Salisbury University Department of Mathematical Sciences

MATH 447 : Cryptography
Syllabus (Tentative)

Description: An introduction to both classical and modern methods of cryptography, cryptoanalysis and the mathematical principles behind these methods. Topics include an introduction to number theoretic concepts, classical cyphers and their history, modern symmetric and public-key cyphers, and a mathematical analysis of the strengths and weaknesses of cryptographic methods. 4 Hours Credit: Meets four hours per week.

Prerequisites: C or better in MATH 210, MATH 306.

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

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

Textbooks: *Introduction to Cryptography with Coding Theory*, Second Edition by Wade Trappe and Lawrence Washington, Pearson Prentice Hall, (2006).

The Code Book by Smion Singh, Anchor Books, A Division of Random House, Inc., (1999)

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

Topic	**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%

- Graduate students will be assigned special homework/test problems or projects.
- Clear descriptions of thought processes, evidence of critical thinking, and effective communication must be demonstrated in written work.
- **Writing Across the Curriculum:** Students will be expected to communicate mathematics and mathematical ideas effectively in speech and writing. At the University Writing Center, trained consultants are ready to help you at any stage of the writing process. In addition to the important writing instruction that occurs in the

classroom and during professors' office hours, the Center offers another site for learning about writing. **All students are encouraged to make use of these important services.**

- **NOTE:** Once a student has received credit, including transfer credit, for a course, credit may not be received for any course with material that is equivalent to it or is a prerequisite for it.