GEORGIA INSTITUTE OF TECHNOLOGY

School of Electrical and Computer Engineering

ECE 6280
Cryptography and Security
Spring Semester 2014

Instructor:

Faramarz Fekri
Office: Centergy 5238
Phone: (404) 894-3335
FAX: (404) 894-8363
email: fekri@ece.gatech.edu

Class Hours:

Tus. Thr. 4:35 PM – 5:55 PM
Bunger-Henry, room# 311

Office Hours:

1. After class
2. Wed. 11:00 AM - 12:30 PM (My office)
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 (Theory and Practice)" by Douglas .R. Stinson (the third edition), Chapman & Hall/CRC, 2006.

Lecture notes will also be provided.

Reading List:

- Faramarz Fekri, Farshid Delgosha, "Finite-Field Wavelets with Applications in Cryptography and Coding," Prentice Hall, 2011, ISBN: 0-13-060020-2.
- William Stallings, "Cryptography and Network Security, Principles and Practice," Second Edition, Prentice Hall, 1998, ISBN: 0-13-869017-0.
- "Handbook of Applied Cryptography," Alfred J. Menezes, Paul C. Oorschot, and Scott A. Vanstone, CRC Press 1996 ISBN: 0-8493-8523-7

Course Prerequisites:

Graduate Standing.

Grading Formula:

Homework	10%
Project	20%
Midterm	30%
Final	40%

Project:

The project will involve writing a C code (or in matlab, the least) for a crypto system or a principle component of a crypto system. The project will be graded according to several criteria including the design, and the results, (and the organization and clarity of the report, if it failed to deliver the correct results).

Homework:

The primary way to learn any ECE subject is to WORK HOMEWORK PROBLEMS: as many as possible, and work them CAREFULLY. Homework will be assigned almost bi-weekly on Thursdays and will be due at the beginning of the second Thursday class (14 days to turn in). Late homework will NOT be accepted for grading***. Avoid the temptation to use old homework solutions as a short cut in doing the assignments. This practice tends to limit your own understanding of the material.*** Homework is to be written up and submitted individually. Working with colleagues is encouraged but simply copying someone else's solution is not acceptable and will be treated as such. Homework will be graded and solutions will be available.

Attendance:

Regular attendance in class is mandatory**.**

Honor Code:

Please uphold the academic honor code (see http://www.gatech.edu/honor/). Violations will be reported to the office of Vice-President for Student Services.

Class Web Page:

http://users.ece.gatech.edu/~fekri/teaching/crypto/spring2014/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. Identification Schemes (time permitting)