MATH 373 Introduction to Cryptography, Section 001
MWF 10:30-11:20am at Life Sciences G15

Instructor	Tony Se
E-mail	tony.se@mail.wvu.edu
Office Hours	TTh 3:30-4:30 pm at Collaborate Ultra, or by appointment

General Course Information

Method of Instruction: Lecture
Students can also attend lectures online. The links will be posted on eCampus.
Credit Hours: 3
Course Prerequisites: MATH 155

Course Materials

Textbook

An Introduction to Mathematical Cryptography, by J. Hoffstein, J. Pipher, and J. Silverman. Available at WVU Libraries.

Calculators

You may use a scientific or graphing calculator on quizzes.

eCampus

Information about this course will be posted on eCampus. Please check eCampus regularly for announcements, homework and quiz solutions, your grade, etc. Any updates to this syllabus will also be posted on eCampus.

Technology Requirements

Internet Connection

You must have a computer with reliable and continuous Internet access, and a webcam if you choose to take a quiz remotely.

Online Proctoring

Quizzes and the Final Exam will be given in person and/or via Zoom. More details will be given during the semester.

Attendance Policy

You may attend the lectures either in person or online. If you attend class online, you will need reliable Internet connection whenever you take a quiz. There are no points for attendance, but you must submit class notes regularly. See Appendix B(ii).

Mastery Grading

This course will use Mastery Grading. In Mastery Grading, students earn their course grade by demonstrating competence in a list of **course objectives**, instead of by accumulating points on an exam. The standards for meeting course objectives are high. See Appendix (A) to (C). However, students will have multiple chances to meet each objective during the semester.

Quizzes and Final Exam

Achievement of course objectives is assessed in take-home or in-class quizzes. You will have at least two times during the semester to demonstrate competence in each objective. Questions on quizzes are graded on a refined pass/fail scale. See Appendix B(i). Your achievement of each objective is given by the objective grade on your latest attempt.

Extra Attempts on Course Objectives

If you are unsatisfied with your current objective grade and would like to reattempt the objective, you can wait for the objective to appear on the next quiz. If the objective has already appeared twice, you may reattempt the objective during office hours, or by appointment. Please try to notify me **24 hours** in advance if you would like to reattempt an objective during office hours or by appointment. You can just walk in to an office hour without notifying me, but then you will need to wait for me to prepare a question for the objective.
You may reattempt the objectives in **one** office hour visit per week. You may reattempt multiple objectives per visit.

Homework and Class Notes

You will need to submit homework and class notes regularly. These are graded on a pass/fail scale. See Appendix B(ii).

Final Paper

You will need to turn in a Final Paper at the end of the semester, which you need to submit and review several times during the semester. A list of topics for the Final Paper, due dates, and grade rubrics will be posted later in the semester.

Calendar

01/19	Tuesday	First day of classes
01/25	Monday	Last day to add a class
03/03	Wednesday	No class
04/02	Friday	No class
04/16	Friday	Withdrawal deadline
05/03	Monday	Make-up lecture for snow day (Jan 20)
05/07	Friday	**Final Paper due at 4pm**

Mental Health Statement

Mental health concerns or stressful events can adversely affect your academic performance and social relationships. WVU offers services to assist you with addressing these and other concerns that you may be experiencing. You can learn more about the broad range of confidential mental health services available on campus at the Carruth Center for Psychological and Psychiatric Services (CCPPS) website: https://carruth.wvu.edu/

- If you are in need of crisis services, call the CCPPS main number 24/7: (304) 293-4431.

Crisis services are also available through text: Text WVU to 741741 for support 24/7 from a trained Crisis Counselor.

Academic Integrity

The integrity of the classes offered by any academic institution solidifies the foundation of its mission and cannot be sacrificed to expediency, ignorance, or blatant fraud. Therefore, instructors will enforce rigorous standards of academic integrity in all aspects and assignments of their courses. For the detailed policy of West Virginia University regarding the definitions of acts considered to fall under academic dishonesty and possible ensuing sanctions, please see the West Virginia University Academic Standards Policy (http://catalog.wvu.edu/undergraduate/coursecreditstermsclassification/). Should you have any questions about possibly improper research citations or references, or any other activity that may be interpreted as an attempt at academic dishonesty, please see your instructor before the assignment is due to discuss the matter.

Notice of Class Recording Policy

Meetings of a course at West Virginia University (WVU), whether online or in-person, may be recorded. Recordings are not guaranteed, and are intended to supplement the planned class session. Recordings will be made available to class participants, which may include students, assistants, guest lecturers, and co-facilitators. Recordings may be shared by the instructor or institution in accordance with WVU Rules and policies. The Recordings are owned by and contain intellectual property of WVU. The Recordings may not be shared, copied, reproduced, redistributed, transferred, or disseminated in any form or by any means without the prior written consent of authorized officials of WVU.

Inclusivity Statement

The West Virginia University community is committed to creating and fostering a positive learning and working environment based on open communication, mutual respect, and inclusion.
If you are a person with a disability and anticipate needing any type of accommodation in order to participate in your classes, please advise your instructors and make appropriate arrangements with the Office of Accessibility Services. (https://accessibilityservices.wvu.edu/) More information is available at the Division of Diversity, Equity, and Inclusion (https://diversity.wvu.edu/) as well.

Sale of Course Material Statement

All course materials, including lectures, class notes, quizzes, exams, handouts, presentations, and other course materials provided to students for their courses are protected intellectual property. As such, the unauthorized purchase or sale of these materials may result in disciplinary sanctions under the Student Conduct Code. (https://studentconduct.wvu.edu/campus-student-code)

Sexual Misconduct Statement

West Virginia University does not tolerate sexual misconduct, including harassment, stalking, sexual assault, sexual exploitation, or relationship violence [BOG Rule 1.6 (https://policies.wvu.edu/finalized-bog-rules/bog-governance-rule-1-6-rule)]. It is important for you to know that there are resources available if you or someone you know needs assistance. You may speak to a member of university administration, faculty, or staff; keep in mind that they have an obligation to report the incident to the Title IX Coordinator (http://titleix.wvu.edu/what-is-title-ix/who-is-the-title-ix-coordinator).
If you want to speak to someone who is permitted to keep your disclosure confidential, please seek assistance from the Carruth Center (http://carruth.wvu.edu/), 304-293-9355 or 304-293-4431 (24-hour hotline), and locally within the community at the Rape and Domestic Violence Information Center (RDVIC, http://www.rdvic.org/), 304- 292-5100 or 304-292-4431 (24-hour hotline).
For more information, please consult WVU's Title IX Office (https://titleix.wvu.edu/resources-offices).

Student Evaluation of Instruction Statement

Effective teaching is a primary mission of West Virginia University. Student evaluation of instruction provides the university and the instructor with feedback about your experiences in the course for review and course improvement. Your participation in the evaluation of course instruction is both strongly encouraged and highly valued. Results are strictly confidential, anonymous, and not available to the instructor until after final grades are released by Admissions and Records. Information about how you can complete this evaluation will provided by your instructor.

Appendix

(A) Course Objectives

I. Foundations of Mathematics
F.1 I understand and can use set notation. F.2 I understand the meaning of if-then and if-and-only-if statements. F.3A, B I can give simple proofs and/or counterexamples.
II. Number Theory
N.1 I can use the Euclidean Algorithm to write the greatest common divisor of two positive integers *a* and *b* as a linear combination of *a* and *b*. N.2 I can perform basic modular arithmetic. N.3 I can carry out the Fast Powering Algorithm in modular arithmetic. N.4 I understand applications of Fermat's Little Theorem. N.5 I can determine whether an element of $\mathbf{F}_p$ is a primitive root. N.6 I can compare functions using order notation. N.7 I can use the Chinese Remainder Theorem to solve systems of congruences. N.8 I can use the Chinese Remainder Theorem to find square roots in modular arithmetic. N.9 I can use Quadratic Reciprocity to calculate Legendre and Jacobi symbols.
III. Mathematical Problems in Cryptography
P.1 I understand the meaning of the Discrete Logarithm Problem. P.2 I understand the meaning of the Diffie-Hellman Problem. P.3 I can use Shanks's Babystep–Giantstep method to solve discrete logarithm problems. P.4 I can use the Pohlig-Hellman Algorithm to solve discrete logarithm problems. P.5 I can use a collision algorithm to solve discrete logarithm problems. P.6 I can use Pollard's ρ Method to solve discrete logarithm problems. P.7 I can use Euler's Theorem to find roots modulo *pq*. P.8 I can use the Miller-Rabin test to check whether an integer is probably prime. P.9 I can use Pollard's *p*-1 method to factor integers.
IV. Methods in Cryptography
C.1 I can encrypt and decrypt messages using simple substitution and affine ciphers. C.2 I can cryptanalyze simple substitution ciphers. C.3 I can encrypt and decrypt messages using the Elgamal public key cryptosystem. C.4 I can encrypt and decrypt messages using the RSA public key cryptosystem. C.5 I can encrypt and decrypt messages using the Goldwasser–Micali public key cryptosystem. C.6 I can create and verify RSA digital signatures. C.7 I can create and verify Elgamal digital signatures. C.8 I can create and verify DSA digital signatures.

Note: This list of objectives is subject to change.

(B) Grade Rubrics

(i) The are four possible grades for questions on the quizzes.

Score	Meaning
3 (E)	Excellent • The student follows the instructions in the question and uses the methods learned *in this course*, and • the student shows all required work, and • the student presents the solution very clearly, and • the student gives a correct or nearly correct final answer, and • the student makes no conceptual errors and no logical errors, and • the student makes at most 1 or 2 minor mistakes in all of mathematics (MAT), notation (NTN), and arithmetic (ARI) combined, depending on the length of the problem.
2 (P)	Passing • The student follows the instructions in the question and uses the methods learned *in this course*, and • (MST) at most 1 or 2 minor steps are missing or incorrect in the student's work, depending on the length of the problem, and • (RCL) the student presents the solution rather clearly, and • the student gives a correct or nearly correct final answer, and • the student makes no conceptual errors and no logical errors, and • (MMI) the student makes at most 2, 3 or 4 minor mistakes in all of mathematics (MAT), notation (NTN), and arithmetic (ARI) combined, depending on the length of the problem.
1 (I)	Improving • The student shows some understanding of the problem and uses the methods learned *in this course*. However, • (INS) the student fails to follow some instructions in the question, or • (STP) at least 1 important step, or at least 2 or 3 minor steps are missing or incorrect in the student's work, depending on the length of the problem, or • (PRS) the presentation of the solution requires the reader to guess the student's intent, or • (FIN) the student gives an incorrect final answer which is not a minor mistake, or • (UNF) the student's answer is unfinished or incomplete, or • (CON) the student makes a conceptual error, or • (LOG) the student makes a logical error, or • (IRR) the student gives an irrelevant or nonsensical argument, or • (REQ) the student makes an error in prerequisite material either from previous courses or from previous objectives in the current course, or • (MIS) the student makes at least 3, 4 or 5 minor mistakes in all of mathematics (MAT), notation (NTN), and arithmetic (ARI) combined, depending on the length of the problem.
0 (N)	Not gradable • The student does not meet the requirements of an I grade.

During a reattempt during office hours, students will have opportunities to correct their mistakes following prompts by the instructor. The grade rubrics for reattempts are the same as the table above, with the following adjustments.

Score	Adjusted meaning for reattempts during office hours
3 (E)	The student makes only minor mistakes (MMI) or misses only minor steps (MST), and is able to correct the errors without any or with only slight instructor prompts.
2 (P)	The student makes only minor mistakes (MMI) or misses some steps (STP), and is able to correct the errors with detailed instructor prompts.
1 (I)	The student shows some understanding of the problem, but • the student has errors other than (MMI), (MST) and (STP), or • the student is not able to correct the errors (MMI), (MST) or (STP) even after detailed instructor prompts.
0 (N)	The student does not show any understanding of the problem.

(ii) There are two possible grades for homework and class notes.

Score	Meaning
2 (P)	Passing The student shows some understanding of the material and made a serious attempt in the assignment.
1 (N)	Not passing The student did not make a serious attempt in the assignment, or the student's work is not gradable (similar to a 0 on a quiz).

(iii) The grade rubrics for the Final Paper will be posted later in the semester.

(C) Course Grade

Initial student grades are calculated as follows. This is not yet the student's final letter grade.

Base grade	Meaning
A	• The student achieves an E in at least 50% of the objectives, and • the student achieves at least a P in at least 90% of the objectives, and • the student achieves at least two Ps in Chapter I, and at least three Ps in Chapters II, III and IV, and • the student achieves at least a P on the Final Paper.
B	• The student achieves an E in at least 35% of the objectives, and • the student achieves at least a P in at least 80% of the objectives, and • the student achieves at least two Ps in Chapter I, and at least three Ps in Chapters II, III and IV, and • the student achieves at least a P on the Final Paper.
C	• The student achieves an E in at least 20% of the objectives, and • the student achieves at least a P in at least 70% of the objectives, and • the student achieves at least two Ps in Chapter I, and at least three Ps in Chapters II, III and IV, and • the student achieves at least a P on the Final Paper.
D	• The student achieves an E in at least 10% of the objectives, and • the student achieves at least a P in at least 60% of the objectives, and • the student achieves at least two Ps in Chapter I, and at least three Ps in Chapters II, III and IV, and • the student achieves at least a P on the Final Paper.
F	The student does not meet the requirements of a D.

The student's **final** letter grade is determined by the following adjustments to the initial grade.

- Students may earn a + grade if they achieve many more E's than required. The meaning of "many more" will be determined at the end of the semester.
- Students will earn one letter grade lower if they achieve a P in less than 80% of the homework or 80% of the class notes without a university-related excuse. Students may fail for excessive missed assignments.

Last updated: January 28, 2021