Instructor: Qi Cheng (qcheng@cs.ou.edu)

Class time and location: MWF 10:30–11:20, CEC 123.

Office hours: MW 1:30-2:45

Topics: In this course, we cover the following topics:

- Basics of computational number theory.
- Block ciphers and cryptographic hash functions.
- The concept of public key cryptography.
- The primality testing, the integer factorization problem and the RSA cryptosystem.
- The finite field discrete logarithm problem and the Digital Signature Algorithm.
- The elliptic curve cryptosystem.

Students who enroll in CS5823 are required to complete a project on elliptic curve cryptosystem. We take an algorithmic approach when introducing abstract mathematical objects. We will use computer algebra systems, e.g. PARI/GP or SAGE, extensively in the class and in the homeworks.


G. Seroussi, Nigel P. Smart and Ian F. Blake, Elliptic Curves in Cryptography, Cambridge Univ Press.

Grading for 4823 students: Assignments (40%), one programming project (20%) and final (40%).

Grading for 5823 students: Assignments(30%), two programming projects (30%) and final (40%).
Specific Outcomes of Instruction: By the end of the semester, the students will increase their: 1. Ability to apply knowledge of computing and mathematics appropriate to the discipline (outcome a), 2. Ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs (outcome c), 3. Understanding of professional, ethical, legal, security, and social issues and responsibilities (outcome e), 4. Ability to use current techniques, skills, and tools necessary for computing practice (outcome i).