The University of North Carolina at Greensboro — Handout 1
CSC 580: Cryptography and Security in Computing — January 17, 2017
Prof. Stephen R. Tate

CSC 580 Class Information and Syllabus

Instructor: Stephen R. Tate (Steve)
Lectures: Tues/Thurs 9:30–10:45, Petty 227
Office: Petty 166
Office Hours: Tues/Thurs 11:00–12:30, 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) explain and critique current basic research in computer security and cryptography.

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

Other Reading:

- Required readings: 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.

- Graduate students will be given copies of current research papers to read and critique — these will also be available on the class web page when possible.

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 nontraditional, as described below.

Written Homework Problems: 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. Since there will be a large number of these quizzes (12–14), 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.

Semester-long Project: The class includes an ongoing project that will culminate in the production of a secure chat system, using cryptography to meet the security goals. The project will be implemented in Java, using the Java Cryptography Architecture (JCA), which is standardized and available in both desktop Java environments and in Android. We will focus on the information management and communication components (and not the user-interface), but ambitious students may want to experiment with user-interfaces on different platforms. The project will be broken up into pieces that will be assigned every 2–3 weeks, and the pieces may include design and analysis of different components, general testing of JCA features for possible inclusion, and implementation of different features. After each design and analysis phase, we will discuss various options in class and standardize a design that everyone will use moving forward. Students may work together on the project, in groups of up to three students, but *must* turn in *independently-written* work, and must name the students they collaborated with. If groups do not function well, the instructor reserves the right to break up groups or disallow certain collaborations.

Final Exam: There will be a traditional final exam, oriented 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: ***Tuesday, May 9, 12:00pm – 3:00pm***.

Graduate Students: In addition to the work described above, graduate students will be given three research papers during the semester to read and report on with a 1–2 page written summary and critique. During the last 4–6 weeks of the semester, graduate students will complete a project based on current research in a security-related topic of their own choosing. The result could be either a pure research focus, with a 10–15 page survey paper summarizing research related to that topic, or it could be implementation-based (including adding research-based advanced capabilities to the class secure chat program) with a shorter (5–6 page) report.

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

Undergraduates	
Project	25%
Quizzes	50%
Final Exam	25%

Graduate students	
Project	20%
Quizzes	45%
Final Exam	25%
Research Readings/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/` Remember that while collaboration is allowed on project assignments, submitted work should be independently written by each student. 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**
Introduction and security overview (2)	Chapter 1
Math basics for cryptography (1)	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
Java Cryptography Architecture (1)	Online Docs
Advanced Encryption Standard –AES (1)	Handouts
Symmetric ciphers – block cipher modes (2)	7.1–7.7
Random and pseudorandom numbers (2)	8.1–8.4, 8.6
Security models and reasoning about security (2)	Handouts
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 12.1–12.5
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.