

SU DEPARTMENT OF MATHEMATICS & COMPUTER SCIENCE
 SYLLABUS (*Tentative*)
 MATH 490. SPECIAL TOPICS: 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: Admission to graduate study or approval by the department.

Texts:

1. *The Code Book* by Simon 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, Maple and various other software packages.*

Topics	Weeks
<i>Classical Cryptography</i>	4
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.	
<i>Selected Topics from Number Theory</i>	3
Congruences, modular arithmetic, the Chinese Remainder Theorem, primitive roots, inversion mod n. matrix inversion mod n, Legendre and Jacobi symbols, finite fields, and continued fractions.	
<i>Modern Cryptography</i>	5
DES, AES, RSA, discrete logarithms, information theory, elliptic curves, digital signatures, and lattice methods.	
<i>Optional Topics and Exams</i>	2
Hash functions, security protocols, digital cash, sharing schemes, games, zero-knowledge techniques, and quantum cryptography.	
Total	14

EVALUATION

Homework	40-60%
Cipher Challenges	0-20%
Exams	20-30%
Final Exam	10-25%