SU DEPARTMENT OF MATHEMATRICS & COMPUTER SCIENCE
SYLLABUS (Tentative)
MATH 447. CRYPTOGRAPHY

Objective: To introduce both classical and modern methods of cryptography, cryptanalysis, and the mathematical principles behind these methods.

Intended for: Junior and Senior Mathematics and Computer Science Majors.

Prerequisite: A C or better in both Math 306 and Math 210.

Texts:

1. *The Code Book* by Smion Singh, Anchor Books, A Division of Random House, Inc., (1999)
2. *Introduction to Cryptography with Coding Theory* Second Edition by Wade Trappe and Lawrence Washington, Pearson Prentice Hall, (2006)

Technology: Mathematica, Maxima, Cryptography Explorer and various other software packages.

Topics	Weeks
Classical Cryptography	3
Shift, substitution, affine, Vigenere, Playfair, ADFGX, ADFGVX, Hill, LFSR, book, one-time pads, and Enigma ciphers. Pseudo-random Bit generation and the early history of cryptography will also be discussed.	
Selected Topics from Number Theory	3
Congruence, modular arithmetic, the Chinese Remainder Theorem, primitive roots, inversion mod n. matrix inversion mod n, Legendre and Jacobi symbols, finite fields, and continued fractions.	
Modern Cryptography	6
DES, AES, RSA, discrete logarithms, information theory, elliptic curves, digital signatures, and lattice methods.	
Optional Topics, Exams, and Presentations	2
Hash functions, security protocols, digital cash, sharing schemes, games, zero-knowledge techniques, and quantum cryptography.	
Total:	14

EVALUATION

Homework	40-60%
In-Class Exercises and Presentations	10-20%
Examinations	20-30%
Final Exam and Final Project	10-25%