Modern Cryptography: Spring 2026

Overview

Modern Cryptography includes seemingly paradoxical notions such as communicating privately without a shared secret, proving things without leaking knowledge, and computing on encrypted data. In this challenging but rewarding course we will start from the basics of private and public key cryptography and go all the way up to advanced notions such as zero-knowledge proofs and secure computation.

The class will focus on rigorous proofs and require mathematical maturity.

Administrative

Instructors: Aditya Hegde (ahegde3 [AT] jhu [DOT] edu), Harry Eldridge (heldrid2 [AT] jhu [DOT] edu)

- Lectures: 3:00pm - 4:15pm, Tuesday and Thursday, Hodson 203

Grading: 15% Midterm 1, 25% Midterm 2, 30% Final, 25% Homework, 5% Class Participation

Homeworks: Submit via Canvas

Discussion Board: Canvas

TA: Shruthi Prusty (sprusty1 [AT] jhu [DOT] edu)

Course Website: https://adishegde.github.io/modern_crypto_sp26/

Lecture Notes, Slides, and Homeworks: Available on the course website

Office Hours

- Aditya Hegde: 4:00pm - 5:00pm, Wednesday, Malone 307
- Harry Eldridge: 11:00am - 12:00pm, Tuesday, Malone 307
- Shruthi Prusty: 1:00pm - 2:00pm, Thursday, Malone 216

Textbook

There is no required textbook. We suggest the wonderful free textbook *A Graduate Course in Applied Cryptography* (https://toc.cryptobook.us/) as a supplemental text.

Homeworks

Format

All homeworks submissions must be typeset (no handwritten submissions). We highly recommend writing in LaTeX (https://www.latex-project.org/) or Typst (https://typst.app/).

Collaboration

Collaboration on homeworks is allowed, though the final words used in the assignment must be your own. When collaborating with other students you are required to state at the beginning of the submission the names of the stuents you collaborated with.

AI

You are allowed to use AI to better understand the materials presented in class. All homework submissions must be your individual work, done without the aid of AI.

Late Policy

Homeworks are due at 11:59pm Eastern Time on the day listed as their due date. You have a total of 48 late hours for submitting homeworks. For example, you could submit homework 1 three hours late, homework 2 ten hours late, and homework 5 thirty-five hours late and receive no penalty. Homeworks submitted at any time past the hour count as consuming a late hour. For example, submitting a homework at 1:00am Eastern Time the day after it is due would consume two late hours. Homeworks submitted after all 48 late hours have been consumed will be worth 0.

For overwhelming obstacles (illness, family emergency, etc.) please reach out to the instructors or TA to request an extension.

Schedule

The syllabus below is tentative and dates and topics may change.

1/20: Introduction and Prerequisites

- Required reading: Pre-requisite lecture notes

(https://adishegde.github.io/modern_crypto_sp26/notes/prerequisite_notes.pdf)

1/22: Provable Security (1)

- HW1 assigned

1/27: Provable Security (2)

1/29: Provable Security (3)

- HW1 due, HW2 assigned

2/3: Provable Security (4)

2/5: Encryption (1)

- HW2 due, HW3 assigned

2/10: Encryption (2)

2/12: Encryption (3)

- HW3 due

2/17: Midterm 1

2/19: Foundations (1)

2/24: Foundations (2)

- HW4 assigned

2/26: Authentication (1)

3/3: Authentication (2)

- HW4 due, HW5 assigned

3/5: Zero-knowledge (1)

3/10: Zero-knowledge (2)

- HW5 due

3/12: Zero-knowledge (3)

3/17: Spring Break

3/19: Spring Break

3/23: Flex/Catch-up class

3/25: Flex/Catch-up class

3/31: Midterm 2

4/2: CCA Security (1)

4/7: CCA Security (2)

- HW6 assigned

4/9: Secure Computation (1)

4/14: Secure Computation (2)

- HW6 due

4/16: Flex/Advanced class

4/21: Flex/Advanced class

4/23: Review

5/5: Final Exam

Students with Disabilities - Accommodations and Accessibility

Johns Hopkins University is committed to providing welcoming, equitable, and accessible educational experiences for all students. If disability accommodations are needed for this course, students should request accommodations through Student Disability Services (SDS) as early as possible to provide time for effective communication and arrangements.

For further information about this process, please refer to the SDS Website or email SDS Homewood: studentdisabilityservices@jhu.edu.

Mental Health Statement

Many students struggle at times with stress and mental health concerns. Johns Hopkins University Mental Health Service has a range of services to support students with their mental health. Beyond clinical services, JHU also has many resources available to support overall student well-being.

For **24/7 behavioral health support**, The Johns Hopkins University Behavioral Health Crisis Support Team (BHCST) pairs experienced, compassionate crisis clinicians with specially trained public safety officers on every shift on and around the Homewood campus, seven days a week. The BHCST will provide immediate assistance to those who need it and link individuals in crisis to ongoing support services in the days and weeks that follow. BHCST can be reached directly at 410-516-9355 or by calling Public Safety, 410-516-4600 or 7777, and asking to be connected to a BHCST clinician.

If you have concerns about yourself or another student, please contact:

- For emergencies (threat to self or others): **Public Safety** 410-516-7777 or 911
- For 24/7 mental health support (mobile, access line and virtual): **BHCST** at 410-516-9355

- For **undergraduate students** who may benefit from Case Management services (1:1 support, coordination and connection to relevant campus resources): **Student Outreach & Support** at 410-516-7857 or studentoutreach@jhu.edu
- For **KSAS Graduate Students**: Renee Eastwood, Assistant Dean for Graduate and Postdoctoral Academic and Student Affairs
- For **WSE Graduate Students**: Megan Barrett, Assistant Dean for Engineering Student Affairs

Academic Integrity

The strength of the university depends on academic and personal integrity. In this course, you must be honest and truthful. Ethical violations include cheating on exams, plagiarism, reuse of assignments, improper use of the internet and electronic devices, unauthorized collaboration, alteration of graded assignments, forgery and falsification, lying, facilitating academic dishonesty, and unfair competition.

Report any violations you witness to the instructor. You can also contact:

- For undergraduates: the associate dean of student conduct (or designee) by calling the Office of the Dean of Student Life at 410-516-8208 or via email at studentconduct@jhu.edu
- For KSAS Graduate Students: rseitz5@jh.edu
- For WSE Graduate Students: christinekavanagh@jhu.edu

Inclusivity

The following statement was provided by the Homewood Council on Inclusive Excellence and is incorporated into all WSE course syllabi.

Johns Hopkins University is committed to creating a classroom environment that values the diversity of experiences and perspectives that each student brings. Everyone deserves to be treated with dignity and respect. Fostering an inclusive climate is important because research and experience show that students who interact with peers who are different from themselves learn new things and experience tangible educational outcomes. We invite you to help create a welcoming, vibrant and intellectually engaging classroom climate. Note that you should expect to be challenged intellectually by the instructor, the TAs, and your peers, and at times this may feel uncomfortable. Indeed, growth often requires being pushed beyond your comfort zone. However, at no time in this learning process should someone be singled out or treated unequally based on any aspect of their identity (visible or invisible).

If you ever have concerns in this course about harassment, discrimination, or any unequal treatment, or if you seek accommodations or resources, please reach out to your instructor or the TAs, who will take your communication seriously and seek mutually acceptable resolutions and accommodations. Reporting will never impact your course grade. You may also share concerns with the department chair, the Director of Undergraduate Studies [link to heads/DUS document], the WSE Associate Dean of Outreach and Belonging (Darlene Saporu, dsaporu@jhu.edu), the KSAS Assistant Dean for Diversity and Inclusion (Araceli Frias, afrias3@jhu.edu) or the Office of Institutional Equity (oie@jhu.edu).

In handling reports, people will protect your privacy as much as possible, but faculty and staff are required to officially report information for some cases (e.g., sexual harassment).