COMP 2018 A – Fall 2025

Applied Cryptography & Authentication

COMP 2108 A – Fall 2024 (Preliminary Version)
School of Computer Science, Carleton University

Course Information

Instructor: Jason Hinek (he/him)
Office Location: HP5332 (Herzberg Building)
Email: jason <dot> hinek <at> carleton <dot>ca

Class Times: Monday & Wednesday
10:05am-11:25am

Course Website: See Brightspace

Teaching Modality

This is an in-person class. Classes, midterm exams, and the final exam are all held in-person (see Carleton Central for class location; final exam will be set by the Registrar's office).

COMP 2108 [0.5 credit]

Applied Cryptography and Authentication

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.
Includes: Experiential Learning Activity
Precludes additional credit for COMP 3109 (no longer offered), COMP 4109 (no longer offered), CSEC 2108.
Prerequisite(s): (COMP 1006 or COMP 1406) with a minimum grade of C-, and COMP 2804.
Lectures three hours a week.

Note: Some classes may be held online using Zoom (live or pre-recorded videos) in special circumstances (such as instructor illness or inclement weather).

Teaching Assistants

Contact information and office hour information will be posted in Brightspcace once the course starts.

Land Acknowledgement

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.

Note: This course will require some programming in Python (and perhaps Java).

Learning Outcomes

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.

At a high level, 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 usually not a good idea.
- It is the misuse of cryptographic tools, not the cryptography itself, that creates security weaknesses.

Required Textbook(s) and Other Resources

Required textbook:
- *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin.* Paul C. van Oorschot. 2021, Springer.

The book can be purchased at the bookstore ($102.50), accessed electronically through the library (free), or can be downloaded (by individual chapters) for free on the author's website (https://people.scs.carleton.ca/~paulv/toolsjewels.html).

Note: this is also the textbook for COMP 4108.

Other assigned readings will come from freely available material (from the Internet) and specified during the semester.

Assessment Scheme

Grades for this course will be determined as follows:

- 60% Assignments and Challenges [A&C]
- 20% Midterm Tests (in-person written tests) [M1&M2]
- 20% Final exam (in-person written exam) [F]

In order to pass the course,
- Your Assignments and Challenges grade must be at least 30/60.
- Your combined test grades (M1&M2&F) must be at least 20/40.

In order to receive an A+ in the course,
- Your Assignments and Challenges grade must be at least 48/60.
- Your combined midterm exams grade must be at least 16/20.
- Your final exam grade must be at least 16/20.

Midterm Exams: Two in-person midterm exams during class time. These are closed book exams. The dates for the midterm exams will be
- Wednesday, October 8th
- Wednesday, November 12th

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

Assignments: There will be several assignments. Assignments are to be done individually unless the specification indicates otherwise (in which case, students may work in groups of two). Details and dates will be given at the start of the course.

Challenges: There will be several challenges. There is a computational aspect to all challenges (i.e., programming needed). Challenges can be submitted as many times as desired before the deadline and will be graded electronically. Details and dates will be given at the start of the course.

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

Important Dates

See the University Calendar for all important dates:
https://students.carleton.ca/academic-dates/

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, etc.), research assistants (e.g., Elicit), and image generators (e.g., Stable Diffusion, Dall-E, etc.), 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/work 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/

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 Laptop Requirement

Every student that has been enrolled in a 1000-level (i.e., first year) course offered by the School of Computer Science after the 2020/2021 school year is required to have a laptop. This includes COMP1001, COMP1005, and COMP1006. For more information, please visit https://carleton.ca/scs/scs-laptop-requirement/ and then review the requirements at https://carleton.ca/scs/scs-laptop-requirement/laptop-specs/.

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".