Math 445
Midterm review topics

- Basic Cryptography
  - Basic framework for a cryptosystem
  - Kerckhoff’s principle
  - Types of attacks
  - Importance of the key size
  - Applications beyond confidentiality

- Classic Cryptosystems
  - Shift cipher
  - Affine cipher
  - Substitution cipher
  - Vigenère cipher
  - Playfair cipher
  - ADFGX cipher
  - Hill cipher
  - One-time pad
  - Linear feedback shift register sequences

- Basic Number theory
  - Divisibility, primes
  - GCD, Extended Euclidean Algorithm
  - Congruences and modular arithmetic
  - Chinese Remainder Theorem
  - Solving linear congruences
  - Matrices modulo n
  - Finding square roots modulo n
  - Concept of a group, notion of the order of an element
  - Fermat’s little theorem, Euler’s theorem, Langrange’s theorem
  - Polynomials modulo p, construction of finite fields
  - generating LFSRs with long period, characteristic polynomial

- Public Key Cryptosystems
  - RSA cryptosystem
  - Attacks on the RSA cryptosystem