School of Mathematics and Statistics - Carleton University
Number Theory and Cryptography, Math 3809, Fall 2021

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

Day and time of course: Mondays and Wednesdays 14:35 - 15:55, Online. **Hybrid, on Zoom:** synchronous on Mondays, and asynchronous on Wednesdays.

Office hours: Mondays 13:35 - 14:25, Online.

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%), Tutorials (8%), Assignment (12%), and Final Examination (50%).

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

Tutorials: Wednesdays 16:35-17:25.
Teaching assistant: TBA.

Tutorials begin on September 22, 2021. Tutorials are a very important part of this course. In each tutorial you will be given a couple of questions to work on. There will be 9 tutorial quizzes in the term for a total of 8% of the final mark. Each quiz is marked as 0, 1/2 or 1; the best eight marks are counted for the tutorial grade, and the lowest grade is discarded; quizzes not completed are marked as zero. TA's office hour will be announced later.

Midterm Exams: There will be two midterm exams on October 13 and November 17, in tutorial; each midterm test is worth 15% of the final mark.

Assignment: There will be an assignment for 12% of the final mark. The assignment will be given by Wednesday October 6. Due date: November 3.

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.

Academic Accommodation

You may need special arrangements to meet your academic obligations during the term. For an accommodation request the processes are as follows:

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).

Tentative lecture schedule

Week	Dates	Topics
1	Sep. 8	Introduction to the course. Divisibility.
2	Sep. 13-15	GCD and LCM. Euclidean algorithm. Linear Diophantine equations.
3	Sep. 20-22	Modular arithmetic. Modular inverses.
4	Sep. 27-29	Classical cryptosystems.
5	Oct. 4-6	Classical cryptosystems (cont). Cryptanalysis. **Assignment handed out by Oct. 6.**
6	Oct. 13	Primes. Unique factorization. **Midterm # 1 on Oct. 13 in tutorial.**
7	Oct. 18-20	Elementary factoring methods. Chinese remainder theorem.
8	Oct. 25-29	**Fall break, no classes.**
9	Nov. 1-3	Fermat theorem. Euler's Phi function. Euler's theorem. Lagrange's theorem. **Assignment handed by Nov. 3.**
10	Nov. 8-10	RSA cryptosystem. Pseudoprimes and Carmichel numbers.
11	Nov. 15-17	Pollard's p-1 and rho factorization methods. **Midterm #2 on Nov. 17 in tutorial.**
12	Nov. 22-24	Order. Primitive roots. Discrete logarithm.
13	Nov. 29 - Dec 1	Diffie-Hellman scheme. ElGamal cryptosystem. Digital signatures.
14	Dec. 6-10	Quadratic residues. Quadratic reciprocity law. Course review.