Instructor Information

Name: Jason LeGrow
Office: McBryde 470
Email: `jlegrow@vt.edu`

Class Times

Monday, Wednesday, Friday 1:25 – 2:15pm

Class Location

McBryde 230

Office hours

Tuesday, Wednesday 2:20 – 3:20pm, and other times by appointment.

Course Website

`https://canvas.vt.edu`

Prerequisites

One of: Math 3034, 3124, 3134, 3144, 3224, 4134, or CMDA 3605

This course will require programming in a language of your choice. Some languages are better suited to the material than others—I recommend Python.

This course will require reading, writing, and understanding mathematical proofs. Prior experience with mathematical proofs—especially in modern algebra, number theory, combinatorics, or probability—would be beneficial.

Textbook

Stinson, D. R., & Paterson, M. (2018). **Cryptography: Theory and practice (fourth edition).** Chapman & Hall/CRC.

The textbook is not required, but it is *highly* recommended.

Course Objectives

This course is an introduction to symmetric-key cryptography. Students will see constructions and cryptanalysis of symmetric-key schemes, learn about "provable security" and how to write proofs in the context of cryptography, and practice implementing cryptographic algorithms.

Course Outline

I intend to cover most of the content of chapters 1–5 of the textbook. In particular:

Chapter 1: Introduction to Cryptography. Cryptosystems; hash functions; message authentication; protocols; the meaning of "security."

Chapter 2: Classical Cryptography. Classical ciphers including shift, substitution, affine, Vigenère, Hill, and permutation ciphers, and their cryptanalysis.

Chapter 3: Shannon's Theory, Perfect Secrecy, and the One-Time Pad. Perfect secrecy, entropy, and their applications.

Chapter 4: Block Ciphers and Stream Ciphers. Substitution-permutation networks; linear cryptanalysis; differential cryptanalysis; the Advanced Encryption Standard (AES); block cipher modes of operation; stream ciphers.

Chapter 5: Hash Functions and Message Authentication. Hash functions and data integrity; hash function security; message authentication codes.

Grading

Assignments will be worth 25% of your grade, two midsemester tests will be worth 40% of your grade (20% each), and the final exam will be worth 35% of your grade.

Assignments. There will be a number of assignments, each due on a **Monday at 11:59pm**. Your lowest assignment grade will be dropped. Late assignments will not be accepted.

Tests and Exams. The tests are tentatively scheduled for

1. **Monday, September 26, in class**
2. **Monday, October 24, in class**

The final exam is scheduled by the registrar's office; check the course schedule.

No books, notes, calculators, cell phones, or collaboration are allowed on tests or exams. No make-up exams will be given without written authorization from the Dean of Students Office (`dos.vt.edu`). Incomplete grades are only assigned in very rare cases (such as documented severe illness during final exams).

Collaboration

You are welcome—in fact, *encouraged*—to collaborate with current Math 4175 students while solving assignment problems. However, you must write your solutions separately, and the solution you submit must be your own. If you do collaborate, you must write the name of all of your collaborators on the first page of your assignment. If you use external resources (e.g. textbooks) you must cite them precisely. You must **not** post assessment problems or solutions on any platform (*e.g.,* CourseHero, Chegg).

Attendance

Attendance is not required, but it is *highly* encouraged. While lectures will mostly follow the textbook, I will provide additional explanation and context that will help you to understand the material.

Academic Integrity

The Undergraduate Honor Code pledge that each member of the university community agrees to abide by states:

"As a Hokie, I will conduct myself with honor and integrity at all times. I will not lie, cheat, or steal, nor will I accept the actions of those who do."

Students enrolled in this course are responsible for abiding by the Honor Code. A student who has doubts about how the Honor Code applies to any assignment is responsible for obtaining specific guidance from the course instructor before submitting the assignment for evaluation. Ignorance of the rules does not exclude any member of the University community from the requirements and expectations of the Honor Code.

Academic Accommodations

Virginia Tech welcomes students with disabilities into the University's educational programs. The University promotes efforts to provide equal access and a culture of inclusion without altering the essential elements of coursework. If you anticipate or experience academic barriers that may be due to disability, including but not limited to ADHD, chronic or temporary medical conditions, deaf or hard of hearing, learning disability, mental health, or vision impairment, please contact the Services for Students with Disabilities (SSD) office (540-231-3788, `ssd@vt.edu`, or visit `ssd.vt.edu`). If you have an SSD accommodation letter, please meet with me privately during office hours or by appointment as early in the semester as possible to deliver your letter and discuss your accommodations. You must give me reasonable notice to implement your accommodations, which is generally 5 business days and 10 business days for final exams.

Policy Changes

This course policy sheet is subject to change pending changes in the university policy. If the university policy changes (*e.g.*, we go all online), a new course policy sheet will be posted to Canvas, and it is your responsibility as a student to inform yourself of the changes made.