

Math 243
Codes and Cryptography
Fall 2006

Dr. Edward E. Allen, Manchester 353, Ext: 4854, allene@wfu.edu

Office Hours:

MWF 11:00-11:50 (other hours by appointment—email me and we can set them up).

Text:

Introduction to Cryptography, with Coding Theory, Second Edition, by Trappe and Washington.

Grades:

The final grade in the class will be computed using a weighted average on two exams (50%) and the final exam (50%). To get complete credit on any problem, complete work must be included. Work must be neat and organized.

Homework will be due Tuesdays each week. Late work will not be accepted without prior approval.

Any missed exam will result in a score of 0 without prior approval.

Grades will be computed on a ten point scale (i.e., 93.33 -100 → A, 90-93.32 → A-, 86.66-89.99→ B+, 83.33-86.65→ B, 80-83.32 → B-,etc.).

Exams:

The first exam is scheduled for Friday, September 22. The second exam is scheduled for Friday, November 3. The final exam is scheduled for Friday, December 8 at 2 p.m. The exams may or may not include take-home sections; some exams may be entirely in-class or take-home.

Topics:

We will cover the following chapters of the text: Chapter 2 (Classical Cryptosystems), Chapter 3 (Basic Number Theory), Chapter 4 (DES), Chapter 5 (Rijndael), Chapter 6 (RSA), Chapter 7 (Discrete Logarithms), Chapter 8 (Hash Functions), Chapter 9 (Digital Signatures), Chapter 11 (Digital Cash), Chapter 12 (Secret Sharing Schemes), Chapter 13 (Games), Chapter 16 (Elliptic Curves) and Chapter 19 (Quantum Techniques). Other sections of the text and other mathematical topics will be discussed and tested as time permits.