School of Mathematics and Statistics - Carleton University
Number Theory and Cryptography, Math 3809, Fall 2024

Instructor: Daniel Panario
Email: daniel@math.carleton.ca
http://www.math.carleton.ca/∼daniel

Day and time of course: Tuesdays and Thursdays, 8:35 - 9:55.
Lecture room: HP 4369.

Office hours: Thursdays 13:35 - 14:25, in **HP 4372**.

Textbook: the course has no official textbook. Recommended reading: (1) *Number Theory and Computer Applications* by R. Kumanduri and C. Romero, 1998; (2) *A Friendly Introduction to Number Theory* by Joseph Silverman, 4th edition, 2013; and (3) *Cryptography: Theory and Practice* by Douglas Stinson and Maura Paterson, 4th edition, 2018.

Prerequisites: MATH 2108 or MATH 3101 or MATH 2100; some knowledge of a computer language.

Course Objective: This course introduces students to the methods and techniques of number theory with a focus on applications to cryptography. Topics include congruences, prime numbers, Diophantine equations, classical cryptography and public-key cryptography using number theory; primality testing, factoring and discrete logarithms in relation to cryptography.

Evaluation: Midterm tests (30%), Assignment (20%), and Final Examination (50%).

You must pass the term work in order to pass the course. If you have a passing term mark (50% of midterm tests and assignment) and you do better on the final exam, then I will count the final exam for 100% of the course.

We will distribute, every week, a list of problems to work and prepare for tests and assignment; those problems are not to be handed-in. Solutions will be given on the following week.

Midterm Exams: There will be two midterm exams on October 10 and November 14; each midterm test is worth 15% of the final mark.

Assignment: There will be an assignment for 20% of the final mark. The assignment will be given by Thursday October 3. Due date: October 31.

Final Examination: There will be a three hour closed-book exam scheduled by the University that will take place sometime during the examination period. The exam is worth 50% of the final mark.

Chat GPT/Generative AI usage: In no component of this course, the use of Chat GPT or Generative AI is allowed.

Tentative lecture schedule

Week	Dates	Topics
1	Sep. 5	Introduction to the course. Divisibility.
2	Sep. 10-12	GCD and LCM. Euclidean algorithm. Linear Diophantine equations.
3	Sep. 17-19	Modular arithmetic. Modular inverses.
4	Sep. 24-26	Classical cryptosystems.
5	Oct. 1-3	Classical cryptosystems (cont). Cryptanalysis. **Assignment handed out by Oct. 3.**
6	Oct. 8-10	Primes. Unique factorization. **Midterm # 1 on Oct. 10.**
7	Oct. 15-17	Elementary factoring methods. Chinese remainder theorem.
8	Oct. 21-25	**Fall break, no classes.**
9	Oct. 29-31	Fermat theorem. Euler's Phi function. Euler's theorem. Lagrange's theorem. **Assignment handed by Oct. 31.**
10	Nov. 5-7	RSA cryptosystem. Pseudoprimes and Carmichel numbers.
11	Nov. 12-14	Pollard's p-1 and rho factorization methods. **Midterm #2 on Nov. 14.**
12	Nov. 19-21	Order. Primitive roots. Discrete logarithm.
13	Nov. 26-28	Diffie-Hellman scheme. ElGamal cryptosystem. Digital signatures.
14	Dec. 3-5	Quadratic residues. Euler's criterion. Course review.

Academic Accommodation

Carleton is committed to providing academic accessibility for all individuals. You may need special arrangements to meet your academic obligations during the term. The accommodation request processes, including information about the Academic Consideration Policy for Students in Medical and Other Extenuating Circumstances, are outlined on the Academic Accommodations website: http://students.carleton.ca/course-outline

Pregnancy obligation: write to me with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website.

Religious obligation: write to me with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website.

Academic accommodations for students with disabilities: The Paul Menton Centre for Students with Disabilities (PMC) provides services to students with Learning Disabilities (LD), psychiatric/mental health disabilities, Attention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorders (ASD), chronic medical conditions, and impairments in mobility, hearing, and vision. If you have a disability requiring academic accommodations in this course, please contact PMC at 613-520-6608 or pmc@carleton.ca for a formal evaluation. If you are already registered with the PMC, contact your PMC coordinator to send me your Letter of Accommodation at the beginning of the term, and no later than two weeks before the first in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, meet with me to ensure accommodation arrangements are made. Please consult the PMC website for the deadline to request accommodations for the formally-scheduled exam (if applicable).