COMP 3109 (Fall 2022)

Applied Cryptography

Page last updated: Aug 30, 2022.

People

- Instructor: David Barrera (he/him/his) - davidbarrera@cunet.carleton.ca
- Teaching Assistants:
  - Kevin Guy (he/him/his) - kevinguy@cmail.carleton.ca
  - Srivathsan Morkonda (he/him/his) - srivathsanmorkonda@cmail.carleton.ca
  - Abdelrahman Soliman (he/him/his) - abdelrahmansoliman@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

COMP 2804 and (COMP 2402 or SYSC 2100). Precludes additional credit for COMP 4109 (no longer offered). Students should be familiar with run-time complexity (big O), basic algorithm analysis, basic probability and statistics, and modular arithmetic. The course involves some mathematics. This course involves programming.

Learning outcomes

After taking this course, students will be able to:

- Compare and contrast encryption schemes (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 several major modern cryptographic libraries correctly in working applications.

Learning Modality

This course has been explicitly re-designed so that those who are unable to attend campus can still obtain a passing grade. 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 generously granted. The only mandatory in-person assessment is the final exam. Our goal is to ensure that students feel safe and supported throughout the term.

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 (1:05pm-2:25pm). 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.

- **Thursdays** - TA-run sessions where students receive support for crypto challenges, final project, 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 required to bring their laptops and in-progress assignments.

Weekly in-person sessions are intended to support students who have questions or need assistance with the week's material. Attendance is not mandatory.

A Discord server will also be available for course discussion and asynchronous support. Details to be posted on Brightspace.

Grading Scheme

- 25% Weekly quizzes
- 25% Crypto challenges
- 25% Final project
- 25% Final exam

Quizzes

To ensure students are keeping up with the lectures, quizzes will be posted (almost) 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.

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. Challenge 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.

Final project

Students will build an application using a popular cryptographic library. The application will need to interact with a remote service by correctly following a cryptographic protocol specification. The final project will evaluate adherence to the specification and the program's robustness under a variety of protocol violations and edge cases. Full project details are available on Brightspace.

Final exam

The final exam will cover all theory topics as well as all practical aspects of the course. As of writing, the exam is scheduled to be in-person. This, however, may change to some form of online or alternative assessment if COVID-19 concerns are high.

Individual work: This course has no group component, and thus all deliverables should be completed and submitted individually. 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 recommended 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.

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

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 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. As defined by Senate, "plagiarism is presenting, whether intentional or not, the ideas, expression of ideas or work of others as one's own". Reported offences will be reviewed by the office of the Dean of Science. Penalties for violations of Carleton's Policy on Academic Integrity will normally be applied as follows:

- First offence, first-year students (< 4.0 credits completed): No credit for assessment(s) in question, or a final grade reduction of one full letter grade (e.g., A- becomes B-), whichever is a greater reduction.
- First offence (anyone else): A grade of F in the course
- Second offence (anyone): A grade of F in the course and a one-term suspension from studies
- Third offence: Expulsion from the University

Note: While these are the standard penalties, more severe penalties may be applied when warranted.

Unauthorized Co-operation or 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". Please refer to the course outline statement or the instructor concerning this issue.

Academic Accommodations for Students with Disabilities. The Paul Menton Centre for Students with Disabilities (PMC) provides services to students with Learning Disabilities (LD), psychiatric/mental health disabilities, Attention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorders (ASD), chronic medical conditions, and impairments in mobility, hearing, and vision. If you have a disability requiring academic accommodations in this course, please contact PMC at 613-520-6608 or pmc@carleton.ca for a formal evaluation. If you are already registered with the PMC, contact your PMC coordinator to send your course instructor your Letter of Accommodation at the beginning of the term, and 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 course instructor to ensure accommodation arrangements are made. Please consult the PMC website for the deadline to request accommodations for the formally-scheduled exam (if applicable) at http://www2.carleton.ca/pmc/new-and-current-students/dates-and-deadlines

Additional Accommodation. Carleton provides academic accommodation to students for reasons of disability, religious observance, pregnancy and/or parental leave, sexual violence, and student activities. Providing accommodations simply means providing alternatives to students who cannot perform the essential requirements of their academic programs due to the reasons mentioned above. At no time does academic accommodation undermine or compromise the learning objectives that are established by the academic authorities of the university. Full details can be found here

COVID-19

It is important to remember that COVID is still present in Ottawa. The situation can change at any time and the risks of new variants and outbreaks are very real. There are a number of actions you can take to lower your risk and the risk you pose to those around you including being vaccinated, wearing a mask, staying home when you're sick, washing your hands and maintaining proper respiratory and cough etiquette.

Feeling sick? Remaining vigilant and not attending work or school when sick or with symptoms is critically important. If you feel ill in any way do not come to class or campus. If you feel ill or exhibit symptoms while on campus or in class, please leave campus immediately. In all situations, you must follow Carleton's symptom reporting protocols.

Masks: Carleton strongly recommends masking when indoors, particularly if physical distancing cannot be maintained. The instructor and TAs have committed to wearing masks during all student interactions.

Vaccines: While proof of vaccination is no longer required as of May 1 to attend campus or in-person activity, it may become necessary for the University to bring back proof of vaccination requirements on short notice if the situation and public health advice changes. Students are strongly encouraged to get a full course of vaccination, including booster doses as soon as they are eligible, and submit their booster dose information in cuScreen as soon as possible.