CSC 580 Class Information and Syllabus

Instructor: Stephen R. Tate (Steve)
Lectures: Tues/Thurs 2:00–3:15, Petty 227
Office: Petty 166
Office Hours: Tues/Thurs 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/580/`

Catalog Description (from the current catalog – being rewritten, and included here just for reference): Modern development of cryptography and secure encryption protocols. Program security and viruses. Operating system protection. Network and distributed system security. Database security. Administering security.

Prerequisites: Grades of at least C (2.0) in CSC 330 and CSC 350.

Student Learning Outcomes: Upon successful completion, students will be able to

- describe basic cryptographic functionality, including symmetric ciphers, public key encryption, digital signatures, hash functions, and related concepts;
- describe how basic cryptographic building blocks are combined to meet high-level security goals in protocols like SSL and IPsec;
- identify specific security technologies that can improve aspects of a system design;
- justify the use of particular technologies, settings, and parameters to meet specified security goals;
- evaluate the security of systems that use cryptography and secure communication techniques;
- discuss how security and privacy issues can impact system design;
- (Graduate students) independently explore research-level computer security and cryptography topics.

Textbook: William Stallings. *Cryptography and Network Security: Principles and Practice (7th Edition)*. Pearson/Prentice Hall, Upper Saddle River, NJ, 2017.

Other Reading: Some topics will involve reading supplemental materials, including instructor-written handouts and published materials. These materials will be handed out as printed material, or will be available electronically from the class web page.

Class Structure and Assignments: The primary method of instruction will be two 75-minute meetings per week that will consist of regular quizzes, lecture, discussion, and problem-solving sessions. The class structure is described below.

Ungraded Homework: On most weeks, students will be given approximately 3 written (non-programming) homework problems on Thursday. These problems will be representative of the kinds of written problems you would traditionally see on an exam — the first time you see the problem it might take some time and effort to figure out how to solve the problem, but once you have mastered the material and practiced you should be able to solve similar problems in around 10 minutes. These should be solved before the following Tuesday, when solutions will be reviewed and discussed. These problems are not graded, but are not optional! If you do not *work out* solutions yourself (and study and practice), then it is unlikely that you will be able to solve the quiz problems, which *do* count for a significant part of your grade.

Quizzes: One week after each set of written problems are assigned, class will begin with a quiz in which students will be given one problem similar to the ones assigned the previous week as homework problems. A typical problem will be designed to be solvable in 10 minutes, and students will be given 15 minutes, so time should not be an issue. While these problems are based on the homework problems, they will not be identical. If you *understand* the solutions to the homework problems and have *practice* solving similar problems, then you shouldn't have any problems with the quizzes. However, if you do not work out solutions to the homework on your own, thinking you can rely on the in-class solution discussion (or other solutions you locate when studying), then you probably will not do well. There will be approximately 10 quizzes, and your two lowest grades will be dropped. There will be no quizzes given at other times for any reason (make-up or in-advance), and if you miss class on a particular day that will need to be one of your dropped scores.

Graded Homework: Throughout the semester there will be 3–4 graded homework assignments. These will consist of a few selected problems that go deeper than can be done with problems that are designed as 10 minute quiz problems.

Guided Research Project: Throughout the semester, we will use cloud storage security as a concrete example of various security and privacy topics. This will be focused around a discussion of research in computer science and security, and students will work in teams of 3–4 people to complete a research project related to the security of cloud storage. As an option for the Spring 2018 semester, we are doing a trial of ***collaborative projects*** between CSC 580 (Cryptography and Security in Computing) and ISM 324 (Secure Networked Systems), with a topic related to cloud storage security. Students in CSC 580 who do not opt for a collaborative project can complete a pure ***technical project*** in teams of just CSC 580 students. We will

discuss this project and the collaborative team approach during a combined meeting with the ISM 324 class on Tuesday, January 16.

Final Exam: There will be a traditional final exam, designed around all of the homework problems that are assigned throughout the semester. The final exam will be held at the university-scheduled day and time: ***Thursday, May 3, 3:30pm – 6:30pm***.

Graduate Students – Independent Research: Graduate students will take the research component one step further, by independently studying a second research topic in addition to the guided research in cloud storage that all students will pursue. In mid-March, Graduate students will select a topic in consultation with the instructor, based on their own interests, identify appropriate research materials, research the topic, and submit a final paper that surveys current research related to that topic. The final paper is due at the time of the final exam (May 3).

Evaluation and Grading: Final grades will be calculated based on the following weighting.

Undergraduates	
Graded Homework	15%
Guided Research Project	20%
Quizzes	40%
Final Exam	25%

Graduate students	
Graded Homework	15%
Guided Research Project	15%
Quizzes	35%
Final Exam	25%
Independent Research Project	10%

Attendance Policy and In-class Behavior: Be a grown-up, respect other students, and be responsible for your own actions. That's it. If further interpretation or enforcement of these principles is needed, the instructor has the final word.

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.

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/` While research projects will be done in teams, graded homeworks are individual assignments, and your submissions must be 100% your own work. It is also important that you clearly cite *any* source of material other than the textbook or in-class discussions that influences your solution. This includes any online videos, tutorials, or other sources of information — if it didn't come from your own head and your own creativity, you need to give credit for where the ideas came from.

List of topics

Numbers after topics indicate approximate time, in class days
(Detailed and updated schedule on class web page)

Topic	**Reading**
Class introduction (1)	Syllabus
Research in Computer Science/Security (1)	Handout
Collaborate project meeting and discussion (1)	Handout
Computer security basics (1)	Chapter 1
Math basics for cryptography (2)	Sect 2.1–2.3
Encryption basics (1)	Sect 3.1, 3.2, and 3.5
Traditional block ciphers – ideas/properties (1)	4.1, 4.2, 4.4
Advanced Encryption Standard –AES (1)	Handout
Symmetric ciphers – block cipher modes (2)	7.1–7.7
Software/implementation best practices (1)	
Random and pseudorandom numbers (1)	8.1–8.3
Security models and reasoning about security (2)	Handout
Public key ideas, math, and RSA (2)	9.1, 2.4–2.6, 9.2
Discrete logs and DL-based crypto (1)	2.8, 10.1–10.2
Cryptographic hash functions (2)	Chapter 11
Message Authentication Codes (MACs) (1)	Sections 12.1–12.6
Authenticated encryption and hash-based PRNG (1)	12.7–12.9
Digital Signatures (1)	13.1, 13.2, 13.4, 13.6
Key Management and Certificates (2)	14.2–14.5
Transport layer security (2)	Chapter 17

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

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.