DALHOUSIE UNIVERSITY

Faculty of Science Course Syllabus
Department of Mathematics and Statistics

Math/CSCI 4116, Cryptography

Winter 2020

"KBXLTKBXSWC, DSQLXEU FSTOTR, AGCCTCCTC PGX GPEU XDIXL, MIX CIADTKT MTBIXU."
- MTDXDBPR DICCTEE

Instructor: Peter Selinger, Chase 303
Email: selinger@dal.ca (please mention "4116" on the subject line)

Lectures: MWF 11:35-12:25, Hicks 217

Course Description

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.

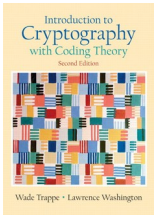
Course Prerequisites

MATH 1000, MATH 1010, MATH 1030, and at least six additional credit hours in Mathematics beyond the first year, or permission of the instructor.

Course Objectives/Learning Outcomes

Cryptography is the art and science of keeping messages secure. It is also used for digital signatures, access control and authentication, timestamping, electronic voting, online auctions, electronic currencies, and in many other applications. The security of modern cryptosystems is strongly linked to mathematics, and in particular to hard problems in number theory. Users should not only know how these techniques work, but must also be able to estimate their efficiency and security. This course is a first introduction to these concepts.

Course Materials



- *Textbook: W. Trappe and L.C. Washington: Introduction to Cryptography with Coding Theory, 2nd edition, Prentice Hall, 2005. This book is available in the Dalhousie bookstore for $183.39 (hardcover), or from Amazon.ca from $40.24 (paperback). If you buy it from the Dalhousie bookstore, look under MATH 4116 (not CSCI 4116).*
- *Course website on Brightspace is accessed through dal.brightspace.com*

Course Assessment

Homework	*20%*	*Assigned and collected in class.*
Midterm 1	*20%*	***Wednesday February 12** in class.*
Midterm 2	*20%*	***Friday, March 20** in class.*
Final Exam	*40%*	*3 hours – Scheduled by the Registrar. Must pass final exam to pass the course.*

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

A+ [90-100]	**B+** [77-80)	**C+** [65-70)	**D** [50-55)
A [85-90)	**B** [73-77)	**C** [60-65)	**F** [0-50)
A- [80-85)	**B-** [70-73)	**C-** [55-60)	

DALHOUSIE UNIVERSITY

Course Policies

1. Calculators, textbooks, and notes are not allowed for Midterm Tests or the Final Examination.
2. Late homework will not be accepted except with the instructor's prior permission.
3. A missed midterm cannot be written at another time. If you miss a midterm without prior permission, then it will count as a 0. Exceptions are made in two cases: (1) if you obtain the instructor's prior permission to miss a midterm, or (2) if you have an officially valid excuse such as a medical doctor's note. In these cases, the weight of the missed midterm will be shifted to the final exam (e.g., the final exam will then count 60% instead of 40%). There is no make-up option for the final exam except in cases of an officially valid excuse such as a medical doctor's note.
4. Student Declaration of Absence forms will be accepted for missed homework, but not for a midterm or final exam. To miss a midterm or final exam, you must always have a doctor's note signed by a medical professional.
5. Students are encouraged to study in groups, but each student must complete their own homework, quizzes, and exams.

Course Content (dates are approximate, details may vary)

January 6-10	The ring of integers, ideals, lcm and gcd. Euclid's algorithm.
January 13-17	Modular arithmetic, classic ciphers, letter frequency attacks.
January 20-24	More classic ciphers. Substitution permutation networks.
January 27-29	Linear cryptanalysis. JANUARY 31 – LAST DAY TO DROP WITHOUT "W"
February 3-7	Differential cryptanalysis. FEBRUARY 7 – MUNRO DAY (NO CLASS)
February 10-14	FEBRUARY 12, WEDNESDAY – FIRST MIDTERM, IN CLASS Chinese Remainder Theorem. Modular exponentiation, uniqueness of prime factorization.
February 17-21	STUDY BREAK (NO CLASS)
February 24-29	Group theory, Fermat's Little Theorem. Euler's Theorem, Euler's phi function.
March 2-6	3-pass protocol. Primality testing, Fermat pseudoprime test, Miller-Rabin test. The RSA cryptosystem.
March 9-13	MARCH 9 – LAST DAY TO DROP WITH "W" Continued fractions, attacks on RSA. Primitive roots modulo n. Discrete logarithms.
March 16-20	Applications of discrete logarithm. Diffie-Hellman key exchange protocol. Computing discrete logarithms. Factoring methods: Fermat's method, quadratic sieve, Pollard rho method. MARCH 20, FRIDAY – SECOND MIDTERM, IN CLASS
March 23-27	ElGamal cipher. Introduction to elliptic curves.
Mar 30 - April 3	Elliptic Diffie-Hellman key exchange and elliptic ElGamal cryptosystem. Elliptic curve factoring.
April 6	Review.

University Policies and Statements

See Brightspace for Part B of this syllabus, "University Policies and Statements".