INF 385T: Applied Encryption 1

Fall 2018
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
Aug. 30	Introduction	Download Python, print 'hello world', introductory python exercises	
Sept. 6	History of encryption before computers (caesar ciphers, postal service, WW 2)	Python: lists	
Sept. 13	History of encryption in the age of computers (clipper chip, fbi, heartbleed, etc...)	Python: for/while loops	Python script: Calculator
Sept. 20	History of the Caesar cipher	Create a script to encrypt a message using a caesar cipher	
Sept. 27	Problems with the	Import a dictionary to cross	Python script:

	Caesar cipher and one-time pad	reference for decryption	caesar cipher decryption
Oct. 4	Introduction to Binary	Modulo	Python script: one time pad
Oct. 11	Binary and ASCII	Learn to read and write in binary	Python script: modulo calculator
Oct. 18	Backdoors (clipper chip, fbi v apple, whatsapp)	Modular Generators	Python script: convert message to or from binary
Oct. 25	Alice and Bob (and eve)	Examples – WEP/WPA	
Nov. 1	What is a cryptosystem, Diffie Hellman	Give examples of Diffie Hellman	Paper proposal
Nov. 8	Man in the middle attacks	Intercepting Diffie Hellman	Python script: Diffie Hellman
Nov. 15	Public key encryption, symmetric key encryption	Examples of ElGamal cryptosystem	Paper rough draft
Nov. 22	Thanksgiving!		
Nov. 29	Rundown of Applied Encryption 2		Python script: Elgamal
Dec. 6	Final Projects	Presentations	Final Paper

VI. Course Requirements

- **Python Scripts**

  Python assignments will make up the majority of your homework. 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.

- **Final Paper**

  Your final paper can come in many forms. I encourage students to find (or create) a cryptosystem not covered in class. Your paper should explain, in an accessible way, what your cryptosystem does. I encourage the use of Alice and Bob illustrations.

  If you are feeling particularly ambitious, I will accept code in place of a paper. If you can create a cryptosystem in Python with sufficiently detailed documentation, the I will know that you understand the material.

- **Class Readings**

  Weekly readings will be posted in canvas. All students are expect to have read all weekly readings before class as the first half of class will be spent discussing them.

- **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

Calculator: (10%)
Caesar Decipher: (10%)
One-time Pad: (10%)
Modulo Calculator: (10%)
Binary: (10%)
Diffie Hellman (10%)
Elgamal: (10%)

Final Paper: (20%)