COMP 4109 (Winter 2021)

Applied Cryptography

Page last updated: Jan 9, 2021.

People

- Instructor: David Barrera (davidbarrera@cunet)
- TAs: Kevin Guy (kevinguy@cmail), Yusef Karim (yusefkarim@cmail)

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). Students should be familiar with run-time complexity (big O), basic algorithm analysis, basic probability and statistics, and modular arithmetic. The course involves some mathematics. This course involves some programming.

Learning Modality

The course will be *delivered entirely online and asynchronously.* Class lecture videos and slide decks will be posted weekly to cuLearn along with a quiz and (when applicable) a crypto programming challenge. Students are expected to complete the quiz and challenge prior to the next quiz/challenge being posted (typically within 1 week).

Class time (Mondays/Wednesdays 8:35 - 9:55) will be used to provide office hours, present additional examples, and review the solutions to the programming challenges. Mondays will typically be reserved for reviewing theory content with the instructor, while Wednesdays will be focused on working through crypto challenges with the TAs. Attendance to these sessions is not mandatory, but encouraged.

A Discord server will also be available for asynchronous support. Details to be posted on cuLearn.

Grading Scheme

- 40% Quizzes
- 40% Crypto challenges
- 20% Group project (details to be posted on cuLearn)
  - 30% Project proposal (due February 10)
  - 60% Project implementation (due April 7)
  - 10% Video demo (due April 7)

Late submission policy: All deliverables (incl. quizzes, challenges, project components and any other deliverable not listed above) will be penalized 10% of the grade for that deliverable per day late. If you require an extension, contact the instructor.

Textbook

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)

- Keith Martin - Everyday Cryptography – Fundamental Principles and Applications
- A.J. Menezes, P.C. van Oorschot and S.A. Vanstone - Handbook of Applied Cryptography

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/equivalences, 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 Writing Tutorial Services.

SCS Computer Laboratory

SCS students can access one of the designated labs for your course. The lab schedule can be found at:https://carleton.ca/scs/tech-support/computer-laboratories/. All SCS computer lab and technical support information can be found at: https://carleton.ca/scs/technical-support/. Technical support is available in room HP5161 Monday to Friday from 9:00 until 17:00 or by emailing support@scs.carleton.ca.

University Policies

Student Academic Integrity Policy. 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. As defined by Senate, "plagiarism is presenting, whether intentional or not, the ideas, expression of ideas or work of others as one's own". Reported offences will be reviewed by the office of the Dean of Science. Penalties for violations of Carleton's Policy on Academic Integrity will normally be applied as follows:

- 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

Note: While these are the standard penalties, more severe penalties may be applied when warranted.

Unauthorized Co-operation or Collaboration. Senate policy states that "to ensure fairness and equity in assessment of term work, students shall not co-operate or collaborate in the completion of an academic assignment, in whole or in part, when the instructor has indicated that the assignment is to be completed on an individual basis". Please refer to the course outline statement or the instructor concerning this issue.

Academic Accommodations for 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 your course instructor 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 applicable). After requesting accommodation from PMC, meet with your course instructor to ensure accommodation arrangements are made. Please consult the PMC website for the deadline to request accommodations for the formally-scheduled exam (if applicable) at http://www2.carleton.ca/pmc/new-and-current-students/dates-and-deadlines

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. More information can be found here.

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 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

Religious Obligation: Write to the course 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: http://www2.carleton.ca/equity/

Pregnancy Obligation: Write to the course 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: http://www2.carleton.ca/equity/

Medical Certificate: The official medical certificate (form) accepted by Carleton University for the deferral of final examinations or assignments in undergraduate courses can be accessed from: http://www.carleton.ca/registrar/forms