CS 4823/5823 CRYPTOGRAPHY  
SPRING 2014

Instructor:  Qi Cheng ( qcheng@cs.ou.edu, DEH 254 )

Class time and location:  MWF 10:30–11:20, CEC 117.

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 public key cryptography.
• The primality testing, the integer factorization and the RSA cryptosystem.
• The finite field discrete logarithm 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. SAGE or NTL, extensively in the class and in the homeworks.


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

Grading for 5823 students:  Assignments (35%), two programming projects (25%) and final (40%).