MATH 437: Cryptography
Spring 2017 Syllabus

Instructor: Jonathan Totushek, Office: Swenson 3024, `mcs-web.uwsuper.edu/jtotushe`
Office Phone: (715) 394-8066
E-Mail: `jtotushe@uwsuper.edu`
Course Website: `mcs-web.uwsuper.edu/jtotushe/teaching/sp17/crypto`

Lectures: Tuesday and Thursday 8:15 - 9:55 (am) in Swenson 3003. Labs will be in Swenson 3011.
Office Hours: Monday, Wednesday, Friday 1:00 - 2:00 (pm), and Tuesday 10:00 - 11:00 in Swenson 3024
Text: *An Introduction to Mathematical Cryptography (*2^{nd} *edition)*; Hoffstein, Pipher & Silverman; Springer.

Course Description: Study of the theory of cryptography together with applied programming projects. Topics include: discrete probability spaces; Shannon's theory of information and perfect secrecy; classical cryptosystems and cryptanalysis; authentication and key exchange; public key cryptosystems; elementary number theory, primality checking, the RSA cryptosystem; and Advanced Encryption Standard (AES).

Course Objectives: Students will understand several classical and modern approaches to encryption and decryption. They will be able to implement cryptosystems and perform cryptanalysis by building software tools using a modern programming language. They will be able to assess the security level of a cryptosystem using concepts from information theory.

Attendance: Attendance is expected everyday.
Notes: During lecture you will be expected to take notes. I will not be using slide presentations or posting my notes online. If you miss a day of class be sure to get notes from a fellow classmate.

Homework: There will be regular homework assignments. Typically, homework will be assigned on Tuesday and due the following Tuesday. The two lowest homework assignments will be dropped and will not affect your final grade.
Labs: Occasionally we will have programming Labs. All programming will use the Java language. Labs will be due the following class period.
Cryptohunt: A cryptohunt is sort of like a scavenger hunt, except each clue must first be decrypted. At some point during the semester, I will organize a cryptohunt. More details will be provided then.

Exams: There will be two exams and one final exam. They will be closed book and closed notes. Make up exams will only be given in exceptional circumstances and will require prior approval of the instructor. In emergency situations (medical, etc.), appropriate documentation will be required. If absences at exams are not adequately documented, the student will receive 0 points. *There will be NO make-up final exam*.

Exam Dates:

- **Exam 1:** Thursday February 23^{rd}, in class.
- **Exam 2:** Thursday April 6^{th}, in class.
- **Final:** Thursday May 18^{st} from 8:00 to 10:00 am.

No Class: Be aware that there will be no class **March 20 - 24** due to Spring Break and no class on **April 14**.

Grading: The overall course grade will be determined from homework assignments, labs, a cryptohunt, two in class exams and a comprehensive final exam. Grades will be determined in the following way:

- **Homework** 25%.
- **Labs:** 15%.
- **Cryptohunt** 5%
- **Exams 1,2:** 15% each.
- **Final Exam:** 25%.

A: 90% - 100%
B: 80% - 89%
C: 70% - 79%
D: 60% - 69%
F: 0% - 59%

Plus and minus grades will be awarded to students within two percentage points of a grade.

Learn @UW-Superior: I will ***not*** be using Learn @UW-Superior. Your grade can be calculated using the breakdown given above.

Disabilities Accommodation: Students with documented medical disabilities, as covered under the 1990 ADA, will be reasonably accommodated once the student has provided the instructor a signed copy of the FAF (Faculty Accommodation Form) provided by Disabilities Support Services (DSS). Since accommodations are not retroactive, students must identify themselves and their reasonable accommodation needs (via FAF) to the instructor at the beginning of each semester accommodations will be needed, or within a reasonable period of time before the accommodations will be required. The DSS office is located in 1024 Swenson Hall. Questions related to DSS accommodation-related needs may be made by calling 394-8515 or e-mailing `disability@uwsuper.edu`

University Policies: The University of Wisconsin-Superior is dedicated to a safe, supportive and nondiscriminatory learning environment. It is the responsibility of all undergraduate and graduate students to familiarize themselves with University policies regarding special accommoda- tions, academic misconduct, religious beliefs accommodation, discrimination and absence for University sponsored events. For details of the Student Disciplinary Procedures:

- Academic Misconduct Disciplinary Process (Chapter 14) can be found at `http://docs.legis.wisconsin.gov/code/admin_code/uws/14.pdf`
- Student Nonacademic Disciplinary Procedures (UWS Chapter 17) can be found at `http://docs.legis.wisconsin.gov/code/admin_code/uws/17.pdf`