# Course Information:

**Prerequisites:** Some experience with proofs - for example Math 304.

**Grades:** We will have three major exams. Each major exam will count for 25%. We will have 7 quizzes roughly similar to the suggested homework problems. The quizzes will count 25% (best 5 of 7).

In calculating your final grade for the semester the usual scale will apply 100-90 A, 89-80 B, 79-70 C, 69-60 D, 59 and below F.

**IMPORTANT!! Exam dates are Friday September 29th, Friday November 10th, and Friday December 1st. DO NOT schedule other activities for these dates and times.**

**Grading Contingency:** At any point in the semester if we move to online instruction due to escalating covid cases and/or hospitalizations, or other exigent events, the grading scheme will change. Items already graded will be counted based on their percentage as above. Only 1 quiz will be dropped and no further quizzes will be administered. The remaining percentage of the grade will be based solely on exams, either take-home or online, with the percentage that each exam will count divided equally between them.

**Course Policies:** Attending class is one of your responsibilities. You will be held responsible for any announcements, information, and/or lecture material (not necessarily from the book) that is presented in class. Make-ups for exams will only be permitted with a university allowable excuse in writing and will be made up at the first opportunity, usually **within 48 hours** . Late work will not be accepted. If you have a university excused absence the day the work is due, you must turn it in no later than the next class period with a copy of your official excuse attached. It must be signed by an appropriate university or medical official. It is expected that your work be solely your own work. No collaboration is permitted, but you should feel free to discuss the problems with the instructor during office hours. Since we are allowing two quizzes to be dropped, **there will be no make-ups for missing a quiz.** You still must present your official University excuse. If you miss more than two quizzes, you will need to speak to me. In all cases, you MUST have a written university excuse signed by an appropriate university or medical official for every quiz or exam you miss.

**Overview:** This course will introduce students to the mathematics and methods used in modern Cryptography and Secure Communications. The course will also touch on mathematical aspects of Cybersecurity and Data Encryption, and if time permits, we will discuss Blockchain technology and Cryptocurrencies such as Bitcoin.

**Learning Objectives:** Upon completion of this course the student should have an understanding of the basic mathematics used in modern cryptographic applications. In addition he or she will gain experience in using that mathematics to construct various ciphers, coding methods, and secure communication protocols.

---

# Course Topics

**Detailed Description:** We will cover roughly half of the book. This will be supplemented with material from other sources.

**Topics**

- **Substitution Ciphers**
- **Modular Arithmetic**
- **Divisibility and GCD's**
- **Unique Factorization and Applications**
- **Primitive Roots**
- **Symmetric and Asymmetric Ciphers**
- **Discrete Logarithms**

- **Diffie Helman Key Exchange**
- **El Gamal Public Key Cryptosystem**
- **Pohlig-Hellman Algorithm**
- **Euler's Formula**
- **RSA and Secret Sharing**
- **Primality Testing**
- **Index Calculus and Sieves**
- **Digital Signatures**
- **Elliptic Curves in Cryptography**
- **Miscellaneous Topics including Cryptocurrencies.**

---

# Course Schedule

## Week 1 August 21st - August 25th

Read: Chapter 1, Sections 1.1-1.2. Try the following exercises:

- Section 1.1, pages 47-49, Exercises 1.2a, 1.3, 1.4a, 1.5b(i).
- Section 1.2, pages 49-51, Exercises 1.6a,b, 1.7c, 1.9a,b, 1.10 (for 1.9a,b), 1.14.

Note: Exercises are for your practice. They will not be turned in for grade unless you are notified in advance.

**Week 1 Lecture Notes.**

## Week 2 August 28th to September 1st

Read: Chapter 1, Sections 1.3-1.5. Try the following exercises:

- Section 1.3, pages 51-53, Exercises 1.16a, 1.17, 1.18b,c,f,g, 1.22a, 1.23, 1.27a.
- Section 1.4, pages 53-54, Exercises 1.28, 1.29, 1.30b, 1.31a.
- Section 1.5, pages 54-56, Exercises 1.32a, 1.33, 1.34a,b, 1.35, 1.36a.

**Homework Solutions Chapter 1**

**Week 2 Lecture Notes.**

## Week 3 September 4th - September 8th (Note: No class Monday 9/4/23 - Labor Day.)

## Quiz #1 Friday September 8th covering Chapter 1.

Read: Chapter 1, Sections 1.6 and 1.7 and Chapter 2, Sections 2.1 and 2.2. Try the following exercises:

- Section 1.6, pages 56-57, Exercises 1.40, 1.41b.
- Section 1.7, pages 57-59, Exercises 1.42, 1.43a,b, 1.44a,b,d,e, 147, 150.
- Section 2.1, page 107, Exercises 2.1 and 2.2. Just read these two essay exercises and think about them.
- Section 2.2, pages 107-108, Exercises 2.3 (Note the discrete log is only defined mod p-1.), 2.4a,b (Check 2 is a primitive root mod 13 as well in part a.)

**Week 3 Lecture Notes Sections 1.6 and 1.7**

**Week 3 Lecture Notes Sections 2.1 and 2.2**

### Week 4 September 11th - September 15th

### Quiz #2 Wednesday September 13th covering Chapter 2: Sections 2.1-2.4.

Read: Chapter 2, Sections 2.3-2.6. Try the following exercises:

- Section 2.3, page 108, Exercise 2.6.
- Section 2.4, pages 108-109, Exercise 2.8.
- Section 2.5, pages 109-110, Exercises 2.11, 2.13a, 2.15b,c.
- Section 2.6, page 110, Exercise 2.16c.

**Homework Solutions Chapter 2 - all sections.**

**Week 4 Lecture Notes Sections 2.3 and 2.4**

**Week 4 Lecture Notes Sections 2.5 and 2.6**

### Week 5 September 18th - September 22nd

### Quiz #3 Friday September 22nd covering Chapter 2, Sections 2.5 - 2.9

Read: Chapter 2, Sections 2.7-2.9. Try the following exercises:

- Section 2.7, page 110, Exercise 2.17a (Try part b if you like to program.)
- Section 2.8, pages 110-112, Exercises 2.18a,b,d, 2.20, 2.21a, 2.23a, 2.24a,b,c, 2.25.
- Section 2.9, page 112, Exercises 2.26, 2.28a.

**Week 5 Lecture Notes Section 2.7**

**Week 5 Lecture Notes Sections 2.8 and 2.9**

## EXAM 1 Friday September 29th over Chapters 1 and 2.

### Week 6 September 25th - September 29th

Read: Chapter 3, Sections 3.1-3.3 Try the following exercises:

- Section 3.1, pages 180-181, Exercises 3.1a,e, 3.3, 3.4a,b,read c, 3.5 read then do (e)(iii), 3.6b(i).
- Section 3.2, pages 182-183, Exercises 3.7a,b, 3.8, 3.9a.
- Section 3.3, page 183, Exercise 3.13 just read this exercise.

**Homework Solutions Chapter 3 Sections 3.1-3.3.**

**Week 6 Lecture Notes Sections 3.1, 3.2 and 3.3**

## Week 7 October 2nd to October 6th

## Quiz #4 Wednesday October 4th covering Chapter 3, Sections 3.1-3.4.

Read: Chapter 3, Sections 3.4-3.6. Try the following exercises:

- Section 3.4, pages 183-186, Exercises 3.14a,b(iii), 3.15a,b,c, 3.17a, 3.18a(iii). Just read exercises 3.19 and 3.20.
- Section 3.5, page 186, Exercise 3.22a.
- Section 3.6, pages186-187, Exercises 3.24a, 3.25a, 3.26a,b.

**Homework Solutions Chapter 3 Sections 3.4-3.6.**

**Week 7 Lecture Notes Section 3.4**

**Week 7 Lecture Notes Sections 3.5 and 3.6**

## Week 8 October 9th - October 13th

Review and catch-up. Monday and Tuesday are Fall Break, so no class on Monday October 9th.

## Week 9 October 16th to October 20th

Read: Chapter 3, continue reading Section 3.6 and read Sections 3.7-3.8. Try the following exercises:

- Section 3.7, page 187, Exercise 3.27b,e
- Section 3.8, page 189, Exercise 3.36.

**Homework Solutions Chapter 3 Sections 3.7-3.10.**

**Week 9 Lecture Notes Section 3.7 and 3.8**

## Week 10 October 23rd - October 27th

## Quiz #5 Wednesday October 25th covering Chapter 3, Sections 3.5 - 3.8.

Read: Chapter 3, Sections 3.9 and 3.10 and Chapter 4, Section 4.1. Try the following exercises:

- Section 3.9, pages 189-190, Exercises 3.37, 3.38, 3.39a,b(i), read 3.40.
- Section 3.10, page 191, Exercise 3.42a.
- Section 4.1, No Exercises.

**Week 10 Lecture Notes Section 3.9.**

**Week 10 Lecture Notes Section 3.10, 4.1 and 4.2.**

### Week 11 October 30th - November 3rd

Read: Chapter 4, Sections 4,2 and 4.3. Try the following exercises:

- Section 4.2, pages 203-204, Exercises 4.1, 4.2, for fun try 4.3.
- Section 4.3, pages 204-205, Exercises 4.5, 4.6, 4.9.

**Homework Solutions Chapter 4 Sections 4.2-4.3.**

**Week 11 Lecture Notes Section 4.3.**

## EXAM 2 Friday November 10th over Chapters 3 and 4.

### Week 12 November 6th - November 10th

Read: Chapter 5, Sections 5.2-5.4. Read Section 5.1 if you are unfamiliar with permutations and combinations. Try the following exercises:

- Section 5.1, pages 282-284, Exercises 5.1a,b,c,d, 5.4a,b, 5.6a, 5.9.
- Section 5.2, pages 284-288, Exercises 5.10a, 5.11a, 5.14, 5.15a, 5.16.
- Section 5.3, pages 288-293, Exercises 5.20, 5.22, 5.23a,b,c,d,just read e, 5.24, 5.27a, 5.28, 5.29, 5.30.
- Section 5.4, pages 246-253, Exercises 5.37 and 5.39.

**Homework Solutions Chapter 5 Sections 5.1-5.3.**

**Week 12 Lecture Notes Sections 5.1, 5.2, and 5.3.**

**Week 12 Lecture Notes Section 5.4.**

### Week 13 November 13th - November 17th

### Quiz #6 Friday November 17th over Chapter 4 and Chapter 5, Sections 5.1-5.2.

Read: Chapter 5 (continue) and Chapter 6, Sections 6.1-6.3. Try the following exercises:

- Section 6.1, page 361, Exercises 6.1, 6.2, 6.4a,d,e.
- Section 6.2, pages 361-362, Exercises 6.5a,b, 6.6a, 6.7a,c.
- Section 6.3, pages 362-363, Exercises 6.8, 6.11a.

**Homework Solutions Chapter 6 Sections 6.1-6.3.**

**Week 13 Lecture Notes Section 6.1.**

**Week 13 Lecture Notes Sections 6.1 continued and 6.2.**

**Week 13 Lecture Notes Sections 6.3 and 6.4.**

**Note: Wednesday November 15th at 5pm is the deadline to Q-drop or to officially withdraw from the University.**

### Week 14 November 20th - November 24th

Chapter 6 (continued) and review.

Reading Day Wednesday November 22 - no class. Also no class Thursday November 23rd and Friday November 24th - Thanksgiving Holiday.

**Week 14 Lecture Notes.**

### Week 15 November 27th - December 1st

### Quiz #7 Wednesday November 29th over Sections 6.1-6.3.

## EXAM 3 Friday December 1st: Comprehensive Exam plus Chapter 5 and Chapter 6 Sections 6.1 to 6.4.

Read: Chapter 6, Sections 6.4 and 6.5. Try the following exercises:

- Section 6.4, pages 363-365, Exercises 6.14a,b, 6.16a,b, read 6.17, read 6.18, do 6.20a,b.
- Section 6.5, no exercises

**Homework Solutions Chapter 6 Sections 6.4-6.6.**

**Week 15 Lecture Notes.**

### Week #16 December 4th

**Monday December 4th is our last day of class.**

Read: Chapter 6, Section 6.6 and the Bitcoin handout. Try the following exercises:

- Section 6.6, page 365 , Exercise 6.21a,c.

---

**University Policy on Absences:** If an absence is excused, the instructor will either provide the student an opportunity to make up any quiz, exam or other work that contributes to the final grade **or provide a satisfactory alternative** by a date agreed upon by the student and instructor. If the instructor has a regularly scheduled make up exam, students are expected to attend unless they have a university approved excuse. The

make-up work must be completed in a timeframe not to exceed 14 calendar days from the last day of the initial absence. The student is responsible for providing satisfactory evidence to the instructor to substantiate the reason for the absence. Among the reasons absences are considered excused by the university are those listed in Student Rule 7 http://studentrules.tamu.edu/rule07 . **The fact that these are university excused absences does not relieve the student of responsibility for prior notification and documentation.** Failure to notify and/or document properly may result in an unexcused absence. Falsification of documentation is a violation of the Honor Code. Other absences may be excused at the discretion of the instructor with prior notification and proper documentation. In cases where prior notification is not feasible (e.g., accident or emergency) the student must provide notification by the end of the second working day after the absence, including an explanation of why notice could not be sent prior to the class. Accommodations sought for absences due to the observance of a religious holiday can be sought either prior or after the absence, but not later than two working days after the absence.

**Additional Course Policies:**

- Only students with university approved excuses IN WRITING will be allowed to make up missed exams! In the case of a missed exam you must notify me by the day of the exam that you will miss and make arrangements with me within one working day after the exam to take a make up.
- An Aggie does not lie, cheat or steal, or tolerate those who do. Academic integrity violations will be vigorously prosecuted according to University policies. See http://aggiehonor.tamu.edu
- The last day of class is Monday, December 4, 2023. **No** make up work (including exams and/or quizzes) will be accepted or possible after that date - December 4th at 5pm.
- There is no such thing as "extra credit". Grades will be based solely on the required tests and quizzes.

**Disabilities:** 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 believe you have a disability requiring an accommodation, please contact Disability Services, currently located in the Disability Services building at the Student Services at White Creek complex on west campus or call 979-845-1637. For additional information, visit http://disability.tamu.edu.

**Title IX and Statement on Limits to Confidentiality:** Texas A&M University and the College of Arts and Science are committed to fostering a learning environment that is safe and productive for all. University policies and federal and state laws provide guidance for achieving such an environment. Although class materials are generally considered confidential pursuant to student record policies and laws, University employees — including instructors — cannot maintain confidentiality when it conflicts with their responsibility to report certain issues that jeopardize the health or safety of our community. As the instructor, I must report (per Texas A&M System Regulation 08.01.01) the following information to other University offices if you share it with me, even if you do not want the disclosed information to be shared:

- Allegations of sexual assault, sexual discrimination, or sexual harassment when they involve TAMU students, faculty, or staff, or third parties visiting campus.

These reports may trigger contact from a campus official who will want to talk with you about the incident that you have shared. In many cases, it will be your decision whether or not you wish to speak with that individual. If you would like to talk about these events in a more confidential setting, you are encouraged to make an appointment with the Student Counseling Service (https://scs.tamu.edu/).

Students and faculty can report non-emergency behavior that causes them to be concerned at http://tellsomebody.tamu.edu.

(The above text related to Title IX and Statement on Limits to Confidentiality was developed by the former College of Liberal Arts and vetted by the Title IX Office and the Office of the General Counsel.)

**COVID Statement** To help protect Aggieland and stop the spread of COVID-19, Texas A&M University urges students to be vaccinated and when appropriate 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.