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


Office hours: W 1:30-2:45 F 9-10:20

Teaching Assistant:

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 finite field discrete logarithm, Diffie-Hellman key exchange and the Digital Signature Algorithm.
- The primality testing, the integer factorization and the RSA cryptosystem.
- The elliptic curve cryptosystem and/or lattice-based cryptosystems.

Students who enroll in CS5823 are required to complete a project on lattice-based cryptosystems. We take an algorithmic approach when introducing abstract mathematical objects. We will use computer algebra systems, e.g. SAGE (http://www.sagemath.org) and/or NTL (http://www.shoup.net/ntl) 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: Attendance (10%), assignments (30%), one programming project (20%) and final (40%). For 5823 students: Attendance (10%), assignments (25%), two programming projects (15+10%) and final (40%). Attendance will be taken at 10 class meetings, selected by the instructor. Your attendance score is determined by

<table>
<thead>
<tr>
<th>Number of sign ins</th>
<th>score</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-10</td>
<td>10</td>
</tr>
<tr>
<td>2 ≤ n ≤ 8</td>
<td>n</td>
</tr>
<tr>
<td>0-1</td>
<td>Your course grade is F or AW</td>
</tr>
</tbody>
</table>