SYLLABUS – MATH 5405

CRYPTOGRAPHY, CODES, AND COMPUTATIONAL NUMBER THEORY

Description: We will cover mathematical and a few non-mathematical aspects of cryptology. We will learn various modern and historical schemes for encrypting and decrypting messages. In some cases, we will also learn how these schemes were broken in the past. We will also learn some related mathematics and its applications such as error correcting codes. Some computer programming will be expected, python will be the default language choice.

- **Time:** Tuesday, Thursday 12:25 – 1:45pm
- **Location:** LCB 225
- **Instructor:** Karl Schwede
- **Contact information:**
  - email: schwede@math.utah.edu
  - office: JWB 323
  - website: `http://www.math.utah.edu/~schwede/math5405`
- **Office hours:** TBD
- **Textbooks:**

  We have two texts.
  - Gordon Savin's notes which you may already be familiar with from Math 4400, *Numbers groups and cryptography*
    `http://www.math.utah.edu/~savin/book15.pdf`
  - Trappe and Washington, *Introduction to Cryptography with Coding Theory*, 2nd edition.

Grade: Your grade will be determined by the following formula.

45% Homework and other activities (worksheets, group work, computer projects etc.)
10% Midterm #1, tentatively February 18th, in class.
15% Midterm #2, tentatively March 31st, in class.
30% Final (cumulative).

Generally speaking, late homework will not be accepted. In unavoidable circumstances, you must speak with the instructor *prior* to missing the homework in order to receive credit. In such situations, the impact on the grade will be dealt with on a case by case basis.

Students are allowed, and even encouraged to work together when solving homework problems (although each student is responsible for their own write-up). Typing of homework is strongly encouraged and to this end, LaTeX use is also encouraged.

Prerequisites: Students should be familiar with modular arithmetic and basic group theory at the level of Math 4400. A basic knowledge of computer programming/scripting will be helpful.

Academic Integrity: All University of Utah policies regarding ethics and honorable behavior apply to this course.

Disabilities: The Americans with Disabilities Act requires that reasonable accommodations be provided to qualified individuals. To discuss any such accommodations, please contact me as well as the Center for Disability Services, (801) 581-5020, at the beginning of the semester.