COMP 4109A – Fall 2019

Applied Cryptography

Course Outline : Preliminary Version, 2019

This is a preliminary version of the course outline and may change.
A final version will be posted at the start of classes.

People

Instructor : Jason Hinek
Teaching Assistants : Cheldon, Hemant and Nicholas

Course Information

Classroom : Azrieli Theatre room AT 101
Class Times : Monday & Wednesday from 11:35am – 12:55pm
Course Website : https://www.carleton.ca/culearn/

Calendar Description

Practical aspects of cryptography. Pseudo random number generation, symmetric cryptography (stream and block ciphers), modes of operation, hash functions, message and entity authentication protocols, zero knowledge, pitfalls deploying public-key encryption and digital signatures, key distribution, secret-sharing.

Prerequisites

COMP2804, one of COMP2402/SYSC2100, and a MATH course at the 2000-level or above.

Precludes additional credit for COMP 4103 (no longer offered).

I will assume that you are familiar with run-time complexity (big O) and basic algorithm analysis. I will assume you are familiar with modular arithmetic.

This course will involve some mathematics. This course will involve some coding.

Textbooks

The course has one mandatory textbook.

- Serious Cryptography – A Practical Introduction to Modern Encryption
  Jean-Philippe Aumasson (https://nostarch.com/seriouscrypto)

There are also several good free resources.

- Handbook of Applied Cryptography, by A. J. Menezes, P. C. van Oorschot and S. A. Vanstone (link)
- Cryptography engineering: design principles and practical applications, by N. Ferguson, T. Kohno, and B. Schneier. (Available in library)

Evaluation

50% : Assignments & Challenges
10% : Project
20% : Tests (two in-class midterm tests; Oct 16th & Nov 20th)
20% : Final Exam (Scheduled by the registrar's office)

Note: There will be a computational aspect to some of the assignment problems and all challenges. This may involve programming with a C++ library like NTL, using the the BigInteger class in Java, using software that does symbolic computation (CAS software) or something similar to work with very large numbers (and perhaps work with elliptic curves). If you are using a non-standard language you must receive approval from the TAs first.

Note: Your assignments must be typeset. My suggestion is to use LaTeX or some other similar variant (such as XeLaTeX if you want to easily use nice fonts). I will post the assignment .tex files on the course webpage if you want to use these as a starting point for your solutions.

Important Dates

See the University Calendar for all important dates:
http://carleton.ca/registrar/registration/dates-and-deadlines/

Wed, Sep 4	First class
Mon, Oct 14	No classes (holiday)
Wed, Oct 16	Midterm 1
Oct 21–25	No classes (Fall break)
Wed, Nov 20	Midterm 2
Fri, Dec 6	COMP 4109 Last class (Friday; acting as missed Monday)

Collaboration Policy

★ Assignment work may be done individually or in pairs. If you work as a pair then you will submit a single assignment on behalf of both students.

Projects will be done in teams of 2–4 people.

There is no collaboration allowed for the challenges, midterms or final exam.

Posting assignment solutions on discussion boards before the due date and time is strictly prohibited. Asking questions about the assignment on discussion boards other than the course forum (cuLearn) is strictly prohibited.

We will be looking for plagiarism in both written solutions and in your submitted code.

Undergraduate Academic Advisor

The Undergraduate Advisor for the School of Computer Science is available in Room 5302C HP, by telephone at 520-2600, ext. 4364 or by email at undergraduate_advisor@scs.carleton.ca.

The undergraduate advisor can assist with information about prerequisites and preclusions, course substitutions/equivalencies, understanding your academic audit and the remaining requirements for graduation. The undergraduate advisor will also refer students to appropriate resources such as the Science Student Success Centre, Learning Support Services and the Writing Tutorial Services.

University Policies

Full academic regulations are found in the University's calendar (link). Some excerpts are below.

Academic Integrity

Every student should be familiar with the Carleton University student academic integrity policy. A student found in violation of academic integrity standards may be awarded penalties which range from a reprimand to receiving a grade of F in the course or even being expelled from the program or University. Some examples of offences are: plagiarism and unauthorized co-operation or collaboration. Information on this policy may be found in the Undergraduate Calendar.

Plagiarism is presenting, whether intentional or not, the ideas, expression of ideas or work of others as one's own. Plagiarism includes reproducing or paraphrasing portions of someone else's published or unpublished material, regardless of the source, and presenting these as one's own without proper citation or reference to the original source.

In cases where an investigation determines that a violation of the Academic Integrity Policy has occurred, sanctions may be applied by the Faculty Dean, the Provost and Vice President (Academic), or by Senate Executive.

Sanctions may include but are not limited to completion of a remediation process, a written reprimand, assignment of a failing grade, withdrawal from a course, suspension from a program, suspension or expulsion from the university.

Please see http://carleton.ca/studentaffairs/academic-integrity/ for more information.

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 ap-

plicable). Requests made within two weeks will be reviewed on a case-by-case basis. After requesting accommodation from PMC, meet with me to ensure accommodation arrangements are made. Please consult the PMC website (www.carleton.ca/pmc) for the deadline to request accommodations for the formally-scheduled exam (if applicable).

Religious Obligations

Carleton University accommodates students who, due to religious obligation, must miss an examination, test, assignment deadline, laboratory, or other compulsory event. The University has a Senate-approved policy on religious accommodation that forms part of its Human Rights Policy, available at: http://www.carleton.ca/equity/

Accommodation will be worked out directly and on an individual basis between the student and the instructor(s) involved. Students should make a formal written request to the instructor(s) for alternative dates and/or means of satisfying requirements. Such requests should be made during the first two weeks of any given academic term, or as soon as possible after a need for accommodation is known to exist, but in no case later than the penultimate week of classes in that term.

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: http://www.carleton.ca/equity/

Medical Certificate

The following is a link to the official medical certificate accepted by Carleton University for the deferral of final examinations or assignments in undergraduate courses. To access the form, please go to
http://www.carleton.ca/registrar/forms/
