The University of North Carolina at Greensboro
CSC 485/685: Modern Cryptography
Prof. Stephen R. Tate

Handout 1
August 15, 2023

CSC 485/685 Class Information and Syllabus

Instructor: Stephen R. Tate (Steve)
Lectures: Tues/Thurs 5:30-6:45 (Petty 223)
Office Hours: Tues/Thurs 3:30-5:00 (or by appointment), in-person or virtual – see below
Office: Petty 157
E-mail: `srtate@uncg.edu` – I answer most emails within one business day – do not expect responses evenings or weekends

Class Web Page: `https://home.uncg.edu/cmp/faculty/srtate/485.f23/`

Catalog Description: Theory and practice of cryptography, emphasizing formal models and security reasoning. Primitives covered include private and public-key encryption, message authentication codes, hash functions, digital signatures, secret sharing, and zero-knowledge proofs.

Prerequisites: The catalog lists prerequisites for undergraduates as “a grade of C or better in CSC 481, or permission of instructor” (for graduate students, replace 481 with 681). However, while familiarity with security concepts and real-world scenarios from CSC 481 (Principles of Computer Security) helps a great deal in giving context for the use and practical applications of cryptography, it is not strictly necessary for understanding the material in this class. If you have successfully completed a number of college-level math classes (at least CSC 250 and CSC 350 and some calculus) and have experience with analyzing algorithms (and in particular, time complexity) at the level of CSC 330, then you probably have the background you need. Students in this situation will be granted “permission of instructor” to enroll in the class and should contact Dr. Tate.

Longer Description: This course covers the basics of the theory and practice of cryptography, which provides some of the most powerful tools available for building secure computing and communication systems. This course emphasizes formal models, rigorous thinking, and reasoning about security. As the textbook states, the focus is in “the logic of composing different building blocks together in provably secure ways.” Composing building blocks is exactly what a system designer or developer does when they incorporate cryptographic capabilities into a system, and being able to reason about the security of this use is vital to developing secure systems. Note that this course is heavy on reasoning about, and writing formal proofs about, properties that are necessarily very abstract. To prove security, you are writing formal proofs about the non-existence of attacks – it's not just matter of saying "I can't think of an attack on this system" – you must prove that such an attack doesn't exist. Most undergraduates (and many graduate students!) are not very comfortable with writing formal proofs. This is understood, and we will take things slow with lots of explanation and in-class practice. However, you must be able to write basic proofs to master this material and pass the class!

Student Learning Outcomes: Upon successful completion of this course students should be able to

1. Explain formal security models for encryption, hash functions, message authentication, and digital signatures;
2. Describe basic algorithms for fundamental cryptographic operations;
3. Select appropriate cryptographic techniques for meeting stated security goals;
4. Create proofs of security or insecurity for cryptographic constructions;
5. Analyze security parameters for cryptographic applications to meet security goals;
6. (Graduate Students Only) Evaluate research in cryptography.

Textbook and Readings: The required textbook is the following, which is freely available online at https://joyofcryptography.com:

Mike Rosulek, *The Joy of Cryptography* (Jan 3, 2021 edition)

Additional readings may be required, and material be provided to students as needed.

Topics: This is the first time this class is being taught using this textbook, so the schedule is fairly tentative. The book is designed so that it can be covered in a single undergraduate-level class, and that is the intent here. Several of the "starred sections" from the textbook will be omitted. The topics to be covered are shown below, with an estimate of how long each topic should take. The schedule on the class web-site will be updated regularly to reflect the actual schedule.

- Class Overview and Start Background Review [1 day]
- Chapter 0: Review of Concepts & Notation [1 day]
- Chapter 1: One-Time Pad [1 day]
- Chapter 2: The Basics of Provable Security [2 days]
- Chapter 3: Secret Sharing [2 days]
- Chapter 4: Basing Cryptography on Intractable Computations [1+ days]

- Chapter 5: Pseudorandom Generators [1 day] (excluding section 5.5)
- Chapter 6: Pseudorandom Functions & Block Ciphers [2 days] (starred material included if time allows)
- Chapter 7: Security against Chosen Plaintext Attacks [1 day]
- Chapter 8: Block Cipher Modes of Operation [2 days]
- Chapter 9: Chosen Ciphertext Attacks [1+ days] (excluding section 9.4)
- Chapter 10: Message Authentication Codes [2 days] (including section 10.2)
- Chapter 11: Hash Functions [1 day]
- Chapter 12: Authenticated Encryption and AEAD [1 day]
- Chapter 13: RSA and Digital Signatures [2 days]
- Chapter 14: Diffie-Hellman Key Agreement [1 day]
- Chapter 15: Public-Key Encryption [1 day]

Teaching Methods and Assignments: This class will meet for two 75-minute periods per week, and class meetings will consist of a combination of lecture/presentation, discussion, and in-class exercises. Students must to come to class prepared, having done all required readings, and are expected to participate in in-class activities. There is currently no plan to use powerpoint or any other kind of slides – problems solved in class (including proofs) will be done on the board, and students are expected to take notes. You may share your notes with others in this class, but I will not provide notes. I will follow the textbook closely, and if I cover topics outside the textbook I will always provide written material.

Before we begin each topic, students will be given several basic “practice problems” for each topic to work on while reading and studying. After we wrap up each topic, these will be worked in class with students being called on to provide solutions – so be prepared! These will not be graded unless it becomes clear that students are not doing the practice problems. As additional incentive, the practice problems will be very similar to the problems you will see on exams.

Graded work will consist of the following:

Assignments: Students will be given 6 written assignments over the course of the semester (approximately every two weeks, adjusted to exclude exam weeks), consisting of problems that delve deeper into the material than the practice problems. Assignments will include reasoning using formal security models, simulating or programming various algorithms, selecting appropriate techniques for providing security in various scenarios, and a significant amount of analysis and writing formal proofs. All work must be submitted in Canvas as PDF documents. These documents can be either electronically prepared (LaTeX and Overleaf are highly recommended) or neatly handwritten and scanned. If you must use a phone camera rather than a scanner, you should use a “scan to PDF” app to produce a proper and readable PDF document with standard letter paper size.

Exams: There will be two mid-term exams and one final exam, which will assess student’s mastery of learning outcomes 1-5 in an exam setting. Tentative exam dates are on the class website schedule. Most problems will be similar to practice problems, with one or two more challenging problems patterned after the written assignments. The final exam will be at the standard university-scheduled time, which is *Tuesday, December 5, 7:00pm–10:00pm*.

Graduate Students: Graduate students (and honors students completing a contract honors requirement with this class) will be given a handout on security research practices and standards, and sample research papers related to various aspects of cryptography to read and critique during the first 2/3 of the semester. For the final 1/3 of the semester, graduate students will select a topic from the research literature according their interests, locate appropriate references, and write a thorough research summary and critique. This addresses the graduate student learning outcome 6.

Evaluation and Grading: Each student work product will be graded, and the student's final grade will be determined by assigning each category of work a weighted score as shown below. Each student's current average, weighted using just the categories with graded work, is always available in Canvas. This grade will also be reported in Genie on September 22 as the student's midterm grade.

For undergraduates:

Category	
Assignments	50%
Mid-term Exam 1	15%
Mid-term Exam 2	15%
Final Exam	20%

Letter Grade Assignment				
	[87.5 , 89.5) = B+	[77.5 , 79.5) = C+	[67.5 , 69.5) = D+	[0 , 59.5) = F
[91.5 , ∞) = A	[81.5 , 87.5) = B	[71.5 , 77.5) = C	[61.5 , 67.5) = D	
[89.5 , 91.5) = A-	[79.5 , 81.5) = B-	[69.5 , 71.5) = C-	[59.5 , 61.5) = D-	

For graduate students:

Category	
Assignments	45%
Mid-term Exam 1	13.5%
Mid-term Exam 2	13.5%
Final Exam	18%
Research Project	10%

Letter Grade Assignment			
	[87.5 , 89.5) = B+	[77.5 , 79.5) = C+	[0 , 71.5) = F
[91.5 , ∞) = A	[81.5 , 87.5) = B	[71.5 , 77.5) = C	
[89.5 , 91.5) = A-	[79.5 , 81.5) = B-		

Note that Canvas uses the same letter grade assignment for undergraduate and graduate students, even though there are no passing grades below a C for graduate students. Any graduate student with a C- or below in Canvas will receive an F in the class.

Note that sanctions for violations of academic integrity or disruptive/unprofessional behavior apply to the overall grade and do not follow this percentage breakdown.

Academic Integrity: Students are expected to be familiar with and abide by the UNCG Academic Integrity Policy, which is online at `https://academicintegrity.uncg.edu/`.

Assignments in this class are for individual work, unless explicitly stated otherwise. General concepts and material covered in the class may be discussed with other students or in study groups, but specific assigned problems should not be discussed and all submitted work should be entirely your own. If you use external references (including web sites, books, etc.) in preparing your solutions, you should clearly mark the part(s) of your solution influenced by these references and provide clear citations to the source of information you are using. Sharing your own work is a serious violation of academic integrity, and if homework is copied then *both* the person who actually did the work and the person who copied it will be punished. Any incidents of academic dishonesty will be handled strictly, resulting in either a zero on the assignment or an F in the class, depending on the severity of the incident, and incidents will be reported to the UNCG Office of Student Rights and Responsibilities.

Attendance Policy: Attendance will not be taken in class, but is expected. All students are responsible for everything done or said in class (this can include changes in assignments, due dates, etc.). Note that this is a very interactive class, with regular in-class activities, so it is highly unlikely that a student who regularly misses classes will be successful in the course. If attendance becomes a problem, then in-class exercises may be collected and included as part of the assignment portion of the grade.

The university allows for a limited number of excused absences for religious observances. Students who plan to take such an absence should notify the instructor at least two weeks in advance so that accommodations can be made (see the late work policy below). It is the student's responsibility to obtain notes from another student if they miss class. Remote attendance or recordings will not be available.

Late Policy and Makeup Exams: Assignments are due at midnight on the due date, and the late submission cut-off is at 5:30 (i.e., before class) one week after the due date. Late assignments will receive a 25% late penalty. Solutions will be discussed in class on the late submission cut-off date, and no assignment can be accepted from any student, for any reason, after the cut-off. Students with planned absences, whether for university events, religious observance, or other reasons, are expected to make arrangements with the instructor to turn in assignments or take exams before the scheduled date of the assignment or test.

Exam/test dates will be announced at least two weeks in advance, and an exam may be made up only if it was missed due to an extreme emergency and arrangements are made before the exam date. Exams may not be taken early or late due to personal travel plans.

In-class Behavior: When you are in class you should be focused on the class, and you should act in a professional and mature manner. During class there should be no eating, drinking, e-cigarettes, cellphone use, non-class related laptop use, or anything else that does not pertain to the class activities. Any distracting items may be confiscated at the discretion of the instructor. Significant violations or disruptive behavior will result in points subtracted from a student's final grade, and possible reporting to the UNCG Office of Student Rights and Responsibilities.

ADA Statement: UNCG seeks to comply fully with the Americans with Disabilities Act (ADA). Students requesting accommodations based on a disability must be registered with the Office of Accessibility Resources and Services located in 215 Elliott University Center: (336) 334-5440 (or on the web at `https://oars.uncg.edu`).

COVID-19 and Communicable Disease: We have been living with COVID for over 3 years now, and at this point it's "just another communicable disease," albeit one with a nasty combination of being highly contagious and very dangerous for vulnerable people (people are still dying every day). As far as this class is concerned, COVID and any other communicable disease should be treated with the following rule: be considerate of others. If you are sick, isolate until you are no longer contagious. If you must be around others and have recently been contagious, take measures to limit risks to others (maintain distance, wear a mask, etc.). The attendance policy above has information about what to do if you must miss class due to illness.

Health and Wellness: Health and well-being impact learning and academic success. Throughout your time in the university, you may experience a range of concerns that can cause barriers to your academic success. These might include illnesses, strained relationships, anxiety, high levels of stress, alcohol or drug problems, feeling down, or loss of motivation. Student Health Services and the Counseling Center can help with these or other issues you may experience. You can learn about the free, confidential mental health services available on campus by calling 336-334-5874, visiting the website at `https://shs.uncg.edu/` or visiting the Anna M. Gove Student Health Center at 107 Gray Drive.

For undergraduate or graduate students in recovery from alcohol and other drug addiction, the Spartan Recovery Program (SRP) offers recovery support services. You can learn more about recovery and recovery support services by visiting `https://shs.uncg.edu/srp` or reaching out to `recovery@uncg.edu`

Elasticity Statement: It is the intention of the instructor that this syllabus and course calendar will be followed as outlined; however, as the need arises there may be adjustments to the syllabus and calendar. In such cases, the instructor will notify students in class and via e-mail with an updated syllabus and calendar within a reasonable timeframe to allow students to adjust as needed.