Math 373: Introduction to Cryptography, Spring 2023

Instructor: Kevin Milans (milans@math.wvu.edu)
Class Meetings: MWF 10:30am-11:20am in Hodges Hall 321
Office Hours: MW 2:00pm-3:00pm and by appointment, in Armstrong Hall 408H
Webpage: http://www.math.wvu.edu/~kgmilans/teaching/sp23/math373/

Welcome: Welcome to Math 373: Introduction to Cryptography. I have the highest hopes and expectations for your academic achievement this semester. It is my responsibility to ensure that you have all the tools you need to succeed, including quality instruction and timely feedback. It is your responsibility to use these tools to learn the course material. Hard work and dedication to the course are necessary for success, but your course grade is ultimately based on how well you understand the course material as measured by quizzes and tests.

Mathematics can be a difficult subject to learn. It takes time, it takes work, and it can even be frustrating at times. Take heart: this is normal, and the reward that comes with understanding a deep piece of mathematics is well worth your struggle. You need not struggle alone. I am happy to answer your questions during office hours and via email. You are also encouraged to work with other students to master course material.

Learning Outcomes: Students will understand the theory of selected cryptosystems (such as elementary ciphers and public-key cryptography), and the underlying mathematics (such as elementary number theory, statistics, and combinatorics). In addition, students will be familiar with some of the historical development of cryptography.

Prerequisite: Math 155

Textbook: *An Introduction to Mathematical Cryptography (second ed.)*, by J. Hoffstein, J. Pipher, and J. Silverman.

Homework: Homework is a crucial part of learning. You are strongly encouraged to work on the homework with other students in the class, but your written work must be your own. In particular, *you must fully understand everything written down on your paper under your own name.* You may not obtain answers to homework exercises by using search engines, other textbooks, scholarly research articles, or other resources. Claiming the work of others as your own is a serious violation of academic integrity known as plagiarism. It also robs you of your chance to learn and defeats the purpose of the homework.

Homework will generally be assigned on Wednesdays and due the following Wednesday. Homework is evaluated on *completeness*, and, depending on availability of resources, *correctness* on selected problems. Your homework is expected to be neat and conform to accepted standards for professional work-products. Handwriting must be clearly legible, and margins must be respected. Except for excused absences, late homework is not accepted. Your lowest two homework scores are dropped.

Computer Use: Some homework problems require use of a computer programming package. You are free to implement algorithms in an environment of your choice. Python is a good option, has plenty of documentation, and is free to install.

Permitted Calculators: On quizzes and tests, you may use a permitted calculator. Simple 4-function calculators and scientific calculators allowed by NCEES testing policy are permitted (e.g. TI-30X, TI-36X). Programmable calculators, or use of cell phones as calculators, are not permitted.

Quizzes: A quiz corresponding to the latest homework will generally be held on Fridays. You may use a permitted calculator; no other aids are allowed. In accordance with the make-up policy, your lowest two quiz scores are dropped.

Tests: There will be 3 tests, each covering between 1/4 and 1/3 of the course material. You may use a permitted calculator and one 8.5 by 11 inch sheet of *handwritten* notes during each test. No other aids are permitted. The tests are scheduled for **Fri. Feb. 3, Fri. Mar. 10, and Fri. Apr. 14**. In accordance with the make-up policy, your lowest test score will be replaced by your score on the final exam if doing so will help your grade.

Final Exam: The final exam is Thursday, May 4, 2:00pm-4:00pm. All students must take the final exam during the scheduled exam period, unless specifically exempted by university rules. You may use a permitted calculator and one 8.5 by 11 inch sheet of *handwritten* notes during the final. No other aids are permitted. The final exam is cumulative.

Attendance: Attendance is expected. Leaving class early or arriving late is disruptive and counts as an absence. Failure to take quizzes/tests and failure to collect quizzes/tests when returned is considered evidence of absence. Students who miss 5 or fewer classes earn an attendance bonus of 2%. All absences, including those related to university Days of Special Concern, are counted against the attendance bonus.

Expected Classroom Behavior: Talking with your neighbors, reading material unrelated to the course, listening to audio entertainment on your headphones, texting, and cell phones are not permitted in class.

Grading Rubric: Course averages are converted to letter grades according to the scale on the right. The instructor reserves the right to lower these thresholds.

Homework	20%
Quizzes	15%
Tests	$15\% \cdot 3 = 45\%$
Final Exam	20%
Total	100%
Attendance Bonus	2%

A:	90–100	B:	80-89.9
C:	70-79.9	D:	60-69.9
F:	0-59.5		

Make-up Policy: Excused absences that result in a missed work are, to the extent possible, accommodated by dropping the assessment (homeworks/quizzes) or by final exam score replacement (tests). Excused absences have the highest priority for dropping/replacing an assessment. In the event that a student's excused absences exhaust the provisions for dropping/replacing, make-up work may be required. Students must notify the instructor of excusable absences as soon as possible.

Regrade Policy: Regrades may be requested by submitting the original work with a written explanation of your request up to 1 week after the work is returned. Regrade requests are to be used to correct errors in grading. Regrade requests that challenge the amount of a deduction are usually not considered, since deductions for common mistakes are applied uniformly to all students. When regrading, the entire problem(s) in question will be reviewed, and all discovered errors in grading (including any that previously favored the student) will be corrected. The resulting grade may be higher than, equal to, or lower than the original.

Academic Integrity: You are expected to practice the highest possible standards of academic integrity. Any deviation from this expectation will, at a minimum, result in an academic penalty of a score of zero on the assignment or test in question. Additional disciplinary measures are possible. For more information, see the university's Student Conduct Code.