Title: Coding Theory and Cryptography

Prerequisite: M349

Description: The first part of the course will cover basic coding theory, including correcting and detecting error patterns, maximum likelihood decoding, generator and parity–check matrices, reliability issues, and various bounds. Other topics from coding theory may include cyclic codes and burst–error–correcting codes. The emphasis on this part of the course will be on the construction, encoding, and decoding of several important and practical families of codes.

The second part of the course will cover basic cryptography, including symmetric–key encryption, DES, RSA, and cryptographic protocols. Other topics from cryptography may include primality testing and discrete logarithms. The emphasis on this portion of the course will be on public key methods.

Some knowledge of elementary linear algebra is the only requirement for the course. It is intended to be a practical course, suitable for junior/senior math majors as well as for beginning graduate students in electrical engineering or computer science. It would also serve as a modeling experience for our XMS majors.


Proposed Syllabus, assuming the above text:

- Chapter 1: Introduction to coding theory
- Chapter 2: Linear codes
- Chapter 3: Perfect and related codes
- Chapter 4: Cyclic linear codes
- Chapter 10: Classical cryptography
- Chapter 12: Public key cryptography
- (time permitting) Chapter 7: Burst–error–correcting codes
- (time permitting) Chapter 11: Topics in algebra and number theory

Justification for Majors: This course will serve as a capstone experience for undergraduate math majors interested in discrete mathematics. It enables such students to build upon their linear algebra experience and see some real world applications. Computer projects and reports will be a part of the course, an important ingredient in any capstone experience.
Impact on other Departments: The 500 level will enable graduate students from other departments, such as EE and CIS, to take this course for credit. An informal e-mail request sent out last year generated responses from at least ten such students who were interested in the course. Faculty from EE also expressed an interest in having such a course regularly offered. Currently there is no such course offered at UD, and there appears to be real need to have such a course on the books.