COMP 2108A (Fall 2026)

Applied Cryptography and Authentication

Instructor: David Barrera
Class location: No assigned classroom (online course)
Email: davidbarrera@cunet.carleton.ca
Office location: HP 5131
Best ways to be in touch: via email
Teaching Assistant: A list of teaching assistants and their contact/office hours information will be posted on Brightspace once the course starts.
Tutorial times: No tutorials
Course website: Brightspace

Important dates and deadlines can be found here: Dates, Deadlines, and Regulations—Registrar's Office, including class suspension for fall, winter breaks, and statutory holidays.

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.

- Precludes: 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.

Learning Material(s) and Other Course/Lab-Related Resources

Computer Security and the Internet: *Tools and Jewels from Malware to Bitcoin*, Second Edition
by Paul C. van Oorschot. Springer, Oct 2021.
2e ISBN: 978-3-030-83410-4 (hardcopy), 978-3-030-83411-1 (eBook)
The official version is available from Springer (2e) and major booksellers.
All official hardback copies (1e and 2e) should have color figures and color highlighted text.
A single-file full-book PDF is **available from university libraries** and SpringerLink (2e).

Topics Covered and Learning Outcomes

Week	Topic/Content
1	Computer security goals, hash functions, randomness
2	Authentication 1
3	Authentication 2
4	Symmetric cryptography basics

5	Encryption modes of operation
6	Midterm
7	Reading week
8	Public key cryptography basics
9	Message authentication codes
10	Authentication protocols
11	Key exchange
12	Public key infrastructure
13	Trust models and web browser cryptography

After completing 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.

Course Delivery

This is an unscheduled fully online course. Every week, students will be asked to independently read specific book sections and articles. It is the student's responsibility to complete these readings in a timely manner. The instructor will post accompanying short videos and slides for certain content known to be challenging. Content will be released on Brightspace on a weekly basis and will remain available until the final exam date.

Assessment Scheme

Grade Breakdown

Please check Brightspace for up-to-date submission deadlines

COMPONENT	GRADE VALUE	DUE DATE
Assignment 0	0 % Required to unlock grading for Assignments 1–4	Sep 20
Assignment 1	5 %	Oct 11
Assignment 2	5 %	Nov 1
Assignment 3	5 %	Nov 22
Assignment 4	5 %	Dec 6
Midterm	35 %	TBD (On Week 6)[1]
Final Exam	45 %	TBD, scheduled by University

[1]The midterm will tentatively be scheduled for Week 6, outside of regular class time. The possible dates are ~~October 23~~ October 16 (Friday) evening, anytime on ~~October 24~~ October 17 (Saturday), or ~~October 25~~ October 18 (Sunday). Once Scheduling and Examination Services confirms the date, we will inform you.

Assignments
Assignments (also referred to as "cryptographic challenges") are designed to help students individually experiment with practical applications of the theory taught in the course. Solutions thus require programming in Python, either locally or on an SCS OpenStack VM. Students are required to submit both the solution and the source code that generated the solution. Solutions without accompanying source code will be given 0 marks. Completion of assignment 0 is necessary to receive marks for assignment 1-4.

Individual work and unauthorized collaboration
All coursework is to be completed individually and without the use of AI. Assignments will be checked against other submission to detect similar/duplicate submissions. The instructor and TAs may ask students for clarification on how specific results were obtained. Failure to provide convincing evidence of understanding a student's own assignment may result in lost marks either partial or full. Unauthorized collaboration or use of AI will be sent to the office of the Dean of Science for further review of potential academic misconduct. If in doubt, please contact the instructor or TAs to ask about your specific situation.

Midterm and Final Exam
The two exams will be written on pen and paper, in person on campus on the specified date. Both exams are closed-book and primarily short answer questions along with some multiple choice. The midterm covers all material (including articles, videos, book chapters, and assignments) reviewed up to the examination date. The final exam is cumulative, covering all material posted to Brightspace.

If you miss the *midterm exam*, or if your midterm grade (as a percentage) is lower than your final exam grade (as a percentage), your final exam grade will be used as your grade for both the midterm and the final exam. Deferrals for the midterm exams will typically not be granted. This substitution does not apply to the final exam; students who miss the final exam remain subject to Carleton's deferred exam policy and the oral exam provision below. If your midterm percentage grade is higher than the final exam percentage grade, your grade will be computed as described in the table above.

Deferrals of the *final exam* will be accommodated in accordance with Carleton's deferred exam policy. To maintain academic integrity in cases where significant time has passed since the original exam date, or where exam content may have circulated, the instructor reserves the right to administer the deferred exam as an oral examination rather than a written one. (This provision does not apply where it would conflict with a student's registered academic accommodation.) An oral deferred exam will cover the same topics and be held to the same grading standard as the original written exam, and will typically run 30–45 minutes. Students will be given advanced notice of the format.

Use of AI during exams: All exams are expected to be completed individually, and without electronic aid; any communication or access of electronic devices (e.g. cellphones) during the test will be considered cheating. Use of Smart Glasses (or other similar assistive technologies) before or during a test is strictly prohibited and is considered an academic integrity violation. Even if you have prescription glasses with assistive technologies, you will not be allowed to use them during the test, so please make sure that you have acceptable prescription glasses. The proctor has the right to ask to inspect your glasses before or during the test. In addition, unless authorized with PMC accommodations, you are NOT allowed to use headphones nor ear buds during a test. Also, during a test, if you choose to wear a baseball cap, sunglasses or anything else that would prevent a proctor from monitoring where your eyes are focused during the test, you will likely be asked by a proctor to move to a different seat. Lastly, you must submit your test before leaving the classroom or it won't be graded.

Late Submission Policy

All deliverables will be penalized 10% of the maximum grade for that deliverable per day late, up to 10 days max. 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.

School of Computer Science Laptop Requirement (only applies to on-campus courses)

Every student that has been enrolled in a 1000-level (i.e., first year) course offered 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/.

Undergraduate Academic Advisors (only for UG course)

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/.

Mental Health and Wellness

The Carleton Wellness Website is a wonderful resource link to include in the course outline for students.

Academic Accommodations and Regulations

Academic Accommodation

Carleton is committed to providing academic accessibility for all individuals. You may need special arrangements to meet your academic obligations during the term. The accommodation request processes are outlined on the Academic Accommodations website (https://students.carleton.ca/course-outline/).

Academic Integrity

Students are expected to uphold the values of academic Integrity, which include fairness, honesty, trust, and responsibility. Examples of actions that compromise these values include but are not limited to plagiarism, accessing unauthorized sites for assignments or tests, unauthorized collaboration on assignments or exams, and using artificial intelligence tools such as ChatGPT when your assessment instructions say it is not permitted.

Misconduct in scholarly activity will not be tolerated and will result in consequences as outlined in Carleton University's Academic Integrity Policy. A list of standard sanctions in the Faculty of Science can be found here.

Additional details about this process can be found on the Faculty of Science Academic Integrity website.

Students are expected to familiarize themselves with and abide by Carleton University's Academic Integrity Policy. Claiming ignorance of or confusion about the academic integrity standards as described in the Policy does not excuse a student from responsibility for violations of those standards."

Student Rights & Responsibilities

Students are expected to act responsibly and engage respectfully with other students and members of the Carleton and the broader community. See the 7 Rights and Responsibilities Policy for details regarding the expectations of non-academic behaviour of students. Those who participate with another student in the commission of an infraction of this Policy will also be held liable for their actions.