UGA Math 4450/6450 -- Cryptography Course Outline -- Spring 2010

Cryptography is the art and science of keeping secrets. In this course we will explore both classical and modern cryptosystems, including those in use today when you send credit card information over the internet. This course will focus on both algorithmic and theoretical aspects of the mathematics of cryptography, which necessarily includes details of implementation and attacks on any cryptosystem we discuss. Prerequisites are a working knowledge of abstract algebra, and the desire to apply this knowledge to work with concrete examples to make and break cryptosystems. A tentative (and fairly ambitious) outline for the course is:

I. Classical Cryptography
1. Shift and Affine Ciphers
2. The Vigenere Cipher
3. Solving Cryptograms
4. Block Ciphers
5. Randomness and Unbreakable ciphers
6. The Enigma Machine
7. DES/AES

II. The Mathematics of Modern Cryptography
1. Modular arithmetic and the units in Z/mZ
2. Continued Fractions and Euclid's Algorithm
3. Solving Linear Diophantine Equations
4. Finite Fields
5. Fast Exponentiation
6. Finding Large Primes (probably)

II. Modern Cryptography Algorithms
1. Diffie-Hellman Secret Sharing
2. RSA
3. El Gamal
4. Digital Signature Algorithms
5. Hash Functions

III. Modern Cryptography Attacks
1. Discrete Log Attacks
2. Factorization Attacks

IV. Additional Topics (only if we have time)
1. Error Correcting Codes
2. Key Distribution
3. Elliptic Curve Cryptography