Cryptography - Syllabus

Department of Mathematics & Statistics

CSCI/MATH 4116, Winter 2024

Dalhousie University acknowledges that we are in Mi'kma'ki, the ancestral and unceded territory of the Mi'kmaq People and pays respect to the Indigenous knowledges held by the Mi'kmaq People, and to the wisdom of their Elders past and present. The Mi'kmaq People signed Peace and Friendship Treaties with the Crown, and section 35 of the Constitution Act, 1982 recognizes and affirms Aboriginal and Treaty rights. We are all Treaty people.

Dalhousie University also acknowledges the histories, contributions, and legacies of African Nova Scotians, who have been here for over 400 years.

Course Instructor(s)

Name	Email	Office Hours
Karl Dilcher, Chase 325	karl.dilcher@dal.ca	Mon., Fri. 12:00-1:00 or by appointment

Course Description (Calendar Entry)

This course is an introduction to modern cryptographic techniques and its mathematical foundations. The material covered includes: elementary number theory and algebra, classical cryptosystems, probability, the Data Encryption Standard, prime number generation and primality tests, public key cryptosystems, and further applications, such as digital signatures and identification.

Course Prerequisites: MATH 1000.03, MATH 1010.03, MATH 1030.03 (or MATH 2030.03), and at least six additional credit hours in Mathematics beyond the first year, or permission of the instructor.

Student Resources

The Math & Stats Learning Centre in the Chase Building is **not** set up to deal with questions related to this course. Instead, visiting office hours is encouraged.

Course Structure

Course Delivery: In-person only. Classes will not be recorded.

Lectures: Mondays, Wednesdays, and Fridays, 10:35–11:25 pm, LSC 236.
First class: Monday, January 8.

Course Materials

- Fully worked-out notes for this course will be posted on Brightspace as a pdf file for free download. This will be your primary resource.
- Further resources will be posted on Brightspace when they are needed. This will always be announced in class.

Assessment

Component	Weight (% of final grade)	Date
Assignments	25%	Weekly (10 or 11)
Midterm Exam	30%	TBA
Final Exam (3 hours)	45%	Scheduled by Registrar

- Detailed instructions about assignment submission and policies will be posted on Brightspace.
- The midterm exam will be scheduled in consultation with the class.

Conversion of numerical grades to final letter grades follows the Dalhousie Grade Scale

A+ (90-100)
A (85-89)
A- (80-84)
B+ (77-79)
B (73-76)
B- (70-72)
C+ (65-69)
C (60-64)
C- (55-59)
D (50-54)
F (0-49)

Course Policies on Missed or Late Academic Requirements

Late assignments will normally not be accepted. However, reasonable accommodations will be made on an individual basis in the case of special circumstances. Student Declarations of Absence will not be necessary, and will not be accepted, for assignments. Detailed guidelines and instructions concerning assignments will be posted on Brightspace along with the first assignment.

Possible serious scheduling conflicts involving the midterm exam must be made known as soon as possible for accommodations to be granted.

Course Policies related to Academic Integrity

See the detailed assignment guidelines and instructions for issues related to academic integrity. In addition, any irregularities detected during or after the midterm or final exam will immediately be referred to the Faculty of Science’s Academic Integrity Officer.

As far as generative AI is concerned, it will not be helpful for this course. However, I will not respond to e-mail messages that are obviously created by generative AI.

Learning Objectives

- An understanding of the mathematical basics of modern cryptography.
- Knowledge and understanding of the currently most important cryptosystems.
- Ability to judge the strength or weaknesses of a cryptosystem.
- Ability to take further courses in mathematical or practical cryptography.

Course Content

With some possible exceptions, the entire content of the course notes will be covered, but the exact schedule will remain flexible. The main topics covered are:

1. Introduction
2. Classical Cryptography
3. Probability and Perfect Secrecy
4. Modern Classical Cryptosystems
5. Public-Key Cryptography
6. Some Additional Topics

University Policies and Statements

Recognition of Mi’kmaq Territory

Dalhousie University would like to acknowledge that the University is on Traditional Mi’kmaq Territory. The Elders in Residence program provides students with access to First Nations elders for guidance, counsel, and support. Visit or e-mail the Indigenous Student Centre at 1321 Edward St or elders@dal.ca. Additional information regarding the Indigenous Student Centre can be found at: https://www.dal.ca/campus_life/communities/indigenous.html

Internationalization

At Dalhousie, ‘thinking and acting globally’ enhances the quality and impact of education, supporting learning that is “interdisciplinary, cross-cultural, global in reach, and orientated toward solving problems that extend across national borders.” Additional internationalization information can be found at: https://www.dal.ca/about-dal/internationalization.html

Academic Integrity

At Dalhousie University, we are guided in all our work by the values of academic integrity: honesty, trust, fairness, responsibility, and respect. As a student, you are required to demonstrate these values in all the work you do. The University provides policies and procedures that every member of the university community is required to follow to ensure academic integrity. Additional academic integrity information can be found at: https://www.dal.ca/dept/university_secretariat/academic-integrity.html

Accessibility

The Student Accessibility Centre is Dalhousie's centre of expertise for matters related to student accessibility and accommodation. If there are aspects of the design, instruction, and/or experiences within this course (online or in-person) that result in barriers to your inclusion, please contact the Student Accessibility Centre (https://www.dal.ca/campus_life/academic-support/accessibility.html) for all courses offered by Dalhousie with the exception of Truro. For courses offered by the Faculty of Agriculture, please contact the Student Success Centre in Truro (https://www.dal.ca/about-dal/agricultural-campus/student-success-centre.html)

Conduct in the Classroom – Culture of Respect

Substantial and constructive dialogue on challenging issues is an important part of academic inquiry and exchange. It requires willingness to listen and tolerance of opposing points of view. Consideration of individual differences and alternative viewpoints is required of all class members, towards each other, towards instructors, and towards guest speakers. While expressions of differing perspectives are welcome and encouraged, the words and language used should remain within acceptable bounds of civility and respect.

Diversity and Inclusion – Culture of Respect

Every person at Dalhousie has a right to be respected and safe. We believe inclusiveness is fundamental to education. We stand for equality. Dalhousie is strengthened in our diversity. We are a respectful and inclusive community. We are committed to being a place where everyone feels welcome and supported, which is why our Strategic Direction prioritizes fostering a culture of diversity and inclusiveness (Strategic Priority 5.2). Additional diversity and inclusion information can be found at: http://www.dal.ca/cultureofrespect.html

Student Code of Conduct

Everyone at Dalhousie is expected to treat others with dignity and respect. The Code of Student Conduct allows Dalhousie to take disciplinary action if students don't follow this community expectation. When appropriate, violations of the code can be resolved in a reasonable and informal manner - perhaps through a restorative justice process. If an informal resolution can't be reached, or would be inappropriate, procedures exist for formal dispute resolution. The full Code of Student Conduct can be found at: https://www.dal.ca/dept/university_secretariat/policies/student-life/code-of-student-conduct.html

Fair Dealing Policy

The Dalhousie University Fair Dealing Policy provides guidance for the limited use of copyright protected material without the risk of infringement and without having to seek the permission of copyright owners. It is intended to provide a balance between the rights of creators and the rights of users at Dalhousie. Additional information regarding the Fair Dealing Policy can be found at: https://www.dal.ca/dept/university_secretariat/policies/academic/fair-dealing-policy-.html

Originality Checking Software

The course instructor may use Dalhousie's approved originality checking software and Google to check the originality of any work submitted for credit, in accordance with the Student Submission of Assignments and Use of Originality Checking Software Policy. Students are free, without penalty of grade, to choose an alternative method of attesting to the authenticity of their work and must inform the instructor no later than the last day to add/drop classes of their intent to choose an alternate method. Additional information regarding Originality Checking Software can be found at: https://www.dal.ca/dept/university_secretariat/policies/academic/student-submission-of-assignments-and-use-of-originality-checking-software-policy-.html

Student Use of Course Materials

Course materials are designed for use as part of this course at Dalhousie University and are the property of the instructor unless otherwise stated. Third party copyrighted materials (such as books, journal articles, music, videos, etc.) have either been licensed for use in this course or fall under an exception or limitation in Canadian Copyright law. Copying this course material for distribution (e.g. uploading to a commercial third-party website) may lead to a violation of Copyright law.