



UNG | UNIVERSITY of
NORTH GEORGIA™

MATH 3540 : Introduction to Cryptography

College of Science and Mathematics - Mathematics Department

Summer 2021

Professor: John Bergschneider
E-mail: john.bergschneider@ung.edu

Class Room: Newton Oakes Center X206
Class Hours: MW 01:00pm-03:15pm

Course Description

This course is an introduction to the mathematics used in cryptography. Among the topics included in the course are the difficulty of an algorithm in terms of polynomial time; number theory topics such as divisibility, greatest common divisor, the Euclidian Algorithm, prime numbers, congruence, Fermat's little theorem, factoring, discrete logarithms; encryption schemes and the associated matrices or linear maps; perfect security; the DES algorithm; public-key encryption; digital signatures. The ability to read mathematical proofs will be expected.

Prerequisites

You must have the following course prerequisite completed: MATH 2460 with a grade of C or better. It is the student's responsibility to check and prove eligibility.

Course Materials

Materials for this course include:

- *Required Textbook*: Introduction to Modern Cryptography 9781466570269/ 1466570261 By Katz, Jonathan and Lindell, Yehuda
- *Technology Resources*: We will be using Python through Jupyterbooks.

Grading

Assignments

Grades in this course will be roughly based on assignments with value according to the following scale:

- * 10% In class assignments
- * 30% Homework
- * 30% Programming Assignments
- * 30% Tests

Grade Scale

- * A 90.00 and higher
- * B 80.00-89.99
- * C 70.00-79.99
- * D 60.00-69.99
- * F 0-59.99
- * Plus/minus grades may be assigned.

Students may withdraw before the UNG designated date with a grade of W. Any student who withdraws after mid-semester will be assigned a grade of WF (as described in the UNG bulletin).

Exam Dates

The midterm is tentatively scheduled to be taken on July 7th. The final is tentatively scheduled to be taken on August 4th.

University Attendance Policy

University of North Georgia expects students to attend all regularly-scheduled classes for instruction and examination. When a student is compelled for any reason to be absent from class, the student should immediately convey the reason for the absence directly to the instructor. The student is responsible for all material presented in class and for all announcements and assignments.

Excused absences include documented illness, deaths in the family and other documented crises, call to active military duty or jury duty, religious holy days, and official University activities. These absences will be accommodated in a way that does not arbitrarily penalize students who have a valid excuse. Consideration will also be given to students whose dependent children experience serious illness.

"Attendance" and participation are required. You will be expected to attend class when scheduled and participate in ongoing discussions of the lesson topics and to interact with other students and your instructor regularly. It is expected that you will demonstrate a positive attitude and courtesy toward other participants in the discussion.

Policy for Missed Assignments

Students must provide advance notice of absences (when possible) as well as relevant documentation regarding absences to the instructor as soon as possible following the illness or event that led to an absence. Regardless of whether an absence is excused or unexcused, the student is responsible for making up all work that is missed.

Missed Assignment

Late assignments will not be accepted without advance approval of the instructor. If the absence is excused then assignment must be turned in by the next class period. An unexcused assignment will result in a grade of zero.

Missed Test

If a test absence is excused then, at the instructor's discretion, a make up exam will be arranged. An excused make-up exam must be taken within one week of the excused absence. If an excused make-up exam is not taken within one week a penalty may be applied to the test grade. No make up tests will be given for an unexcused absence or for the final test.

Tutoring

Free online tutoring through Tutoring Services is available for enrolled UNG students. Tutoring sessions are conducted by UNG professional and peer tutors. Please contact Tutoring Services at tutoring.services@ung.edu, or find more information at <https://ung.edu/tutoring-services/index.php>.

Syllabus Change Policy

Specific details of this syllabus may be subject to change. Students are expected to refer to the Supplemental Syllabus for the following information: <https://ung.edu/academic-affairs/policies-and-guidelines/supplemental-syllabus.php>

1. Academic Exchange
2. Academic Integrity Policy
3. Academic Success Plan Program
4. Class Evaluations

5. Course Grades and Withdrawal Process
6. Disability Services
7. Disruptive Behavior Policy
8. Campus Carry
9. Inclement Weather
10. UNG 5 Core Institutional Values
11. UNG Alert