DALHOUSIE UNIVERSITY

# Faculty of Science Course Syllabus
# Department of Mathematics and Statistics

*Math/CSci 4116, Cryptography*
*Winter 2019*

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

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

**Lectures**: MWF 2:35-3:25, LSC C332

---

## 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 1000.03, 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.*

## 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 $30.27 (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 13** in class.* |
| *Midterm 2* | *20%* | ***Friday, March 22** 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 7-11 | The ring of integers, ideals, lcm and gcd. Euclid's algorithm. |
| January 14-18 | Modular arithmetic, classic ciphers, letter frequency attacks. |
| January 21-25 | More classic ciphers. Substitution permutation networks. |
| January 28-30 | Linear cryptanalysis.<br>FEBRUARY 1 – MUNRO DAY (NO CLASS) |
| February 4-8 | FEBRUARY 4 – LAST DAY TO DROP WITHOUT "W"<br>Differential cryptanalysis. |
| February 11-15 | FEBRUARY 13, WEDNESDAY – FIRST MIDTERM, IN CLASS<br>Chinese Remainder Theorem.<br>Modular exponentiation, uniqueness of prime factorization. |
| February 18-22 | STUDY BREAK (NO CLASS) |
| Feb 25-Mar 1 | Group theory, Fermat's Little Theorem.<br>Euler's Theorem, Euler's phi function. |
| March 4-8 | 3-pass protocol.<br>Primality testing, Fermat pseudoprime test, Miller-Rabin test.<br>The RSA cryptosystem. |
| March 11-15 | MARCH 11 – LAST DAY TO DROP WITH "W"<br>Continued fractions, attacks on RSA.<br>Primitive roots modulo n. Discrete logarithms. |
| March 18-22 | Applications of discrete logarithm. Diffie-Hellman key exchange protocol.<br>Computing discrete logarithms.<br>Factoring methods: Fermat's method, quadratic sieve,<br>Pollard rho method.<br>MARCH 22, FRIDAY – SECOND MIDTERM, IN CLASS |
| March 25-29 | ElGamal cipher. Introduction to elliptic curves. |
| April 1-5 | Elliptic Diffie-Hellman key exchange and elliptic ElGamal cryptosystem.<br>Elliptic curve factoring. |
| April 8 | Review. |

## University Policies and Statements

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