Syllabus: CSC 409/509 Cryptography

Day time Room

Instructor: Alessandra Scafuro (webpage)

E-Mail: ascafur@ncsu.edu

Office Hours: Monday 3-4 PM

Location of Office Hours: EB2 3264

Course Description

Cryptography is the study of mathematical techniques for securing digital information, systems and distributed computation against adversarial attacks.

In this class you will learn the concepts and the algorithms behind the most used cryptographic protocols: you will learn how to formally define security properties and how to formally prove/disprove that a cryptographic protocol achieves a certain security property.
You will also discover that cryptography has a much broader range of applications. It solves absolutely paradoxical problems such as proving knowledge of a secret without ever revealing the secret (zero-knowledge proof), or computing the output of a function without ever knowing the input of the function (secure computation).
Finally, we will look closely at one of the recent popular application of cryptography: the blockchain technology.

Objectives

By the end of the course, students should be able to:

- State and motivate the formal definition of the most common cryptographic goals (such as data confidentiality and integrity).
- Formally prove/disprove security of a cryptographic scheme (such as encryption scheme, digital signatures).
- Identify the cryptographic tools needed in real world protocols (such as Bitcoin).
- State and motivate more advanced cryptographic goals (such as zero-knowledge, secure two-party computation).

Prerequisites

There are no hard requirements, but familiarity with concepts in probability theory (such as computation of expectation, conditional probability) and complexity theory (such as Turing machine, NP-completeness) would be helpful for an easier understanding of formal security definitions and proofs.

Required Materials

Students **must** read the material indicated by the instructor upon each class. The readings are mostly based on the following book.
Introduction to Modern Cryptography - Jonathan Katz, Yehuda Lindell (**electronic version is free** for ncsu students)

Topics

Date	Sections	Topics
Week 1 - 3	Section 1: Computational Security and Pseudorandomness	One-time pad, Computational Security, Indistinguishability Pseudo-random generators (PRGs)
Week 3 - 4	Symmetric Key Encryption	Pseudo-random functions (PRFs) PRF from PRG CPA-security Pseudo-random permutation (PRP) PRP from PRF Feistel Transform. PRP in practice: Block ciphers and Modes of Operation
Week 5	Section 2: Public key Encryption	Number Theory for Crypto
Week 6 - 9		Public Key Cryptography RSA trapdoor function, Textbook RSA El-Gamal encryption, Trapdoor OWF
Week 9 - 10	Section 3. Data Integrity and Authenticity	Message Authentication Code Hash Functions
Week 11		Digital Signatures
Week 12-13	Section 4: Advanced Cryptographic Protocols	Consensus Blockchain technology
Week 14		Zero-Knowledge, Sigma-Protocols
Week 15		Commitment Schemes
Week 16		Secure 2PC - Garbled Circuits Oblivious Transfer

Homeworks Due Dates (Tentative)

Due Date	Homework	Topics
Sep 11	Homework 1	Section 1
Oct 2	Homework 2	Section 1
Oct 22	Homework 3	Section 2
Nov 5	Homework 4	Section 3
Dec 2	Homework 5	Section 4

Late Policy & Attendance

No late assignments will be accepted.
Attendance is required.

Additional Requirements for Students Enrolled at 5XX Level

Each student enrolled in CSC 591 will be required to present one topic in depth in an oral exposition.

Grading Information

Graded Elements	**Description**	**Weight for CSC 495**	**Weight for CSC 591**
Homeworks	Students will be given problem sets at the end of each section.	20%	20%
Test 1	Intermediate Evaluation	30%	30%
Test 2	Intermediate Evaluation	30%	30%
Final Exam	Final exam	20%	20%
Oral Exposition	CSC 591 students will present a specific topic in depth.	NA	[0,-5]%

The following grade scale will be used:

(∞, 98] A+, (98, 92] A, (92, 90] A-
(90, 86] B+, (86, 80] B, (80, 75] B-
(75, 70] C+, (70, 68] C, (68, 65] C-
(65, 63] D+ (63, 60] D, (60, 55] D-, (55, 0] F

Students are expected to conduct themselves in a respectful and professional manner at all times. Grades will be adjusted if students do not handle themselves in a respectful and professional manner with all members of the teaching staff and with others in the class, including message board posts.

Communication Policy

Students can communicate with the TAs and the instructor by posting on Moodle, or by email. Answers should be expected only during weekdays.

Academic Integrity

All students are expected to maintain traditional standards of academic integrity by giving proper credit for all work. All suspected cases of academic dishonesty will be aggressively pursued. Students are required to comply

with the university policy on academic integrity found in the Code of Student Conduct found at http://policies.ncsu.edu/policy/pol-11-35-01

Working together on some aspects of the class is required. Pairings and teams will be assigned (with your input) for some assignments and for presentations. The requirements of enforcing academic integrity and achieving instructional effectiveness poses a dilemma to instructors as well as students. Academic integrity in the classroom translates to professional integrity in the workplace. Moreover, awarding similar grades to students who have maintained academic integrity and to students who have cheated results is not only unfair but also reduces the value of degree in the workplace. It is thus to the interest of every student as well as the responsibility of the instructor to see that this is not allowed to happen. On the other hand, discussion of material presented in class, and homework assignments, can provide good opportunities for learning, and is encouraged among students. The key thing to keep in mind is that collaboration is different from collusion. It is acceptable and indeed highly desirable for students to talk over a problem and work together in solving the problem, but not okay for one student to use the fruits of another's work. The "Clean Board Policy" may make this more concrete: when you work together with other students, do so at a whiteboard (or the equivalent) on which you collaborate. Once your discussion is over, wipe the board clean. Each student must walk away with the results of the discussion only in his/her head; do not copy anything down. When you are working on your homeworks and project, do so alone (or within your group if it is a group task) according to your own understanding.

Accommodations for Disabilities

Reasonable accommodations will be made for students with verifiable disabilities. In order to take advantage of available accommodations, students must register with the Disability Resource Office at Suite 304, University College Commons, Campus Box 7509, 919-515-7653. For more information on NC State's policy on working with students with disabilities, please see the Academic Accommodations for Students with Disabilities Regulation (REG02.20.01) (https://policies.ncsu.edu/regulation/reg-02-20-01/).

Policies on Incomplete Grades

If an extended deadline is not authorized by the Graduate School, an unfinished incomplete grade will automatically change to an F after either (a) the end of the next regular semester in which the student is enrolled (not including summer sessions), or (b) by the end of 12 months if the student is not enrolled, whichever is shorter. Incompletes that change to F will count as an attempted course on transcripts. The burden of fulfilling an incomplete grade is the responsibility of the student. The university policy on incomplete grades is located at http://policies.ncsu.edu/regulation/reg-02-50-03. Additional information relative to incomplete grades for graduate students can be found in the Graduate Administrative Handbook in Section 3.18.F at http://www.ncsu.edu/grad/handbook/index.php

---

Academic Integrity

NC State University provides equality of opportunity in education and employment for all students and employees. Accordingly, NC State affirms its commitment to maintain a work environment for all employees and an academic environment for all students that is free from all forms of discrimination. Discrimination based on race, color, religion, creed, sex, national origin, age, disability, veteran status, or sexual orientation is a violation of state and federal law and/or NC State University policy and will not be tolerated. Harassment of any person (either in the

form of quid pro quo or creation of a hostile environment) based on race, color, religion, creed, sex, national origin, age, disability, veteran status, or sexual orientation also is a violation of state and federal law and/or NC State University policy and will not be tolerated. Retaliation against any person who complains about discrimination is also prohibited. NC State's policies and regulations covering discrimination, harassment, and retaliation may be accessed at http://policies.ncsu.edu/policy/pol-04-25-05 or http://www.ncsu.edu/equal_op/. Any person who feels that he or she has been the subject of prohibited discrimination, harassment, or retaliation should contact the Office for Equal Opportunity (OEO) at 919-515-3148.