# CSC 580 Class Information and Syllabus

**Instructor:** Stephen R. Tate (Steve)
**Lectures:** Mon/Wed/Fri 1:00–1:50, Petty 227
**Office:** Petty 166
**Office Hours:** Wed/Fri 9:00 – 11:00, 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 of this course 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 (5th Edition)*. Pearson/Prentice Hall, Upper Saddle River, NJ, 2011.

**Other Reading:**

- 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.
- Optional supplemental information: There are many other excellent sources of information on cryptography and computer security. Please see the class web page for an up-to-date list of good material and links to online information.

**Teaching Methods and Assignments:** The primary method of instruction will be three 50-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++, and Java (check with me in advance if you want to use another language), and you should turn in a printout of your source code. 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 three research papers to read during the semester. After reading each paper, students are expected to write a 1–2 page summary and critique of the assigned reading. In addition, graduate students will complete a project based on current research in a security-related topic of their own chosing, 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 | 30% |
| Tests (2) | 40% |
| Final Exam | 30% |

| Graduate students | |
|---|---|
| Assignments | 25% |
| Tests (2) | 35% |
| Final Exam | 25% |
| 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 (2) | Chapter 1 |
| Symmetric ciphers – classical (1) | Chapter 2 |
| Symmetric ciphers – block ciphers and DES (2) | Chapter 3 |
| Some math – finite fields (2) | Chapter 4 |
| Symmetric ciphers – AES (3) | Chapter 5 |
| Symmetric ciphers – block cipher modes (1) | Chapter 6 |
| Pseudorandom generators and stream ciphers (1) | Chapter 7 |
| More math – some number theory (2) | Chapter 8 |
| Public key crypto – RSA (2) | Chapter 9 |
| Public key crypto – Other systems (1) | Chapter 10 |
| Security models and reasoning about security (2) | Handouts |
| Cryptographic hash functions (2) | Chapter 11 |
| Message Authentication Codes (MACs) (2) | Chapter 12 |
| Digital signatures (1) | Chapter 13 |
| Key management and distribution (2) | Chapter 14 |
| User authentication (3) | Chapter 15 |
| Transport layer security (2) | Chapter 16 |
| Network security – intrusion detection and firewalls (3) | Chapters 20,22 |
| Additional topics or review – to be determined (3) | |

**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 any 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. It is particularly important for graduate students to keep this in mind in writing up research summaries or in their project — if there are any questions about standards for proper

citations or attribution, please discuss the matter with the instructor. 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.

Students are required to sign the Academic Integrity Pledge on any work they do (assignments and exams). The pledge is the statement "I have abided by the UNCG Academic Integrity Policy on this assignment."

**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 (also see the late work policy below). It is the student's responsibility to obtain notes from another student if they miss class.

**Laptop/Cellphone Policy:** Laptops can be both a benefit and a distraction in a classroom. While many students benefit from taking notes using a laptop, or having access to outside class-related resources during class, other students cannot resist the temptation of checking e-mail, chatting, or even playing games during class time. This class has a strict "no non-class related use" rule for laptops — if you are found violating this policy, then your in-class laptop privileges will be taken away. Cellphones are a distraction for everyone, and should be turned off during class. If there is a special situation where you need to have your phone on for a particular day, please let the instructor know the situation before 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.

**Final Exam:** Wednesday, December 7, 3:30 – 6:30.

**ADA Statement:** UNCG seeks to comply fully with the Americans with Disabilities Act (ADA). Students requesting accommodations based on a diability must be registered with the Office of Disability Services located in 215 Elliott University Center: (336) 334–5440.