SPRING 2010 SYLLABUS FOR MATH 4450/6450

INSTRUCTOR: JONATHAN HANKE

Course Title and Number: Computational Number Theory and Cryptography – Math 4450/6450

Course Description: Recognizing prime numbers, factoring composite numbers, finite fields, elliptic curves, discrete logarithms, private key cryptology, key exchange systems, signature authentication, public key cryptology.

Prerequisites, corequisites, and cross-listings for the course: Prerequisites – MATH 4000/6000. Cross-listed as Math 4450 or Math 6450 (for graduate credit).

Course Objectives: 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.

Topical Outline: A tentative (and fairly ambitious) outline for the course is:

(1) Classical Cryptography
  (a) Shift and Affine Ciphers
  (b) The Vigenere Cipher
  (c) Solving Cryptograms
  (d) Block Ciphers
  (e) Randomness and Unbreakable ciphers
  (f) The Enigma Machine
  (g) DES/AES
(2) The Mathematics of Modern Cryptography
  (a) Modular arithmetic and the units in Z/mZ
  (b) Continued Fractions and Euclid's Algorithm
  (c) Solving Linear Diophantine Equations
  (d) Finite Fields
  (e) Fast Exponentiation
  (f) Finding Large Primes (probably)
(3) Modern Cryptography Algorithms
  (a) Diffie-Hellman Secret Sharing

(b) RSA
(c) El Gamal
(d) Digital Signature Algorithms
(e) Hash Functions
(4) Modern Cryptography Attacks
(a) Discrete Log Attacks
(b) Factorization Attacks
(5) Additional Topics (only if we have time)
(a) Error Correcting Codes
(b) Key Distribution
(c) Elliptic Curve Cryptography

The Honor Code and Academic Honesty Policy: As a University of Georgia student, you have agreed to abide by the University's academic honesty policy, " A Culture of Honesty," and the Student Honor Code. All academic work must meet the standards described in "A Culture of Honesty" found at www.uga.edu/honesty. Lack of knowledge of the academic honesty policy is not a reasonable explanation for a violation. Questions related to course assignments and the academic honesty policy should be directed to the instructor.

Mandatory Disclaimer: The course syllabus is a general plan for the course; deviations announced to the class by the instructor may be necessary.

Principal Course Assignments. The assignments for this course are homework problems given out by the instructor, and two in-class tests. There will also be assigned readings from the book "Introduction to Cryptography with Coding Theory" by Trappe and Washington. For Graduate Credit (i.e. Math 6450) there will also be an in-class (50 minute) presentation as well as a 10-page paper on a specialized/advanced topic in cryptography.

Specific Course Requirements: In addition to the written homework assignments listed above, this course requires you to demonstrate your knowledge of cryptography (without the benefit of a calculator) on in-class written tests and a on written final examination. There may also be occasional in-class quizzes.

Grading Policy: The numerical course grade percentage for Math 4450 (for undergraduate credit) will be determined by the following weighting scheme:

- 40% – homework assignments
- 30% – in-class exam
- 30% – final exam

The numerical course grade percentage for Math 6450 (for graduate credit) will be determined by the following weighting scheme:

- 40% – homework assignments
- 20% – in-class exam
- 20% – final exam
- 20% – final paper and presentation

Attendance Policy: Attendance in class is not required, though there will be no make-up exams for in-class tests or quizzes without an appropriate excuse for the absence (either officially recognized by UGA or approved by the instructor). However attendance in class should improve your knowledge of the material and better prepare you for the homework and tests used to compute your final grade.

Required Course Material: This course is based on the required textbook "University Calculus" by Hass, Weir and Thomas.

Policy for Make-up of Examinations: Make-up examinations will generally not be given, but may be given under exceptional circumstances with approval from the instructor. They require either a written medical excuse note from a doctor stating why you were medically unable to attend the exam at that time, or some other UGA-approved excuse justifying the need for a makeup-exam.

Additional Instructor Information.

- Instructor: Jonathan Hanke
- Instructor Office: Boyd Graduate Center, Room 447.
- Office Hours: Monday & Friday 3:30pm-4:30pm (after class) in the Boyd Graduate Center, Room 447.
- Office Phone: (706) 542-2644
- E-mail: `jonhanke@math.uga.edu`