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

Class time: MWF 10:30-11:20

Office hours: M 2:30-3:30 W 3:30-4:30

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. The PARI/GP computer algebra system is used extensively in the class and in the homeworks.

ABET Student Outcomes to be addressed
- A: An ability to apply knowledge of computing and mathematics appropriate to the discipline
- C: An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs
- E: An understanding of professional, ethical, legal, security and social issues and responsibilities
- I: An ability to use current techniques, skills, and tools necessary for computing practice


References:
- 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 nal (40%).

Grading for 5823 students: Assignments(30%), two programming projects (30%) and nal (40%).