Math 470.500
Communication and Cryptography
Course Information

Course Description

From the Catalog. Introduction to coded communications, digital signatures, secret sharing, one-way functions, authentication, error control and data compression.

Prerequisites. Math 222 or 304, and approval of the instructor.

Description. Cryptography is the science and study of secret writing. A cipher is a secret method of writing. Cryptanalysis is the science and study of methods of breaking ciphers. Although cryptography and cryptanalysis have an ancient history, there has probably never been more activity in these areas than at the present time.

The purpose of this course is provide a solid introduction to the theory of cryptography and cryptanalysis. This course will consider both theoretical and computational aspects of cryptography, with the weighting more towards the theoretical. Modern cryptography/cryptanalysis is a multidisciplinary field. Some of the topics include:

- Basic number theory
- Classical cryptosystems
- The Data Encryption Standard (DES)
- AES
- The RSA Algorithm
- A selection of applications

Instructor and Class Information
Jon Pitts
Office: MILN 312
Email: j-pitts@tamu.edu
URL: http://www.math.tamu.edu/~jon.pitts/
Class meets MWF 9:10–10:00 in BLOC 117.
Office hours are (tentatively) MW 10:30-11:30 and by appointment.
Required Items


- **Computer Program.** We will use MATLAB. MATLAB is widely available on university computers. If you wish to purchase MATLAB for home use, then you may consider MATLAB R2009a, Student Version, available from The MathWorks (http://www.mathworks.com/academia/student_version/index.html). Please note that the Student Version does not contain some features that we may need at some point in the course.

Basis for Grading

Course grades will be awarded as follows: A (90-100%), B (80-89%), C (70-79%), D (60-69%), F (59% or less). Semester grades will be determined on the basis of classwork, (at least two) major examinations, and a final exam, all equally weighted. Classwork includes both class participation, and also either or both of homework and quizzes. Problem sets will be assigned periodically. Class participation, in the form of meaningful questions, answers, proofs, constructions, and discussion, is required.

Make-up Policy

Makeups are subject to university policy. In accordance with university regulations, make-ups for missed exams and assignments will be allowed only for a university approved excuse in writing. Whenever possible, students should inform the instructor before an work is missed.

Americans with Disabilities Act (ADA) Policy Statement

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you believe you have a disability requiring an accommodation, please contact the Department of Student Life, Disability Services Office, in Room B118 of Cain Hall or call 845-1637.

Academic Integrity Statement

*An Aggie does not lie, cheat, or steal or tolerate those who do.* The Honor Council Rules and Procedures are available on the web at http://www.tamu.edu/aggiehonor.