GEORGIA INSTITUTE OF TECHNOLOGY
School of Electrical and Computer Engineering

ECE 6280
Cryptography and Security
Spring Semester 2008

Instructor:

Faramarz Fekri
Office: Centergy 5227
Phone: (404) 894-3335
FAX: (404) 894-8363
email: fekri@ece.gatech.edu

Class Hours:

MWF 11:05 AM – 11:55 AM
Van Leer C241

Office Hours:

1. After class
2. Friday 10:00-11:00
3. Other times by arrangement

Course Objectives:

This course is an introduction to the basic theory and practice of cryptographic techniques used in security coding. Emphasizing on algebraic and number theory approaches, the coverage includes the mathematics that is relevant to the cryptography, the secret key and public key encryption techniques, signature schemes, hash functions and message authentication codes, and key distribution.

Text:

The textbook is "Cryptography" by D.R. Stinson (the third edition), Chapman & Hall, 2005. Class notes will be provided.

Course Prerequisites:

Graduate Standing.

Grading Formula:

Homework (& Quizzes)	15%
Project	20%
Midterm	25%
Final	40%

Projects:

The project will be graded according to several criteria including the design, the organization and clarity of the report.

Attendance:

Regular attendance in class is mandatory**.**

Homework:

Problem sets will be posted on the class web site every other week on Fridays and will be due at the Friday class of the following week.

Honor Code:

Please uphold the academic honor code. Violations will be reported to the office of Vice-President for Student Services.

Class Web Page:

http://users.ece.gatech.edu/~fekri/teaching /crypto/spring2008/main.html

Course Outline:

1. Introduction
   - Overview of cryptography.
   - Simple classical cryptosystems
   - Cryptanalysis
2. Complexity of Computations
   - The big-O notation
   - Time estimates
   - P, NP, and NP-completeness
3. Shannon's Theory
   - Information theoretic security
   - One time pad
4. Secret Key Encryption (Block Ciphers)
   - Description of DES
   - Description of AES (advanced encryption standard)
5. Brief Review of Algebra and Number Theory
   - Groups, fields, Rings
   - Euclidean algorithm for polynomials
   - Chinese remainder theorem
   - Other useful facts
6. RSA Cryptosystem and factoring Integers (Public Key Cryptosystem)
   - RSA cryptosystem
   - Implementing RSA
   - Probabilistic primality testing
   - Square root modulo n
   - Factoring algorithms (Pollard P-1 alg., Polard Rho alg., Dixon's random square alg., etc)
   - Other attacks on RSA: Decryption exponent, Bit security, Timing attacks
   - Rabin cryptosystem
7. Public Key Cryptosystems based on Discrete Logarithm Problem
   - ElGamal cryptosystem
   - Algorithms for discrete log (Shanks, Pollard Rho, Pohlig-Hellman, and Index Calculus methods)
   - Elliptic curve cryptosystem (Abstract Discrete Log, Discrete Log Ciphers, Elliptic Curves)
8. Digital Signatures
   - How to sign using RSA
   - ElGamal signature scheme
   - Digital Signature Standard (DSS)
9. Hashing
   - Collision-free hash functions, Motivation and applications,
   - Discrete-Log Hash function,
   - Merkle-Damgard and other constructions
   - Message Authentication codes (keyed hash functions)
10. Key Distribution and Key Agreement
    - Key predistribution
    - Deffie-Hellman key exchange
11. Other Topics (time permitting)