COMP 4109A – Fall 2020

Applied Cryptography

Course Outline : Updated Version, Sept 2020

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 and Hemant

Course Information

Classroom : Wherever you are
Class Times : Tuesday & Thursday from 10:05am – 11:25pm
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 and COMP2402/SYSC2100.

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

It is assumed that you are familiar with run-time complexity (big O), basic algorithm analysis, basic probability and statistics, and modular arithmetic.

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

Learning Modality (Online Course)

In Fall 2020, this course will be completely online. Initially, classes will be live (using Zoom, BigBlueButton, or some other freely available platform) and held in the scheduled class times. A recording of the class will be posted to the course website within 24-hours of the class. As the semester progresses, some lectures may be pre-recorded and posted to the course website before the scheduled class. Class time, for lectures with pre-recorded and posted material, will then be used for working through examples, class discussions or Q&A.

Textbooks

The course does not have a mandatory textbook. However, some readings might be given from the following books (which are either free online or available electronically in the library)

- Everyday Cryptography – Fundamental Principles and Applications, 2nd ed. Keith Martin. (Available in library)
- Handbook of Applied Cryptography
  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

40%	:	Assignments & Challenges
20%	:	Project
20%	:	Tests (two in-class midterm tests; Thursday Oct 22nd & Thursday Nov 26th)
20%	:	Final Exam (Scheduled by the registrar's office)

Study Group Manager Option

If you choose to participate as a 1st year study group manager (details to appear on the course cuLearn page), your final grade will be determined as follows:

35%	:	Assignments & Challenges
20%	:	Project
20%	:	Tests (two in-class midterm tests; Oct 22nd & Nov 27th)
20%	:	Final Exam (Scheduled by the registrar's office)
5%	:	Study Group Manager
+5%	:	bonus marks for completing study group manager project

The bonus 5% to your final grade will be added for anyone that completes the study group manager project.

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/

Thur, Sep 10 COMP4109 First class

Thur, Oct 22 Midterm 1

Oct 26-30 No classes (Fall break)

Thur, Nov 27 Midterm 2

Tue, Dec 9 COMP 4109 Last class

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 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/.

Academic Integrity and the Faculty of Science

Please see https://science.carleton.ca/academic-integrity/. In particular, take note the following standard penalties for violations of Carleton's Policy on Academic Integrity:

- First offence, first-year students (< 4.0 credits completed): No credit for assessment(s) in question, or a final grade reduction of one full letter grade (e.g., A- becomes B-), whichever is a greater reduction
- First offence (anyone else): A grade of F in the course
- Second offence (anyone): A grade of F in the course and a one-term suspension from studies
- Third offence: Expulsion from the University

Academic Accommodations

Requests for Academic Accommodation

You may need special arrangements to meet your academic obligations during the term. For an accommodation request, the processes are as follows:

Pregnancy obligation

Please contact your instructor 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: carleton.ca/equity/wp-content/uploads/Student-Guide-to-Academic-Accommodation.pdf

Survivors of Sexual Violence

As a community, Carleton University is committed to maintaining a positive learning, working and living environment where sexual violence will not be tolerated, and is survivors are supported through academic accommodations as per Carleton's Sexual Violence Policy. For more information about the services available at the university and to obtain information about sexual violence and/or support, visit: carleton.ca/sexual-violence-support

Academic Accommodations for Students with Disabilities

If you have a documented disability requiring academic accommodations in this course, please contact the Paul Menton Centre for Students with Disabilities (PMC) at 613-520-6608 or pmc@carleton.ca for a formal evaluation or contact your PMC coordinator to send your instructor your Letter of Accommodation at the beginning of the term. You must also contact the PMC no later than two weeks before the first

in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, meet with your instructor as soon as possible to ensure accommodation arrangements are made. See carleton.ca/pmc

Religious obligation

Please contact your instructor 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: carleton.ca/equity/wp-content/uploads/Student-Guide-to-Academic-Accommodation.pdf

Accommodation for Student Activities

Carleton University recognizes the substantial benefits, both to the individual student and for the university, that result from a student participating in activities beyond the classroom experience. Reasonable accommodation must be provided to students who compete or perform at the national or international level. Please contact your instructor 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.
carleton.ca/senate/wp-content/uploads/Accommodation-for-Student-Activities-1.pdf

For more information on academic accommodation, please contact the departmental administrator or visit: students.carleton.ca/course-outline

---