DALHOUSIE UNIVERSITY

Faculty of Science Course Syllabus
Department of Mathematics & Statistics
MATH 4116: Cryptography (online)
Winter 2021

Instructor: Karl Dilcher, karl.dilcher@dal.ca

Lectures: Synchronous, through Collaborate Ultra (within BrightSpace). Lectures will be recorded.

Office Hours: Through Collaborate Ultra; times TBA.

Course Description (from Calendar)

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.

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 Materials

- Course Notes: “Cryptography”; made available electronically and free of charge in the Brightspace page for the course.
- Additional materials will also be made available, as required.

DALHOUSIE UNIVERSITY

Course Delivery (online)

- Synchronous, through the course Brightspace page → Contents → Collaborate Ultra.
- Mondays, Tuesdays, Thursdays, 1:35 – 2:25 pm.
- Attendance is strongly encouraged, but not required.
- Classes will be recorded.

Course Assessment

Component	Weight (% of final grade)	Date
Assignments	***30 %***	weekly (except around midterm)
Midterm test	***30 %***	TBA (in consultation with class)
Final exam	***40 %***	(Scheduled during exam period)

Conversion of numerical grades to Final Letter Grades follows the Dalhousie Common Grade Scale

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

Course Policies on Missed or Late Academic Requirement

- *Missed midterm or final exam:* Make-up exams will be offered; SDA forms required.
- *Assignments:* The lowest two (including missed assignments) will not count. Further information can be found in a detailed set of guidelines posted on Brightspace.

Course Content

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