CS499: Cryptography

George Mason University, Computer Science, Fall 2018

Instructor: Prof. Foteini Baldimtsi (foteini@gmu.edu)
Office Hours: Mondays 2:00PM-4:00PM, Engineering 5333
Lectures: Tuesdays 4:30PM-7:10PM, Location: Blueridge Hall 129

Course Summary

The course will provide an introduction to modern cryptography. We will cover many block ciphers and hash functions for the most common tasks: encryption and messa several recent topics in cryptography, such as the use of blockchains for crypto curre knowledge, and searching encrypted databases.

Objectives
The main objectives are to convey the importance of provable security, to teach stud is provably secure, to provide students with the ability to decide whether a protocol is can be achieved with provable security.

Course Outcomes: Students taking this class will be able to: (a) understand the se cryptographic mechanisms such as encryption or digital signatures, (b) be familiar w available to solve a variety of problems (message integrity, privacy, authentication, p on how cryptographic tools are used to secure modern systems such as cryptocurre

Prerequisites: There is not hard prerequisite for this course but being familiar with material taught on CS 330, CS483 and MATH 125 is . 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 (computation of expectation, conditional probability etc) and complexity theory (Turing machines, NP-completeness etc) would be helpful for an easier understanding of formal security definitions and proofs. This is not a course about computer hacking or computer security.

Required Materials

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

There will also be additional readings for each class (available online for free) listed below.

Grading

Midterm: 25%
Assignments: 35% (5 assignments, bonus points offered in all of them)
Final: 30%
Quizzes: 10% (6 quizzes, lower grade dropped)

Assignment Submission and Late Policy: Homework questions will be posted on Blackboard and solutions have to be submitted through Blackboard (no credit will be given otherwise). Assignments received within 24 hours after the deadline lose 20%, within 48 hours 40% and after that no credit will be given. To be fair with everyone in class no exception will be made to the rule above.

Grading Scale:

A+ >97% A >92% A- >90%
B+ >87% B >82% B- >80%
C+ >77% C >72% C- >70%

Graduate Students (CS 595): Graduate students will be given an extra HW problem to solve in each of the five assignments. They will also have to solve an extra question in both midterm and final.

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!

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.

Class Schedule (Tentative):

Lecture	Topics	Suggested Readings	HWS/ Quizzes
08/28 Lec. 1	Introduction Logistics Notions of Encryption		HW1 out
09/04 Lec. 2	Encryption and Indistinguishability		Quiz 1
09/11 Lec. 3	Pseudorandom Generators and Pseudorandom Functions		Quiz 2
09/18 Lec. 4	Key Agreement Public Key Encryption		HW1 in HW2 out
09/25 Lec. 5	Message Authentication Codes Hash Functions		Quiz 3
10/02 Lec. 6	Signatures		HW2 in HW3 out
10/09	No class due to Fall Break		
10/16 Lec. 7	Review		HW3 in
10/23	Midterm		
10/30 Lec. 8	Commitments and Zero Knowledge Proofs		HW4 out
11/6 Lec. 9	Secret Sharing, Multiparty Computation		Quiz 4
11/13 Lec 10	Other flavors of Encryption (Searchable..)		HW4 in HW5 out
11/20 Lec 11	Bitcoin and Cryptocurrencies		Quiz 5
11/27 Lec 12	TBA		HW5 in
12/04 Lec 13	Review		Quiz 6
12/11	Final		