Math 373/578: Introduction to Cryptography, Spring 2014

Instructor: Kevin Milans (milans@math.wvu.edu)
Class Meetings: MWF 8:30am-9:20am in Armstrong Hall 117
Office Hours: MW 9:30am-10:30am, Th 1:00-2:00pm, and by appointment, in Armstrong Hall 408H
Webpage: http://www.math.wvu.edu/~milans/teaching/sp14/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 and Course Goals: Students will understand the theory of selected cryptosystems (such 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*, by J. Hoffstein, J. Pipher, and J. Silverman.

Approved Calculators: A simple arithmetic/scientific calculator is permitted during quizzes and tests. Calculators with graphing capabilities, built-in programming languages, networking, or computer algebra systems are not permitted during quizzes and tests. If you are unsure whether a particular calculator is acceptable, please see the instructor.

Homework: In mathematics classes, most of your learning occurs while doing homework exercises. Late homework is not accepted. Your two lowest homework scores are dropped. You are strongly encouraged to work on the homework with other students in the class, but your written work must be your own. Homework will be collected and graded for *completeness* and *accuracy*, weighted equally. To earn credit for *completeness*, your homework must be complete, stapled, your writing must be clear, and your work must not be cramped. The *accuracy* of your work is checked on a selected problem.

Homework Workshop: Homework workshop sessions will be held once a week, tentatively scheduled for Wednesdays 5pm-6pm. The workshops are dedicated to working on the current homework assignment in small groups (at most 3 students per group). Students are encouraged to make serious attempts to solve some problems before the weekly sessions. Students will discuss the problems, brainstorm ideas, and find solutions together. The instructor will be available for assistance and to offer hints. Attendance is optional but recommended.

Graduate Credit: Most homework assignments will contain challenge problem(s). These problems are *required* for Math 578 students and are *extra credit* for Math 373 students.

Sage: Most homework assignments will contain computer problems. These problems are to be solved using Sage, an open source mathematics engine. You may download sage to your computer, or you may use sage through a web interface at http://www.sagenb.org/. Both options are free of charge.

Quizzes: We will have short quizzes in class on most Fridays. Quizzes cover material on the corresponding homework. Each quiz will feature at least one problem that is very similar to a homework problem. No make-up quizzes are offered. Your lowest two quiz scores are dropped. No aids are permitted, except an approved calculator.

Tests: There will be 3 tests, administered in class. No make-up tests are offered. However, I will replace one of your test scores with your score on the final exam if doing so will help your course average. You may use an approved calculator and one 8.5 by 11 inch *handwritten* sheet of notes during each test. No other aids are permitted. Each test covers roughly 1/3 of the course material. The tests will be on Fri. January 31, Fri. February 28, and Fri. April 4.

Final Exam: The final exam is Wednesday, April 30, 11:00am-1:00pm. All students must take the final exam during the scheduled exam period, unless specifically exempted by university rules. Students who miss the final exam will receive a score of zero. You may use an approved calculator and one 8.5 by 11 inch *handwritten* sheet of 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 4 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 using a laptop or cell phone are not permitted in class.

Classroom Participation: A bonus of up to 2% is possible for excellent classroom participation. The bonus is to be earned cooperatively by all students in the course, and all students receive the same classroom participation bonus. Activities that have a positive effect on the classroom participation bonus include asking and answering mathematical questions. To earn a high classroom participation bonus, a large portion of the class must ask or answer questions occasionally. *Activities that are not permitted in class have a strong negative effect on the classroom participation bonus.* Determination of the classroom participation bonus is entirely at the discretion of the instructor. In general, it is easy to reduce the classroom participation bonus quickly, and increasing the classroom participation bonus requires a prolonged period of good classroom participation.

Office Visit Bonus: Students who visit the instructor's office during regularly scheduled office hours (or when the instructor is in) on or before Jan. 22, 2014 earn a 0.25% course bonus.

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	15%
Quizzes	15%
Tests	$15\% \cdot 3 = 45\%$
Final Exam	25%
Total	100%
Office Visit Bonus	0.25%
Attendance Bonus	2%
Classroom Participation Bonus	up to 2%

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

Make-up Policy: No make-up quizzes or tests will be offered. Since the lowest two quiz grades are dropped, you may miss two quizzes and still earn full credit in the course. Since up to 1 test score can be replaced by your grade on the final exam, you may miss 1 test and still earn full credit in the course. This policy covers all absences, including absences due to university Days of Special Concern. In truly exceptional cases, students may be excused from additional quizzes or tests. Students with truly exceptional circumstances should contact the instructor as soon as possible, and appropriate arrangements will be made on a case by case basis.

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.

University Statement on Social Justice: West Virginia University is committed to social justice. I concur with that commitment and expect to maintain a positive learning environment based upon open communication, mutual respect, and non-discrimination. Our University does not discriminate on the basis of race, sex, age, disability, veterans status, religion, sexual orientation, color or national origin. Any suggestions as to how to further such a positive and open environment in this class will be appreciated and given serious consideration.

If you are a person with a disability and anticipate needing any type of accommodation in order to participate in this class, please advise me and make appropriate arrangements with the Office of Disability Services (304-293-6700).