DEPARTMENT OR PROGRAM OFFERING COURSE: Mathematics

NEW COURSE NUMBER: 75

NEW COURSE TITLE: Applied Topics in Number Theory and Algebra

ABBREVIATED TITLE: Appl Topics Number Th/Algebra

INSTRUCTORS: Rotating (e.g., Pomerance, Shemanske, Wallace)

TERM(S) TO BE OFFERED: Spring, every second year

PERMANENT COURSE OR ONE-TIME OFFERING: Permanent

DISTRIBUTIVE REQUIREMENT CATEGORY: QDS

ORC Description:
Provide some applications of number theory and algebra. Specific topics will vary; two possibilities are cryptology and coding theory. The former allows for secure communication and authentication on the Internet, while the latter allows for efficient and error-free electronic communication over noisy channels. This course counts toward the mathematics major, and is a culminating experience.

Prerequisite: Mathematics 25 or 31 or permission of the instructor.

Course Objective: The objective of this course is to provide an introduction to applications of number theory and/or algebra. Traditionally "applied mathematics" has meant applications of differential equations. Increasingly in the digital age, other parts of mathematics have become useful. In the field of electronic communication especially, number theory and algebra have been applied to make possible clear and accurate transmissions over noisy channels, as well as transmissions secure from eavesdroppers and unauthenticated users.

Course Format: A traditional lecture-oriented class is envisioned. Students may be responsible for presenting special topics to the class.

Week-by-week syllabus for a sample course on Cryptology:

(1) Overview and the history of cryptology. Starting from Caeser ciphers (from the time of Caesar) to the dawn of mathematical cryptology with the German Enigma Code, and the way it was broken by Polish and British mathematicians. See [K].

(2) Number theory from a computational perspective. Some number theoretic problems are easy to do, even if it is not apparent that this is so. Other number theoretic problems remain difficult. See [WT] (all subsequent weeks are taken from [WT]).

(3) Continuing with the thoughts from week 2, primality testing and factoring are discussed, as well as discrete logarithms. Finite fields are introduced.

(4) The Data Encryption Standard. The standard for secret key encryption in the late 20th century.

(5) Rijndael and RSA. The Data Encryption Standard was replaced in 2000 by Rijndael. RSA is one of the basic public-key systems. It was introduced in the 1970s and is still in use today.

(6) Diffie–Hellman and ElGamal. These public-key systems are based on the supposed intractability of the discrete logarithm problem.

(7) Digital signatures and secret sharing. Cryptology can be used for much more than encrypting messages.

(8) Elliptic curves over finite fields. This old mathematical topic is now of vital interest in cryptology.

(9) Factoring using elliptic curves, cryptology using elliptic curves. It is interesting that elliptic curves can not only be used to construct (supposedly) secure cryptosystems, they also can be used to attack the RSA cryptosystem, through the elliptic curve factoring algorithm.

(10) Student reports plus review.

References:

[K] The Codebreakers : David Kahn, "The Comprehensive History of Secret Communication from Ancient Times to the Internet", Scribner, 1996.

[WT] Wade Trappe and Lawrence C. Washington, "Introduction to cryptography and coding theory", Prentice Hall, 2002.

EVALUATION: Homework: 20%, Midterms: 40%, Final Exam: 40%