PMAT 329 Introduction to Cryptography

Course Outline:

I Basic Ideas and Definitions

II Classical (one-key) cryptosystems
- Substitution ciphers
- Cryptanalytic techniques

III Information Theory
- Entropy
- Perfect secrecy
- One-time pad

IV Modern (one-key) cryptosystems
- Transposition ciphers and product ciphers
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

V Taxonomy of Cryptosystems
- Modes of operation
- Stream ciphers

VI Number Theory
- Linear Diophantine equations, Euclidean Algorithm
- Fast exponentiation
- Euler's ϕ function, primitive roots

VII Public Key Cryptography
- One-way functions
- Cryptographic key exchange
- one-way trapdoor functions
- RSA
- Authentication
- Other applications (if time permits)

VIII Special topics (if time permits)

Quizzes and Exams:

Quiz dates: Wednesday, September 29
Wednesday, October 20
Wednesday, December 1

Midterm exam: Wednesday, November 10

Quizzes are 50 minutes long and will be written during the Wednesday tutorials.

The midterm exam is 2 hours long and will be written class and tutorial time on Nov. 10.