Math 470
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 cryptsystems
- The Data Encryption Standard (DES)
- AES
- The RSA Algorithm
- A selection of applications

Instructor and Class Information

Jon Pitts
Email: j-pitts@tamu.edu
URL: http://www.math.tamu.edu/~jon.pitts/

Schedule. Math 470 is web-based. Course materials are available at all hours. Web based contact hours will be determined in consultation with the class.
Required Items


Basis for Grading

The course grade will be based on graded written assignments, sometimes web-oriented. There will be regular homework assignments and papers. The homework scores will be totaled and your score adjusted to count for 2/3 of your course grade. The papers will count for 1/6 of your course grade. Homework and papers will normally be submitted through WebCT.

Course grades will be awarded as follows.

- A – Excellent performance in all aspects of the course.
- B – Satisfactory completion of all course requirements.
- C – Passing.