MATH 5405 Cryptography and Codes

Bronson Lim

Spring 2020

E-mail: bronson@math.utah.edu
Webpage: math.utah.edu/ bronson/teaching/5405-s20
Office Hours: TR 1:45-3:00 and by appointment.
Class Hours: TR 12:25-1:45PM
Office: JWB 101
Class Room: LCB 222

Prerequisites and Course Information

• “C” or better in MATH 4400.
• MATH 5405, Cryptography and Codes, is a 3 credit course.
• Textbook: An Introduction to Mathematical Cryptography by Hoffstein, Pipher, and Silverman.

Course Description

This is a mathematics course on Cryptography. We will discuss various schemes for encryption and decryption of messages including the RSA cryptosystem, elliptic curve cryptography, lattice based cryptography, and the NTRU cryptosystem. We will also discuss other “advanced” applications of Number Theory.

Additional Resources

• Tutoring Center & Computer Lab: There is free tutoring in the T. Benny Rushing Mathematics Student Center (room 155, the lower level between JWB and LCB), as well as a computer lab. For more information see http://www.math.utah.edu/ugrad/tutoring.html. It is unclear if they will have tutors for this course. But they may have tutors for the number theory part.

• Private Tutoring: University Tutoring Services, 330 SSB. There is also a list of tutors at the math department office JWB 233.
Course Policy

Grading Policy

- **50%** of your grade will be determined by your homework scores. You are encouraged to discuss the problem sets among yourselves and with me at office hours, but the final write-up must be your own work. The lowest homework percentage will be dropped. Variable Extra Credit will be given to those students who type their assignments in \LaTeX\ (typically this will increase your grade 1-2% at the end of the semester). Homework is due on Thursdays by 11:59pm.

- **30%** of your grade will be determined by two exams (that’s 15% each). These will be take-home exams.

- **20%** of your grade will be determined by the **final project**. Details about the final project will be available later. It will be due on the last day of regular class session.

Student Responsibilities

All students are expected to maintain professional behavior in the classroom setting, according to the Student Code (the Code), spelled out in the Student Handbook. Students have specific rights in the classroom as detailed in Article II of the Code. The Code also specifies proscribed conduct (Article XI) that involves cheating on tests, plagiarism, and/or collusion, as well as fraud, theft, etc. Students should read the Code carefully and know they are responsible for the content. According to Faculty Rules and Regulations, it is the faculty responsibility to enforce responsible classroom behavior, and I will do so, beginning with verbal warnings and progressing to dismissal from class and a failing grade. Students have the right to appeal such action to the Student Behavior Committee (http://regulations.utah.edu/academics/6-400.php).

ADA Policy

The University of Utah seeks to provide equal access to its programs, services, and activities for people with disabilities. If you will need accommodations in the class, reasonable prior notice needs to be given to the Center for Disability and Access (CDA), 162 Olpin Union Building, 801-581-5020. CDA will work with you and the instructor to make arrangements for accommodations. All written information in this course can be made available in alternative format with prior notification to the CDA.

Addressing Sexual Misconduct

Title IX makes it clear that violence and harassment based on sex and gender (which includes sexual orientation and gender identity/expression) is a civil rights offense subject to the same kinds of accountability and the same kinds of support applied to offenses against other protected categories such as race, national origin, color, religion, age, status as a person with disability, veterans status, or genetic information. If you or someone you know has been harassed or assaulted, you are encouraged to report it to the Title IX Coordinator in the Office of Equal Opportunity and Affirmative Action, 135 Park Building, 801-581-8365, or the Office of the Dean of the Students, 270 Union Building, 801-581-7066. For support and confidential consultation, contact the Center
for Student Wellness, 426 SSB, 801-581-7776. To report to the police, contact the Department of Public Safety, 801-585-2677 (COPS).

**Student Names and Personal Pronouns**

Class rosters are provided to the instructor with the students legal name as well as Preferred first name (if previously entered by you in the Student Profile section of your CIS account). While CIS refers to this as merely a preference, I will honor you by referring to you with the name and pronoun that feels best for you in class, on papers, exams, group projects, etc. Please advise me of any name or pronoun changes (and update CIS) so I can help create a learning environment in which you, your name, and your pronoun will be respected. If you need assistance getting your preferred name on your UIDcard, please visit the LGBT Resource Center Room 409 in the Olpin Union Building, or email bpeacock@sa.utah.edu to schedule a time to drop by. The LGBT Resource Center hours are M-F 8am-5pm, and 8am-6pm on Tuesdays.

**Wellness Statement**

Personal concerns such as stress, anxiety, relationship difficulties, depression, cross-cultural differences, etc., can interfere with a student’s ability to succeed and thrive at the University of Utah. For helpful resources contact the Center for Student Wellness at www.wellness.utah.edu or 801-581-7776.

**Safety Statement**

The University of Utah values the safety of all campus community members. To report suspicious activity or to request a courtesy escort, call campus police at 801-585-COPS (801-585-2677). You will receive important emergency alerts and safety messages regarding campus safety via text message. For more information regarding safety and to view available training resources, including helpful videos, visit safeu.utah.edu.