FoteiniBaldimtsi

CRYPTOGRAPHY

CS487/ CS587: Introduction to Cryptography

George Mason University, Computer Science, Fall 2023

Instructor: Prof. Foteini Baldimtsi (foteini@gmu.edu)
Office Hours: Wednesdays 2:30PM - 4:00PM, ENG 5333
Lectures: Wednesdays 4:30PM-7:10PM, Location: Krug Hall, Room 7
Class website: https://www.baldimtsi.com/teaching/crypto_f23
Teaching Assistant: Quan Minh Nguyen (qnguye31@gmu.edu), TBD

Course Description

The course will provide an introduction to modern cryptography. We will cover many practical topics, such as how to correctly use block ciphers and hash functions for the most common tasks: encryption and message authentication, the differences between public key cryptography and symmetric key cryptography, and a few ways to build public key encryption and signatures. We will learn about how to properly define security, and how to prove that our constructions are secure. In addition, and if time permits, we will also cover some recent topics in cryptography, such as the use of blockchains for crypto currencies (i.e. Bitcoin), zero-knowledge proofs of knowledge, and searching on encrypted databases.

Objectives: The main objectives are to convey the importance of *provable* security, to teach students how to use cryptographic tools in a way that is provably secure, to provide students with the ability to decide whether a protocol is secure, and to demonstrate the range of what can be achieved with provable security.

Course Outcomes: Students taking this class will be able to: (a) understand the security properties achieved by common cryptographic mechanisms such as encryption or digital signatures, (b) be familiar with a number of cryptographic protocols (toolbox) available to solve a variety of problems, (c) gain some experience on how cryptographic tools are used to secure modern systems such as cryptocurrencies.

Prerequisites: The prerequisites for the class are CS 310, CS 330 and STAT 344.

Although we will learn about practical topics in cryptography, students will need some level of mathematical maturity, i.e. being familiar with concepts in probability theory security definitions and proofs. This is not a course about computer hacking or computer security.

Logistics

Communications: We will use Piazza to communicate with you. If you have a question about the course you should: (a) Come to office hours, OR (b) Post on Piazza. We have already set up different tags for HW problems and lectures. Please don't use private posts/emails to ask technical questions. The rest of the class is probably also interested in your question, so make it public!

Lectures: The class will meet in person once a week on Wednesdays. I use an electronic whiteboard during lecture and all notes are uploaded on blackboard after class. I highly recommend asking questions during lecture and I will often ask questions and give short problems to solve in a group fashion during class.

Class Material: All class material (slides, notes, videos etc) will be posted on Blackboard.

Assignment Submission and Late Policy: We will have 6 sets of assigned homework problems (roughly bi-weekly). Assignments will be posted on **Gradescope** and solutions have to be submitted on Gradescope by Thursday 5:00pm. No credit will be given to late submissions. To be fair with everyone in class no exception will be made to the rule above. The lowest HW grade will be dropped. HWs will often include bonus problems.

Quizzes: We will have bi-weekly quizzes (roughly) that will take place at the beginning of the class, electronically on Blackboard. You need to have an electronic device with you in class (laptop, tablet, smartphone) with access to Blackboard. If you need special accommodations please contact the instructor in advance.

Graduate Students (CS 587): Graduate students will be given an extra HW problem to solve in most of the assignments. They will also have to solve an extra problem in both midterm and final and will have to independently study some additional material.

Text Book: Katz and Lindell. *Introduction to modern cryptography*, Third Edition. **(Required).**

Alternative readings (available online for free) listed below.

- A Graduate Course in Applied Cryptography, Dan Boneh, Victor Shoup
- Cryptography Primitives and Protocols, Aggelos Kiayias
- The Joy of Cryptography, Mike Rosulek
- A course on Cryptography, Rafael Pass & abhi shelat
- Cryptography, an introduction, Nigel Smart
- Introduction to Modern Cryptography, Mihir Bellare & Phil Rogaway

Grading Policy

- Assignments: 25% (6 assignments, lowest grade dropped)
- Quizzes: 10% (6-7 quizzes, lowest grade dropped)
- Midterm: 30% or 35%
- Final: 30% or 35% (The highest greade between midterm/final will count for 35% and the lowest for 30%).

Class Schedule (Tentative):

Schedule Fall 2023

Honor code: All students must adhere to the GMU Honor Code. You can discuss lecture material with other students in class but you have to work on the assignments alone. More specifically: (1) You must work on the homework problems and write your solutions completely on your own, without looking at other people's write-ups. (2) You are welcome to use any textbooks, online sources, blogs, research papers, Wikipedia, etc to better understand a notion covered in class or in a homework question. If you do so you have to properly cited it in any submitted work. Failure to do this is plagiarism and is serious violation of the GMU Honor Code and basic scientific ethics, and will not be tolerated. Note that it is not OK to search for solutions to HW problems online.

ChatGPT or other Generative-AI models may **not** be used in this course as an assistant in projects and homework assignments unless otherwise specifically stated by the instructor.

Disability Accommodations: Disability Services at George Mason University is committed to providing equitable access to learning opportunities for all students by upholding the laws that ensure equal treatment of people with disabilities. If you are seeking accommodations for this class, please first visit http://ds.gmu.edu/ for detailed information about the Disability Services registration process. Then please discuss your approved accommodations with me. Disability Services is located in Student Union Building I (SUB I), Suite 2500. Email:ods@gmu.edu | Phone: (703) 993-2474

Misconduct Report: As a faculty member, I am designated as a "Non-Confidential Employee," and must report all disclosures of sexual assault, sexual harassment, interpersonal violence, stalking, sexual exploitation, complicity, and retaliation to Mason's Title IX Coordinator per University Policy 1202. If you wish to speak with someone confidentially, please contact one of Mason's confidential resources, such as Student Support and Advocacy Center (SSAC) at 703-380-1434 or Counseling and Psychological Services (CAPS) at 703-993-2380. You may also seek assistance or support measures from Mason's Title IX Coordinator by calling 703-993-8730, or emailing titleix@gmu.edu.