ITIS 6240/8240

Course title: Applied Cryptography

Course date: class meeting times are: August 26, September 2, 9, 16, 23, 30, October 7, 14, 21, 28, November 4, 11, 18, December 2, 9

Location: Woodward Hall 125

Meeting day(s): Wednesday

Meeting time(s): 6:30-9:15pm

Textbooks


October 1996

Instructor Information

Name: Yongge Wang
Email: yonwang@uncc.edu
Office location: Woodward 330E

Office hours: Wednesday 3:00-5:00pm
Phone: (704)6878665

Teaching assistants:

Attendance

Rules: Attendance is required for all scheduled classes. One unexcused absence will cost you 5 points deduction from your final points, two unexcused absences will cost you 10 points deduction from your final points, and three or more unexcused absences may result in the failure of the course.

Topic 1 Classical Cryptography
Topic 2 E-Cash
Topic 3 Block Ciphers
Topic 4 Hash functions
Topic 5 Public key cryptography
Topic 6 PKCS standards
Topic 7 Identity Based Cryptography
Topic 8 Elliptic Curve Cryptography
Topic 9 Secure Password Authentication Protocols
Topic 10 Pseudorandom and statistical testing
**Topic 11**  Quantum key agreement and Shor’s quantum attack algorithm on RSA
**Topic 12**  Privacy preserving garbled computation in Cloud

**Grading**
Policy:
- Midterm exam: 25%
- Final exam: 25%
- Projects, assignments and research: 50%

Typically, A will be given for a total of 90 and above, B will be given for a total of 80 and above, C will be given for a total of 70 and above, D will be given for a total of 60 and above.

**Later submission**
Cost: Students who fail in submitting their assignments by the specified deadlines will receive a reduced mark, on the basis of a 33% reduction for every day after the deadline (regardless of whether it is a working day or not). Projects submitted three days after the deadline will not be graded and the students will receive a 0 mark. Academic Integrity

**Important Dates**
Notice: These dates may change, please check this site regularly for the most recent version

Dates: October 14 (tentative): Midterm Exam
       December 16 (8:00pm-10:30pm): Final exam (please check [http://registrar.uncc.edu/calendar-and-exam-schedules/exam-schedules](http://registrar.uncc.edu/calendar-and-exam-schedules/exam-schedules) for updated schedule)

**Academic Integrity**
Policy: Students have the responsibility to know and observe the requirements of The UNC Charlotte Code of Student Academic Integrity (Catalog p. 375). This code forbids cheating, fabrication, or falsification of information, multiple submission of academic work, plagiarism, abuse of academic materials, and complicity in academic dishonesty. There are no special requirements regarding academic integrity in this course. The code will be strictly enforced and is binding on the students. Grade and academic evaluations in this course include a judgment that the student's work is free from academic dishonesty of any type; and grades in this course therefore should be and will be adversely affected by academic dishonesty. Students who violate the code can be expelled from UNC Charlotte. The normal penalty for a first offense is zero credit on the work involving dishonesty and further substantial reduction of the course grade. In almost all cases the course grade is reduced to an F. Copies of the Code can be obtained from the Dean of Students Office. Standards of academic integrity will be enforced in this course. Students are expected to report cases of academic dishonesty to the instructor immediately.