COMP 2108 for Winter 2024 (Preliminary Version)

Applied Cryptography and Authentication

Course Information

Instructor: Jason Hinek
Contact: jasonhinek@cunet.carleton.ca

Class Times: Tuesdays & Thursdays, 4:05 - 5:35 (online)
Course Website: Brightspace/Discord

ONLINE COMBINED SYNCHRONOUS/ ASYNCHRONOUS. In-term assessments (midterm and final exams) will be held in person. Students must write the midterm exams on the dates and times that appear in the course outline. Midterms will be in-person or online using the distance exam service through Scheduling and Examination Services (for a fee), see https://carleton.ca/ses/distance-exams/

Teaching Assistants

Rebecca, Robert and Sam.

Contact/office hours information will be posted once the course starts.

Course 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.

Prerequisites

COMP 1406 with a minimum grade of C-, and COMP 2804.
Precludes additional credit for COMP 3109 (no longer offered), COMP 4109 (no longer offered).
(Note: This course will require some programming in Python.)

Required Textbook(s) and Other Resources

Any required or supplemental readings will come from freely available content and will mostly come from the following:

- *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin*
Paul C. van Oorschot. 2021, Springer (https://people.scs.carleton.ca/~paulv/toolsjewels.html)
Note: this is also the textbook for COMP 4108

- *Handbook of Applied Cryptography*
Alfred. J. Menezes, Paul. C. van Oorschot and Scott. A. Vanstone. 1996, CRC Press.
(https://cacr.uwaterloo.ca/hac/)

Learning Outcomes

Generally speaking, students should gain an appreciation and understanding that:

- Good cryptography is not easy to create.
- Developing your own cryptography for use in real products is not a good idea.
- It is the misuse of cryptographic tools, not the cryptography itself, that create security weaknesses.

More specifically, after taking this course, students should be able to:

- Compare and contrast encryption schemes (e.g., symmetric vs. asymmetric) and modes of operation as well as identify use cases for each scheme.
- Explain, in their own words, the differences between cryptographic hash functions, message authentication codes, digital signatures, and other cryptographic primitives, and determine which is an appropriate tool for different situations.
- Have an understanding of secure user authentication infrastructure, including the use of passwords and multifactor authentication, secure credential storage and management.
- Analyze cryptographic exchanges between systems to determine what security properties are afforded by the communication channel.
- Use cryptographic libraries correctly in working applications.

Learning Modality

Midterm exams and final exam must be written in-person. All lectures will be recorded (either live during class time or pre-recorded) and posted in Brightspace. Office hours will be a mix of in-person and online (discord). Some classes will be live lectures. Some classes might be interactive sessions to discuss content from previously posted lecture material. Some classes might be TA-run. If there is interest, there might be some in-person classes (during class time) that will be live-streamed via Zoom and recorded.

Assessment Scheme

Grades for this course will be determined as follows:

- 10% Weekly Quizzes (online). [Q]
- 50% Assignments and Challenges [A&C]
- 20% Two midterm exams (in-person written tests) [M1&M2]
- 20% Final exam (in-person written exam) [FE]

In order to pass the course,

- Your Assignments and Challenges grade must be at least 25/50.
- Your combined exams grade (M1&M2&FE) must be at least 20/40.

In order to receive an A+ in the course,

- Your Assignments and Challenges grade must be at least 40/50.
- Your combined midterm exams grade must be at least 16/20.
- Your final exam grade must be at least 16/20.

Quizzes: Short Brightspace quizzes to ensure students are keeping up with the course content.

Assignments: There will be several assignments. We will use Gradescope for assignment submissions. Assignments are to be done individually unless the specification indicates otherwise (in which case, students may work in groups of two).

Challenges: There will be several challenges. There is a computational aspect to all challenges (i.e., programming needed). Challenges will be submitted to Gradescope (or other places).

New for Winter 2025: For every Assignment and Challenge, a random set of students will be selected to meet with TAs or the instructor to discuss their solution. Selected students must demonstrate an understanding of their submissions (either code or written solutions), as well as be able to talk through alternative solutions. Failure to do so convincingly will result in losing up to the full marks for that assignment or challenge.

Midterm Exams: Two in-person midterm exams during class time. These are closed book exams. The dates for the midterm exams will be

- Tuesday, February 13th
- Tuesdsay, March 26th

Location of the midterm exams will be posted in Brightspace (when a room is booked).

Final Exam: In-person final exam scheduled by the registrar's office. Do NOT make travel plans before the final exam schedule is posted.

Academic Integrity

<TL;DR> Don't cheat.

This course has no group component, unless otherwise specified, and so all deliverables should be completed and submitted individually. Unless it is explicitly stated otherwise, the use of any A.I. systems will be considered academic misconduct. This includes, but is not limited to, chatbots (e.g., ChatGPT, Google Bard, Bing Chart), research assistants (e.g., Elicit), and image generators (e.g., Stable Diffusion, Dall-E), etc. Note that the above rule does not hold for automated grammar and punctuation checking tools (such as Grammarly).

To help enforce this policy, students may be randomly selected after each deliverable (Assignment or Challenge) to explain their code to the TAs/instructor in a one-on-one session.

In addition, sharing assignment, challenge, quiz, midterm or final exam specifications or posting them online (to sites like Chegg, CourseHero, OneClass, etc.) is ALWAYS considered academic misconduct. You are NEVER permitted to post, share, or upload course materials without explicit permission from your instructor

For more information about academic integrity please see https://science.carleton.ca/students/academic-integrity/

Important Dates

See the University Calendar for all important dates: https://carleton.ca/registrar/registration/dates/academic-dates/#sect4

Undergraduate Academic Advisors

The Undergraduate Advisors for the School of Computer Science are available in Room 5302HP; 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 Writing Tutorial Services.

SCS Computer Laboratory

Students taking a COMP course can access the SCS computer labs. The lab schedule and location 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/tech-support/. Technical support staff may be contacted in-person or virtually, see this page for details: https://carleton.ca/scs/tech-support/contact-it-support/.

University Policies:

Academic Accommodations

Carleton is committed to providing academic accessibility for all individuals. Please review the academic accommodation available to students here: https://students.carleton.ca/course-outline/.

Academic Integrity

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 sanctioned with penalties which range from a reprimand to receiving a grade of F in the course, or even being suspended or expelled from the University. Examples of punishable offences include plagiarism and unauthorized collaboration. Any such reported offences will be reviewed by the office of the Dean of Science. More information on this policy may be found on the ODS Academic Integrity page: https://carleton.ca/registrar/academic-integrity/.

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". Such reported offences will be reviewed by the office of the Dean of Science. More information and standard sanction guidelines can be found here: https://science.carleton.ca/students/academic-integrity/.

Unauthorized 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".

Carleton University acknowledges the location of its campus on the traditional, unceded territories of the Algonquin nation. In doing so, Carleton acknowledges it has a responsibility to the Algonquin people and a responsibility to adhere to Algonquin cultural protocols.