Math 110.376: The Mathematics of Cryptography and Cybersecurity
Course Syllabus

Instructor Information
Lauren Ross
Email: lblount2@jhu.edu
Office Hours: Online, by appointment

Course Description
The Mathematics of Cryptography and Cybersecurity is an introduction to modern cryptography with an emphasis on the mathematics behind the theory of public key cryptosystems, cybersecurity, and digital signature schemes. The course develops the mathematical tools needed for the construction and security analysis of diverse cryptosystems.

Other topics central to mathematical cryptography covered are: classical cryptographic constructions, such as Diffie-Hellmann key exchange, discrete logarithm-based cryptosystems, the RSA cryptosystem, and digital signatures.

Fundamental mathematical tools for cryptography studied include: primality testing, factorization algorithms, probability theory, information theory, and collision algorithms. A survey of important recent cryptographic innovations, such as elliptic curves, elliptic curve and pairing-based cryptography are included as well.

This course is an ideal introduction for mathematics and computer science students to the mathematical foundations of modern cryptography.

Learning Outcomes:
By the conclusion of this course, you are expected to have gained the ability to:

- Encrypt, decrypt using Caesar ciphers, Monoalphabetic Substitution ciphers, RSA, and Elliptic Curves.
- Apply elementary number theory to various cryptosystems and information sharing algorithms.
- Understand the strengths, weaknesses, and processes of a variety of public key cryptography methods.

Textbook

An Introduction to Mathematical Cryptography, by Hoffstein, Pipher, and Silverman, 2014 Edition

ISBN-13: 978-1441926746

Lectures

Prerecorded lectures will be posted for the week in Canvas. There will be live synchronous sessions each week through zoom, with dates posted in the course. During these live synchronous components, homework problems and exam review will take place. Links to the recordings of each live online session will be posted in Canvas. For more information regarding Zoom, please see the Zoom Student Quick Start Guide.

Homework

Homework is assigned for each week from the text. Work should be hand-written, scanned, and uploaded as an image or .pdf in Canvas. The lowest homework grade will be dropped.

Quizzes

There will be an online quiz at the end of each chapter. There are two attempts at this quiz and the higher of the two attempts counts for the grade.

Midterm & Final Exam

There will be one midterm exam a final exam. The exams will be released in Canvas and is to be completed individually, by hand, and submitted as an image or pdf by 11:59pm ET on the posted due dates. Follow all directions on the exam. Any official course resources, as well as student notes, may be used during the exam. No additional outside resources are permitted.

Discussion Forums

There will be six required discussion forums in the class. To receive full credit for each discussion forum, you must post an original discussion and at least one response to another discussion or to a response within your original post.

Project

The project gives you the opportunity to explore an area of cryptography that interests you. Your final project will consist of a 10–20-minute video explaining your topic as well as a topic or question for your classmates to discuss.

Collaboration

Collaboration on homework is allowed and encouraged. However, each individual must write up their solutions to the problems in their own words - copying from another individual's paper is prohibited. Homework is an essential part of learning the course material. Failing to give it proper attention will significantly harm your performance on the exams and your overall grade for the class.

Grading

Your final grade for the class will be given as a weighted average with the weights given as follows:

- Discussion Forums: 10%
- Homework: 20% (lowest grade dropped)
- Quizzes: 15%
- Midterm Exam: 20%
- Project: 15%
- Final: 20%

The letter grades are as follows based on your final weighted average:

A: 90-100
B: 80 - 89
C: 70 - 79
D: 55 - 69
F: < 55

Support

There are many sources of help and support if you are having difficulty with the class, material or anything else. These include:

- Office hours: Online, by appointment
- The Learning Den: https://academicsupport.jhu.edu/learning-den/
- Office of Academic Support: https://academicsupport.jhu.edu

Please do not feel shy about asking for help, or just checking that you understand something correctly.

Students with Disabilities

Students with documented disabilities or other special needs who require accommodation must register with the Office of Academic Advising. After that, remind the instructor of the specific needs at least one week prior to each exam; the instructor must be provided with the official letter stating all the needs from the Office of Academic Advising. (https://studentaffairs.jhu.edu/disabilities/)

Academic Integrity: Academic Misconduct Policy

All students are required to read, know, and comply with the Johns Hopkins University Krieger School of Arts and Sciences (KSAS) / Whiting School of Engineering (WSE) Procedures for Handling Allegations of Misconduct by Full-Time and Part-Time Graduate Students.

This policy prohibits academic misconduct, including but not limited to the following: cheating or facilitating cheating; plagiarism; reuse of assignments; unauthorized collaboration; alteration of graded assignments; and unfair competition. You may request a paper copy of this policy at this by contacting jhep@jhu.edu.

JHU Ethics Statement

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 may consult the associate dean of students and/or the chairman of the Ethics Board beforehand. Read the "Statement on Ethics" at the Ethics Board website for more information.