INF 385T: Applied Encryption 2 (27500)

Spring 2019
UTA 1.210B
Thursdays 9:00 am – 12:00 pm

Instructor: Walker Riley
walker.riley@utexas.edu

Office Hours: 12pm-3pm Thursday in the Makerspace

I. Course Description

Encryption is at the heart of almost everything we do online. It keeps our traffic safe and makes e-commerce possible by allowing us to trust that our financial information cannot be intercepted. Encryption is also key to confidentiality and privacy online, which is a fundamental value of the ALA.
This course aims to give students a thorough understanding of how encryption works by examining and implementing the most foundational and widely used forms of encryption. This knowledge will arm students with the technical security literacy that is vital to understanding and combating threats to confidentiality and privacy.

II. Pre-Requisites

None. Some experience with programming will be helpful, but it is by no means required. Every skill you need to do well in this course will be built, from the ground up, in this course.

III. Course Aims and Objectives

After taking this course, students will be able to:

- Discuss cyber-security with a grounding in both theory and application
- Write efficient and effective code using the scripting language Python
- Read and write in Binary
- Implement their own custom unbreakable and nearly-unbreakable crypto-systems
- Understand and utilize number theory without a background in mathematics

IV. Disclaimer

This syllabus is subject to change at any time.

V. Tentative Course Schedule

Week	Discussion Topic	In Class Exercise	Assignment Due
Jan. 24	Review		
Jan. 31	Collision Algorithms	Shanks' Baby-step Giant-step	
Feb. 7	Fast Powering in very large moduli	Chinese Remainder Theorem	Shanks bsgs
Feb. 14	Composite Moduli	Euler's formula for PQ	Chinese Remainder Thrm
Feb. 21	RSA	Send a message	
Feb. 28	Primality Testing	Miller Rabin	RSA
Mar. 7	Digital Signatures	Signatures using RSA and DH	Miller Rabin
Mar. 14	Elliptic Curves	Calculations in this space	
Mar. 21	No class	Spring Break!	

Mar. 28	Application of ECC	Send a message	EC calculator
Apr. 4	Quantum computing	Shor's Algorithm and how it affects security	ECC
Apr. 11	Overview of Lattices	Working with small lattices	
Apr. 18	Firewalls	Build a firewall	
Apr. 25	Security Standards	Security Certifications	
May 2	Final Projects	Presentations	Final Paper

VI. Course Requirements

- **Python Scripts**

  Python assignments will make up the majority of your grade because they are where you will do the majority of your learning. You are welcome to work with other students, but do let me know who you are working with. All code should be documented. This documentation should be done in commented out lines in your code and should explain what each piece of code is doing.

  While working together on code is fine, all documentation is expected to be unique. I need to see that you are able to explain your code in your own words.

  Most assignments will offer a chance to earn extra points by coding concepts not explicitly covered in class.

- **Final Paper**

  Your final paper should cover a cryptographic topic not explicitly taught in class. Your goal is to not only understand the topic, but to explain it in a digestible way.

  As an alternative to a traditional paper, students are free to write code in place of the above mentioned paper. The code should be an application of a cryptographic topic not covered in class.

  I will be flexible on topics, and if you have an idea for a project that does not strictly fit within the description I provided here, I will gladly consider allowing students to think outside the box, but I reserve the right to say no to any project idea if I deem it inappropriate or otherwise unsuitable for this project

- **Class Readings**

  Weekly readings will be mentioned in class, and will serve as reference material for assignments, but will likely not be formally posted in canvas.

  These readings will be from our textbook, and will supplement what we discuss in class.

- **Participation**

  All students are expected to attend every class. Attendance will be taken. What you get out of this course will be significantly impacted by your participation, and as such, I expect everyone to not just show up, but to be engaged and contribute.

  Having that been said, I understand that life gets in the way some times. If you know you will be missing class, try to let me know as soon as possible. If you miss class and I never hear from you about why, your participation grade will be lowered accordingly.

VII. Lab Hours (Thursday Noon – 3pm, Makerspace)

Every Thursday after class I will be in the Makerspace. You can find me there if you need to talk about anything, or if you would like to work on python. I encourage all students to come in even if they do not need assistance. The Makerspace is an excellent collaborative learning environment to work on homework, and it allows you to reach out to me in the off-chance you get stuck on a problem.

VIII. Grading Procedure

Grades will be determined as follows:

Attendance and Participation: (10%)
Python Scripts/Assignments: (70%)
Final Paper: (20%)

Note: Participation operates on a deduction system. Everyone starts the semester with all 10 points. Unexcused absences, tardiness, not participating, etc… will reduce this grade.