CSC 580 Class Information and Syllabus

Instructor: Stephen R. Tate (Steve)
Lectures: Tues/Thurs 2:00–3:15, Stone 215
Office: Petty 166
Office Hours: Tues/Thurs 10:00–12:00, or by appointment
Phone: 336-256-1033
E-mail: `srtate@uncg.edu`

Prerequisites: Grades of at least C (2.0) in CSC 330 and one of CSC 471, CSC 561, CSC 562, or CSC 567, or permission of instructor

Catalog Description: Modern development of cryptography and secure encryption protocols. Program security and viruses. Operating system protection. Network and distributed system security. Database security. Administering security.

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;
- design sound network architectures by applying security technologies such as firewalls, intrusion detection systems, and virus scanners;
- 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 privacy issues can impact system design;
- (Graduate students) explain and critique current basic research in computer security and cryptography.

Class Web Page: `http://www.uncg.edu/cmp/faculty/srtate/580/`

Textbook: William Stallings. *Cryptography and Network Security: Principles and Practice (6th Edition)*. Pearson/Prentice Hall, Upper Saddle River, NJ, 2014.

> *Warning: Make sure you have the proper edition — when you are given homework assignments from the book, they refer to problem numbers in* ***this*** *edition!*

Other Reading:

- Required readings: Some topics will require reading of supplemental materials, including instructor-written handouts and published materials. Hardcopies will be handed out in class, and electronic copies will be made available when possible.
- 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.

Teaching Methods and Assignments: The primary method of instruction will be two 75-minute periods per week for lecture and discussion, with students responsible for completing assigned readings, assignments, and preparing for exams outside of class. Assignments will be a mix of written analysis and applied programming or system experimentation. Written assignments should be turned in on paper and may be either neatly handwritten or printed. Please do not e-mail written homework solutions unless it is an emergency situation, and in that case please use a system-independent format such as a text file or a PDF — *do not e-mail Word files*. Programs may be written in any language that can satisfy the assignment requirements and that I can run, including C, C++, Java, Python, and Sage (a Python-based language/system that directly supports the mathematical structures that are fundamental to cryptography) – check with me in advance if you want to use another language. In some cases programming assignments should also be submitted electronically, in which case instructions will be given with the assignment.

Graduate Students: In addition to the work described above, graduate students will be given approximately four research papers during the semester to read and report on with a 1–2 page written summary and critique. In addition, graduate students will complete a project based on current research in a security-related topic of their own choosing, with the result typically being a 10–15 page survey paper summarizing research related to that topic.

Evaluation and Grading: Each assignment will be labeled with the number of points that it will count, relative to other assignments. Scores will be combined to produce a final average according to the following weighting scheme:

Undergraduates	
Assignments	35%
Midterm Exam	30%
Final Exam	35%

Graduate students	
Assignments	30%
Midterm Exam	25%
Final Exam	30%
Research Readings/Project	15%

List of topics

(Numbers after topics indicate approximate time, in class days)

Topic	**Reading**
Introduction and class policies (1)	Syllabus
Overview of computer security (1)	Chapter 1
Symmetric ciphers – general concepts and classical techniques (2)	Chapter 2
Symmetric ciphers – block ciphers and DES (1)	Chapter 3
Some math – finite fields (2)	Chapter 4
Symmetric ciphers – AES (1)	Chapter 5
Symmetric ciphers – block cipher modes (1)	Chapter 6
Security models and reasoning about security (3)	Handouts
More math – some number theory (1)	Chapter 8
Public key crypto – RSA (1)	Chapter 9
Public key crypto – elliptic curves and other systems (2)	Chapter 10
Cryptographic hash functions (1)	Chapter 11
Pseudorandom generators and stream ciphers (2)	Chapter 7 + handouts
Message Authentication Codes (MACs) (1)	Sections 12.1–12.5
Digital Signatures (1)	Chapter 13
Key Management and Distribution (1)	Chapter 14
User authentication (1)	Chapter 15 + handouts
Transport layer security (1)	Chapter 17
Anonymous Communication – Onion Routing and Tor (1)	Handouts
Implementation issues: case study	Handouts

Exams:

- Midterm: Tuesday, March 1
- Final: Thursday, April 28, 3:30pm – 6:30pm

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 assignments should not be discussed and *all submitted work should be entirely your own.* It is expected that the class textbook will be used as a reference, but if

any other reference materials are used in preparing homework solutions they should be clearly cited. 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 appropriate UNCG office.

Attendance Policy: Attendance will not be taken in class, and is voluntary; however, all students are responsible for everything done or said in class (this can include changes in assignments, due dates, etc.). 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.

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.

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.

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`).

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.