**Lecturer:** Larry Washington  
Office: Math 4415    Phone: 301-405-5116    e-mail: lcw@math.umd.edu  
Office hours: Monday 11-12, Wednesday 1-2

Course Web page: www.math.umd.edu/~lcw/crypto.html

**Grader/assistant:** Kate Rendall (rendke@math.umd.edu)

**Grading:** Homework: 15% , Two midterms: 25% each, Final: 35%.  
The midterms are tentatively scheduled for Friday, March 7, and for Wednesday, April 30. The final exam will be on Thursday, May 22, 8-10am.  
Please submit homework as hard copy, not via e-mail. Homework is due by midnight on the due date. Late homework will be accepted up to 1 week late; however, the score will be reduced by a factor of 50%. Homework more than 1 week late will not receive credit.

**Text:** *Introduction to Cryptography with Coding Theory* by W. Trappe and L. Washington.

Cryptology is the study of the design and analysis of various encryption schemes, and related topics. The course will cover the basics of the subject and then touch on several recent developments.

**Approximate Syllabus** (subject to adjustment):
1. Construction and analysis of simple cryptosystems  
2. The Data Encryption Standard and the Advanced Encryption Standard  
3. Public key cryptography  
4. Signature schemes  
5. Secret sharing schemes  
6. Key distribution  
7. Zero-knowledge techniques  
8. Elliptic curves

*Legal notice:* Working together on homework problems, especially computer problems, is fine. However, each person should write answers in her/his own words. It is University policy that undergraduate and graduate students are to be asked to write by hand and sign (on any exam) the following pledge:  

*I pledge on my honor that I have not given or received any unauthorized assistance on this examination.*