COMP 3109A - Winter 2023

Applied Cryptography and Authentication

Course Outline : Preliminary Version, January 2,2022

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 (he/him)
Teaching Assistants : tba

Course Information

Classroom : Loeb C264
Class Times : Tuesday & Thursday from 1:05pm - 2:25pm
Course Website : Brightspace and Discord

Calendar Description

Practical aspects of cryptography. Topics include: stream and block ciphers; modes of operation; hash functions; message and user authentication; authenticated key establishment protocols; random number generation; entropy; proof of knowledge; secret sharing; key distribution; pitfalls deploying public-key encryption and digital signatures.

Learning Objectives

To gain an appreciation and understanding that (i) good crypto is not easy to create, (ii) developing your own crypto for use in real products is not a good idea, and (iii) it is the misuse of cryptographic tools, not the crypto itself, that create security weaknesses.

Prerequisites

COMP2804 and COMP2402/SYSC2100.

Precludes additional credit for COMP 4109 and COMP 4103 (both 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. This course will involve using some cryptographic libraries for some of the coding.

Learning Modality

This is an in-person course. Classes will be held, in-person, in the scheduled room and time. Midterm exams will be written during class time in the scheduled classroom. Some classes *might* be recorded and posted afterwards in Brightspace. Some recordings of some topics from some past semesters *might* be posted[1].

In the event of an instructor illness, classes will either move online (via zoom) or recorded lectures will be posted to Brightspace.

[1] There is no guarantee that all topics and all classes will be posted in video form.

Midterms will be (hand) written during class time.

There will be a discord server for the class. This will be used as the class forum as well as for office hours. Brightspace will be used for posting content, making announcements, and holding marks. Gradescope will be used for assignment submissions.

Textbooks

Any required reading will come from **freely available** content and will likely come from the following:

- **Computer Security and the Internet: Tools and Jewels**.
  Paul C. van Oorschot. 2020, Springer (https://people.scs.carleton.ca/~paulv/toolsjewels.html)
  Note: this is also the textbook for COMP 4108

- **Handbook of Applied Cryptography**
  A. J. Menezes, P. C. van Oorschot and S. A. Vanstone. 1996, CRC Press. (link)

Evaluation

60%	:	Assignments & Challenges
20%	:	Tests (two in-class midterm tests; Thursday February 16 & Thursday March 23)
20%	:	Final Exam (Scheduled by the registrar's office)

Note: To receive an A+ in the course, you must receive at least an 80% in each of the three grade components.

Note: If you do not receive at least an A- (80%) in each of the three grade components and your calculated final grade is above 90% then you will receive a final grade of A.

Note: There will be a computational aspect to some of the assignment problems and all challenges. That is, you will be required to write code to solve some assignment problems, all challenges and perhaps your project.

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. You are free to use whatever too you wish and not need to use LaTeX. Alternatives, such as troff, Google docs, MS Word, etc., are all acceptable. As long as the output (pdf) looks good to the reader it is fine.

Important Dates

See the University Calendar for all important dates:
https://carleton.ca/registrar/registration/dates/academic-dates/#sect3

Collaboration Policy

Assignments: work may be done individually or in pairs. Detailed instructions for submitting when you work in a pair will be given in the assignment specifications.

Challenges/Midterms/Final Exam: must be done individually. 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 may look for plagiarism in both written solutions and in your submitted code.

Undergraduate Academic Advisor

The Undergraduate Advisors for the School of Computer Science are available in Room 5302C HP, by telephone at 520-2600, ext. 4364 or by email at scs.ug.advisor@cunet.carleton.ca.

The undergraduate advisors can assist with information about prerequisites and preclusions, course substitutions/equivalencies, understanding your academic audit and the remaining requirements for graduation. The undergraduate advisors 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 https://carleton.ca/registrar/academic-integrity/.

Academic Integrity and the Faculty of Science

Please see https://science.carleton.ca/academic-integrity/.

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:
https://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 the website:
https://carleton.ca/equity/focus/sexual-violence-prevention-survivor-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 https://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: https://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.
https://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: https://students.carleton.ca/course-outline

---

COVID

In place of a doctor's note or medical certificate, students are advised to complete the self-declaration form available on the Registrar's Office website to request academic accommodation for missed course work including exams and assignments. Students will also be encouraged to connect directly with their instructors to discuss required accommodations arising from the COVID-19 situation.

https://carleton.ca/registrar/cu-files/covid-19-self-declaration-form/