Tentative Syllabus
CMSC 443
Cryptology

Instructor: Dr. Lomonaco

1. **Classical cryptography**
2. **Abstract algebra: Groups, rings, fields**
3. **Linear feedback shift registers**
4. **Shannon theory, i.e., information theory**
5. **Block Ciphers and the AES**
6. **Cryptographic hash functions**
7. **The RSA crypto system**
8. **Public-key crypto and discrete logs**
9. **Signature Schemes**
10. **Pseudo-random number generators**
11. **Identification schemes and entity authentication**
12. **Key distribution**
13. **Key agreement schemes**
14. **Secret sharing schemes**
15. **Computational models and computational complexity**
16. **Zero-knowledge proof systems**
17. **Quantum cryptography**

Method of Evaluation: Homework: 25% ; Exam 1: 25% ; Exam 2: 25%; Final: 25%.

All exams including the Final Exam will be with closed books, closed notes, and open mind. Late homework will not be accepted. Exams will be given only at the scheduled times. No makeup exams. Exceptions to this policy may be made in cases of extreme hardship.

Academic Conduct:
By enrolling in this course, each student assumes the responsibilities of an active participant in UMBC's scholarly community in which everyone's academic work and behavior are held to the highest standards of honesty. Cheating, fabrication, plagiarism, and helping others to commit these acts are all forms of academic dishonesty, and they are wrong. Academic misconduct could result in disciplinary action that may include, but is not limited to, suspension or dismissal.

To read the full Student Academic Conduct Policy, consult the UMBC Student Handbook, the Faculty Handbook, or the UMBC Policies section of the UMBC Directory.