COMP 2108 (Winter 2025)

Applied Cryptography and Authentication

Last updated: Dec 29, 2024.

People

- Instructor: Nicholas Rivard (NicholasRivard@cunet.carleton.ca)
- Teaching Assistants:
  - Timothy Dao (TimothyDao@cmail.carleton.ca)
  - Brandon Le (BrandonLe4@cmail.carleton.ca)
  - Nickolas Zamachnoi (NICKOLASZAMACHNOI@cmail.carleton.ca)
  - Ahmad Alkfri (AHMADALKFRI@cmail.carleton.ca)

- Office hours:
  - Instructor: Via Zoom by appointment
  - TAs: Thursdays during class time

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

Renumbered from COMP 3109. New prerequisites are (COMP 1006 or COMP 1406 or SYSC 2004) with a minimum grade of C-, and COMP 2804. Precludes additional credit for COMP 3109 (no longer offered) and COMP 4109 (no longer offered). COMP 2108 is new prerequisite for COMP 4108. See 2024-25 Undergraduate Calendar.

This course involves programming in Python.

Learning Outcomes

After taking this course, students will 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 in what situations to use each one.

- Design 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 modern cryptographic libraries correctly in working applications.

Learning Modality

Flipped classroom. Lectures for the following week's content will be video-recorded and posted to Brightspace on Thursdays. Students are asked to allocate time to watch the lectures and review supporting materials (slides, book chapters, source code, etc.) prior to the in-person sessions on Tuesdays and Thursdays (16:05 - 17:25). In-person class time will be used as follows:

- **Tuesdays** - interactive sessions where the instructor assigns questions/problems sets for students to solve (sometimes in groups) and discuss together. These problems are designed to deepen understanding of the material, as well as help clarify concepts presented in the video lectures. Note that the instructor will not lecture during this time, nor is the aim of the session to recap the week's lecture. TAs will take notes of salient discussions and clarifications, and post them to Brightspace after the session for those who are unable to attend. These sessions are intended to support students who have questions or need assistance with the week's material. Attendance is not mandatory.
- **Thursdays** - TA-run sessions where students receive support for crypto challenges or any other practical aspect in the course. Later in the term, sessions may be used to review solutions to earlier crypto challenges. These sessions are designed to be hands-on, so students who attend are asked to bring their laptops and in-progress assignments.

Our goal is to ensure that students feel safe and supported throughout the term, so this course has been designed to support all students, including those who are unable to come to campus. All assessment material is available to review remotely, office hours and TA support is available through Discord, email or video meetings, and properly justified extensions are generally granted. Students, however, must ensure they are on campus for the two in-person assessments (midterm and final).

Grading Scheme

- 10% Weekly quizzes
- 25% Crypto challenges
- 30% Midterm
- 35% Final exam

Quizzes

To ensure students are keeping up with the lectures, quizzes will be posted (approximately) weekly to Brightspace. These quizzes are short, mostly multiple choice, and must be completed before the following week's quiz is made available. Quizzes may only be attempted once, and have a time-limit once started. Please monitor the course calendar closely to ensure you complete your quizzes on time. PMC student should notify the prof ASAP to ensure they are given the correct completion time overrides.

Crypto challenges

Approximately every 2 weeks, a new crypto challenge will be assigned for students to solve independently. These challenges are designed to help students experiment with practical applications of the theory taught in the course. Solutions will be due before the next challenge is made available, which is typically within 2-3 weeks. This pacing should give students at least 2 TA support sessions (Thursdays) to attend, if needed.

For every deliverable, 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 the code they have written, 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 challenge.

Midterm and final exam

The two exams are written on pen and paper, in person on campus on the specified date. The midterm covers all material (including articles, videos, book chapters, quizzes, and challenges) reviewed up to the examination date. The final primarily covers the period between the midterm and the end of the course, but requires a cursory review of the midterm content.

Individual work: This course has no group component, and thus 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. To help enforce this policy, students will be randomly selected after each deliverable to explain their code to the TAs/instructor in a one-on-one session. Please see the policy on unauthorized collaboration below.

Late submission policy: All deliverables (incl. quizzes, challenges, project components and any other deliverable not listed above) will be penalized 10% of the maximum grade for that deliverable per day late. For example, if a challenge solution worth 30 points is submitted 6 hours late, the maximum possible grade for that assignment would be 27/30. If you require an extension, contact the instructor to avoid losing marks.

Textbook

The textbook for the course is Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin by P.C. van Oorschot (2021, second edition, Springer). Available in hardcopy from bookstores, softcopy via university library, PDFs for personal use from author's website. Chapters 1, 2, 3, 4 and 8 will be used as reference material for the course.

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.

Academic Integrity violations within the Faculty of Science

Students found in violation of the Student Academic Integrity Policy (below) in Computer Science (COMP) courses are subject to severe penalties, as detailed at the Office of the Dean of Science (ODS) page: https://science.carleton.ca/academic-integrity. If you are unsure of the expectations regarding academic integrity (how to use and cite references, how much collaboration with lab- or class-mates is appropriate), ASK your instructor or the head TA for your labs. Sharing assignment or quiz specifications or posting them online (to sites such as Chegg, CourseHero, OneClass) is considered academic misconduct. You are never permitted to post, share, or upload course materials without explicit permission from your instructor.

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

Academic Accommodations. Carleton is committed to providing academic accessibility for all individuals. Please review the academic accommodation available to students here.

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.

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”.