Instructor Information	**Name:** Jason LeGrow **Office:** McBryde 470 **Email:** `jlegrow@vt.edu`
Class Times	Monday, Wednesday, and Friday, 1:25 – 2:15pm
Class Location	Derring 3092
Office Hours	Tuesday 3:30 – 5:00pm, and other times by appointment.
Course Website	`canvas.vt.edu`
Prerequisites	Background in abstract algebra (at the level of Math 4124) or number theory (at the level of Math 4134) is required. Some programming may be required.
Textbook	No textbook is required. The following books may be useful references: Boneh, D. and Shoup, V. **A Graduate Course in Applied Cryptography**. Available online at `https://toc.cryptobook.us/` Hoffstein, J., Pipher, J., and Silverman, J. **An Introduction to Mathematical Cryptography**. Springer.
Course Objectives	We will study fundamental topics in public-key cryptography and their mathematical foundations. In particular, we will see problems from computational algebra and number theory, and how they can be used to construct key establishment protocols, public-key cryptosystems, and digital signatures.
Course Outline	Topics will be chosen from the following list: **Computational Problems in Cryptography:** Factoring, the discrete logarithm problem, quadratic residuosity, group actions arising in post-quantum cryptography. **Key Establishment:** Diffie-Hellman. **Public-Key Encryption:** Classical schemes: e.g., RSA, ElGamal, Goldwasser-Micali. Semantic security: e.g., Cramer-Shoup. **Proof Systems:** Interactive proof systems, proofs of knowledge, zero-knowledge proofs, zero-knowledge proofs of knowledge. **Digital Signatures:** RSA, Schnorr, group action-based schemes. **Provable Security:** Security models, security definitions. **Advanced Protocols:** Ring signatures, adaptor signatures, blind signatures.
Grading	Assignments will be worth 40% of your grade, one midsemester test will be worth 25% of your grade, and the final exam will be worth 35% of your grade. **Assignments.** There will be a number of assignments, each due on a **Tuesday at 11:59pm**. Your lowest assignment grade will be dropped. Late assignments will not be accepted. **Exams.** The test is tentatively scheduled for **Monday, February 24, in class**. The final exam is scheduled by the registrar's office; check the course schedule. A final numerical grade of 90, 80, 70, or 60 will guarantee a final letter grade of at least A-, B-, C-, or D-, respectively.

Collaboration

You are welcome—in fact, *encouraged*—to collaborate with current Math 5174 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 be based on the textbook or similar resources, 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. Students are strongly discouraged from misusing sites such as Chegg and CourseHero, as well as misusing ChatGPT and other Generative Artificial Intelligence. Students are strongly encouraged to consult their faculty members regarding the use of such outside materials as the misuse of these sources may constitute a violation of the Honor Code. Ignorance of the rules does not exclude any member of the University community from the requirements and expectations of the Honor Code.

The Virginia Tech honor code pledge for assignments is as follows:

"I have neither given nor received unauthorized assistance on this assignment."

The pledge is to be written out on all graded assignments at the university and signed by the student. The honor pledge represents both an expression of the students support of the honor code and a commitment to uphold the academic standards at Virginia Tech.

Academic Accommodations

Virginia Tech welcomes students with disabilities into the Universitys 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.