The University of North Carolina at Greensboro
CSC 495/680: Modern Cryptography
Prof. Stephen R. Tate

Handout 1
January 14, 2019

CSC 495/680 Class Information and Syllabus

Instructor: Stephen R. Tate (Steve)
Lectures: Mon/Wed 5:30-6:45, Petty 007
Office: Petty 166
Office Hours: Mon/Wed 3:30-5:00, or by appointment
Phone: 336-256-1033
E-mail: srtate@uncg.edu

Class Web Page: http://www.uncg.edu/cmp/faculty/srtate/495/

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: Grade of C or better in CSC 581, or permission of instructor.

Longer Description: This course is a second-semester security course, following the first-semester CSC 581 (Principles of Computer Security) and focusing on the theory and practice of cryptography, one of the most powerful sets of tools available for building secure computing and communication systems. This course emphasizes formal models, rigorous thinking, and reasoning about security. Cryptographic primitives covered include private and public-key encryption, message authentication codes, hash functions, digital signatures, secret sharing, and zero-knowledge proofs.

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) Evaluate research in cryptography.

Textbook and Readings: The required textbook is

> Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition*. Chapman and Hall/CRC, 2014. ISBN-13 978-1466570269.

Additional readings may be assigned during the semester. If additional readings are assigned, they will either be freely available or copies will be provided for students.

Topics: Since Spring 2019 is the first semester this class is being offered, the schedule is not completely determined. 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 Intro to Cryptography [1 day]
Principles of Modern Cryptography [1 day]
Review of bitwise operations and probability theory [1 day]
Perfectly-secret encryption (one-time pad) [1 day]
Private-key encryption [4 days]
Message authentication codes [3 days]
Hash functions and applications [2 days]
Constructions of symmetric-key primitives [2 days]
Number theory and cryptographic hardness assumptions [3 days]
Key management and public-key revolution [1 day]
Public-key encryption [3 days]
Digital signature schemes [2 days]
Secret sharing and threshold cryptography [1 day]
Zero-knowledge proofs [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 "teach from slides" – problems solved in class (including proofs) will be done on the board, and students are expected to take notes. Graded work will consist of the following.

Assignments: For practice and to demonstrate abilities, students will be given 5-6 written assignments over the course of the semester (approximately every two weeks, adjusted to exclude exam weeks). 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.

Exams: There will be one mid-term exam and one final exam, which will assess student's mastery of learning outcomes 1-5 in an exam setting. Problems will be similar to written homework problems, but will be somewhat simplified from the homework assignments, due to time limitations of testing. The final exam will be at the standard university-scheduled time, which is *Friday, May 3, 7:00pm–10:00pm*.

Graduate Students: Graduate students will be given a handout on security research practices and standards, and sample research papers 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 according to the following distribution:

Undergraduates	
Assignments	65%
Mid-term Exam	15%
Final Exam	20%

Graduate Students	
Assignments	55%
Mid-term Exam	15%
Final Exam	20%
Research Readings/Project	10%

Academic Integrity: Students are expected to be familiar with and abide by the UNCG Academic Integrity Policy, which is online at `http://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: This is a small and highly-interactive class, and while attendance will not be taken it is unlikely that you can succeed in this class without regular attendance. Students are responsible for knowing everything done or said in class (this can include changes in assignments, due dates, etc.). If attendance becomes a problem, then the instructor may change this policy by either assigning points to attendance or giving graded in-class work or quizzes.

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.

Late Policy and Makeup Exams: Assignments are due at the beginning of class on the due date, and may be turned in up to 7 calendar days late with a 25% late penalty. Students with planned absences, whether for university events, religious observance, or other reason, are expected to make arrangements with the instructor to turn in assignments or take exams before the scheduled date of the assignment or test. No assignment will be accepted more than 7 calendar days after the original due date!

Exam/test dates will be announced at least two weeks in advance, and may be made up only if it was missed due to an extreme emergency and arrangements are made before the exam date. Exams (including the final) 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, or anything else that does not pertain to the class activities. Any distracting items may be confiscated at the discretion of the instructor.

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 `http://oars.uncg.edu`).

University Closings: If university facilities are closed due to flu outbreak or other emergencies, it does not mean that classes are canceled. In such an event, please check the class web page and Canvas site for information about if and how the class will proceed.

Commercial note-taking services: Selling class notes for commercial gain or purchasing such class notes in this or any other course at UNCG is a violation of the University's Copyright Policy and of the Student Code of Conduct. Sharing notes for studying purposes, or borrowing notes to make up for absences, without commercial gain, are not violations.