WHEATON COLLEGE
DEPARTMENT of MATHEMATICS

Mentored Research Study Plan - Cryptography

MATH 493 – Dr. Lovett

Meeting Coordinates: T 1:15-3:05pm, Room 129 Meyer Science Center

Required Text: Introduction to Cryptography and Coding Theory, by Wade Trappe and Lawrence Washington (TW)

Other Useful References:

Introduction to Cryptography, by Johannes Buchmann (JB)
Applied Cryptography, by Bruce Schneier (BS)
An Introduction to Cryptography, by Richard Mollins (RM)

Topic Description:

For thousands of years, for military purposes or to conceal political ideologies, people have devised methods to transcribe a message in such a way that if an unintended person intercepted the message, he or she would be incapable of understanding the content thereof. Now, in the faceless world electronic communication, where one cannot always afford to trust the medium of communication to be free of criminal eavesdroppers or the receiver to not harbor harmful intentions, techniques are absolutely necessary to preserve the integrity and secrecy of communication. Without information security, no electronic financial transaction is safe from an identity thief, no military communication will remain secret, no portion of our social infrastructure that involves any form of automation is safe from criminals.

This course is designed to introduce the student to the mathematical theory and practical uses of cryptography. We will emphasize information security, in particular file encryption, though we will mention applications of related techniques to integrity, authenticity and non-repudiation issues. This course is about discovery. Though we will study both communication protocols and the number theory (and statistics) behind cryptography, the student should understand that we can only scratch the surface and that he or she can learn far more through personal discovery.

Course Objectives:

- Understand the broad mathematical theory of information security.
- Describe the differences between block algorithms and stream ciphers.
- Implement some standard algorithms and some algorithms of our creation.
- Articulate some methods of cryptanalysis.
- Become aware of the issues of presenting a new algorithm to the public.
- Articulate and discuss ethical issues concerning applications of mathematics with an emphasis on information security.

A) Projects

The academic dimension will involve background study, some exercises of your own choosing, and a few projects. We can study all we want but, as a key take-away from this seminar, I would like you to be able to implement in a computer program some of the algorithms that we will discuss. Here are some of the projects we may consider.

1. Implement some basic block algorithms.
2. Implement the DES algorithm for file encryption.
3. Implement the AES algorithm for file encryption
4. Implement a stream cipher (linear or nonlinear) for file encryption.
5. Study and implement project Spartacus.

B) Spiritual/Personal Mentoring function

Professor: Dr. Stephen Lovett
Office / Phone: SCI 177 / 752-5694
Email: Stephen.Lovett@wheaton.edu

In addition to the academic work, the mentored research seminar is intended to provide a closer relationship between students and faculty that is otherwise fostered in usual seminars. For part of our meeting times every week, we will discuss social and ethical issues that are particular to Christian mathematicians. We may also meet outside the classroom.

Assessment:

I have signed you all into this seminar with the tacit assumption that you are motivated. I am hoping that your anticipation will drive you more than the desire for a grade. I will assign a grade for this course according to the following distribution of involvement: Homework 20%; Participation 20%; Projects 60%.

Course Policies:

1) **Inclusive Language**: For academic discourse, spoken and written, the faculty expects students to use gender-inclusive language for human beings. Coarse and culturally insensitive language is not accepted in class. (Gal 3:28; Eph 4:1-6)
2) **Attendance**: I do not require attendance but I will count unexcused attendances against your participation grade.
3) **Special Accommodations**: Wheaton College is committed to providing reasonable accommodations for students with disabilities. Any student with a documented disability needing academic adjustments is requested to contact the Academic and Disability Services Office as early in the semester as possible. Please call 630.752.5941 or send an e-mail to jennifer.nicodem@wheaton.edu for further information.

Tools:

1) **Computer Programming**: I would encourage you also to be ready to program in some computer language. We will often need to open and manipulate files in binary mode. A language with some decent mathematical modules is helpful too.
2) **Maple ®**: If you are not particularly adept with computer programming, I would encourage you to try to figure out some programming in *Maple*.

Schedule and Assignments

Days off:
February 2nd: Faculty Development Day.
March 5-13: Spring Break.

Order of Topics:

1) Cryptography and Cryptanalysis Overview (TW 1.1-2.5)
2) Basic Number Theory (TW 3.1-3.8)
3) Groups & Finite Fields (TW 3.9-3.12)
4) Block Ciphers and Modes of Operation (TW 2.6-2.12 and DB 3.8 or TW 4.5)
5) DES – Data Encryption Standard (TW 4.1-4.4)
6) AES – Advanced Encryption Standard (TW 5.1-5.4)
7) Discuss the Spartacus Project
8) Public Key Algorithms; RSA (TW 6.1-6.7)
9) Diffie-Hellman and Discrete Logarithms (TW 7.1-7.5)
10) Topics of choice out of the rest of the book. (One of my favorites is elliptic curve cryptography but that's because I'm a mathematician.)