ENEE459E/CMSC498R: Introduction to Cryptology

Instructor: Dana Dachman-Soled
Email: danadach@ece.umd.edu
Time/Place: Tues/Thurs 2:00pm-3:15pm, ITV 1100
Office Hours: Tues 3:30pm-4:30pm
Course Webpage: http://www.ece.umd.edu/~danadach/Intro_Crypto_Spring_14
TA: Arthita Ghosh, arthita@umd.edu

Course Description:
Over the past two decades, cryptography has become a highly relevant field: In addition to military and national security applications, cryptography is currently being used in critical financial, legal, and social applications. The aim of cryptography is to construct efficient schemes that allow parties to interact to implement some functionality, even when some subset of parties are malicious and behave adversarially. In contrast to the classical approach based on heuristics and ad-hoc solutions, modern cryptography aims for specific, rigorous security guarantees based on precise mathematical definitions and provably secure protocols.

Course Prerequisites:
Any two 400-level MATH courses; or (CMSC351 and CMSC330); or (ENEE322 and ENEE380).

Textbook:

Course Objectives:
- Understand the theoretical foundations for real-world cryptosystems
- Study formal security models for widely used cryptographic applications
- Analyze various cryptographic schemes and understand their proofs of security
- Become familiar with number theoretic tools used in cryptography

Topics Covered:
- Classical ciphers, Shannon perfect security and impossibility results
- Computational security
- Symmetric-key encryption
- Pseudorandom generators
- Pseudorandom functions, pseudorandom permutations, Feistel transform
- Stream ciphers, block ciphers, modes of operation
- MACs, Authenticated Encryption
- Number theory background
• Collision resistant hash functions
• Public Key Encryption
• Digital Signature Schemes
• Additional advanced topics as time permits

**Grading Method:**
Homeworks (30%) [There will be 5 homeworks assigned.]
Midterm (35%)
Final (35%)