UNIVERSITY OF CALGARY
FACULTY OF SCIENCE

Department of Computer Science
ICT 602
403 220-6015
cpsc@cpsc.ucalgary.ca

COURSE OUTLINE

1. **Course:** CPSC 418, Introduction to Cryptography - Winter 2021

   Lecture 01: MWF 14:00 - 14:50 - Online

Instructor	Email	Phone	Office	Hours
Dr. Renate Scheidler	rscheidl@ucalgary.ca	220-6628	MS 436	MF immediately after class or by appointment

Online Delivery Details:

Some aspects of this course are being offered in real-time via scheduled meeting times. For those aspects you are required to be online at the same time.

To help ensure Zoom sessions are private, do not share the Zoom link or password with others, or on any social media platforms. Zoom links and passwords are only intended for students registered in the course. Zoom recordings and materials presented in Zoom, including any teaching materials, must not be shared, distributed or published without the instructor's permission.

This course has a registrar scheduled, asynchronous final exam. The writing time is 3 hours + 0% buffer time, but the exam can be written any time in a 24-hour window.

Lectures delivered synchronously MWF 14:00-14:50 and recorded

Tutorials delivered synchronously M 16:00-16:50, W 15:00-15:50 weekly and W 18:00-18:50 as needed, and recorded

Course Site:

D2L: CPSC 418 L01-(Winter 2021)-Introduction to Cryptography

Note: Students must use their U of C account for all course correspondence.

Course web page: people.ucalgary.ca/~rscheidl/crypto

2. **Requisites:**

See section 3.5.C in the Faculty of Science section of the online Calendar.

Prerequisite(s):
Computer Science 331 and 3 units from Computer Science 351, Mathematics 271, 273, 315 or Pure Mathematics 315.

Antirequisite(s):
Credit for Computer Science 418 and any of Computer Science 429, 557, Mathematics 318, Pure Mathematics 329 or 418 will not be allowed.

Note(s):

a. Students who have credit for Computer Science 319 instead of Computer Science 331 should contact the department for instructions on how to enrol in this course.

3. **Grading:**

The University policy on grading and related matters is described in F.1 and F.2 of the online University Calendar.

In determining the overall grade in the course the following weights will be used:

Component(s)	Weighting %	Date
Assignments (3)	30	(Anticipated due dates: February 10, March 10, April 14)
Midterm Exam (1)	30	(Take-home, anticipated due date: March 17)
Final Exam	40	Registrar scheduled exam

Each piece of work (reports, assignments, quizzes, midterm exam(s) or final examination) submitted by the student will be assigned a grade. The student's grade for each component listed above will be combined with the indicated weights to produce an overall percentage for the course, which will be used to determine the course letter grade.

The conversion between a percentage grade and letter grade is as follows.

	A+	A	A-	B+	B	B-	C+	C	C-	D+	D
Minimum % Required	95 %	90 %	86 %	82%	78%	74 %	70 %	66%	62%	58 %	50 %

A passing grade in the final exam (at least 50%) is essential if the student is to pass the course as a whole (grade of C- or better).

This course will have a final exam that will be scheduled by the Registrar. The Final Examination Schedule will be published by the Registrar's Office approximately one month after the start of the term. The final exam for this course will be designed to be completed within 3 hours.

The final exam will be administered using an on-line platform. Per section G.5 of the online Academic Calendar, timed final exams administered using an on-line platform, such as D2L, will be available on the platform. Due to the scheduling of the final exams, the additional time will be added to **the end** of the registrar scheduled **synchronous** exam to support students. This way, your exam schedule accurately reflects the **start time** of the exam for any **synchronous** exams. E.g. If a **synchronous** exam is designed for 2 hours and the final exam is scheduled from 9-11am in your student centre, the additional time will be added to the **end** time of the **synchronous** exam. This means that if the exam has a 1 hour buffer time, a synchronous exam would start at 9 am and finish at 12pm. – **updated April 6, 2021**

- the latest you should start an asynchronous exam would be 8 am in order to be able to submit the exam at 11am and have the full 3 hours.

4. **Missed Components Of Term Work:**

The university has suspended the requirement for students to provide evidence for absences. Please do not attend medical clinics for medical notes or Commissioners for Oaths for statutory declarations.

In the event that a student legitimately fails to submit any online assessment on time (e.g. due to illness etc...), please contact the course coordinator, or the course instructor if this course does not have a coordinator to arrange for a re-adjustment of a submission date. Absences not reported within 48 hours will not be accommodated. If an excused absence is approved, then the percentage weight of the legitimately missed assignment could also be pro-rated among the components of the course.

5. **Scheduled Out-of-Class Activities:**

There are no scheduled out of class activities for this course.

6. **Course Materials:**

Recommended Textbook(s):

D. R. Stinson and M. B. Paterson, *Cryptography - Theory and Practice*: CRC 2019.

Additional course materials such as lecture slides, assignments, handouts and links to useful resources are available on the course website.

In order to successfully engage in their learning experiences at the University of Calgary, students taking online, remote and blended courses are required to have reliable access to the following technology:

- A computer with a supported operating system, as well as the latest security, and malware updates;
- A current and updated web browser;
- Webcam/Camera (built-in or external);
- Microphone and speaker (built-in or external), or headset with microphone;
- Current antivirus and/or firewall software enabled;
- Stable internet connection.

For more information please refer to the UofC ELearning online website.

7. **Examination Policy:**

   - Exam are open-book.
   - **All work must be done individually.**
   - Exams are designed to be no more than 3 hours in length.
   - Students will have 24 hours from the release date/time to complete the exam.

   Students should also read the Calendar, Section G, on Examinations.

8. **Approved Mandatory And Optional Course Supplemental Fees:**

   There are no mandatory or optional course supplemental fees for this course

9. **Writing Across The Curriculum Statement:**

   For all components of the course, in any written work, the quality of the student's writing (language, spelling, grammar, presentation etc.) can be a factor in the evaluation of the work. See also Section E.2 of the University Calendar.

10. **Human Studies Statement:**

    Students will not participate as subjects or researchers in human studies.

    See also Section E.5 of the University Calendar.

11. **Reappraisal Of Grades:**

    A student wishing a reappraisal, should first attempt to review the graded work with the Course coordinator/instructor or department offering the course. Students with sufficient academic grounds may request a reappraisal. Non-academic grounds are not relevant for grade reappraisals. Students should be aware that the grade being reappraised may be raised, lowered or remain the same. See Section I.3 of the University Calendar.

    a. **Term Work:** The student should present their rationale as effectively and as fully as possible to the Course coordinator/instructor within **ten business days** of either being notified about the mark, or of the item's return to the class. If the student is not satisfied with the outcome, the student shall submit the Reappraisal of Graded Term work form to the department in which the course is offered within 2 business days of receiving the decision from the instructor. The Department will arrange for a reappraisal of the work within the next ten business days. The reappraisal will only be considered if the student provides a detailed rationale that outlines where and for what reason an error is suspected. See sections I.1 and I.2 of the University Calendar

    b. **Final Exam:**The student shall submit the request to Enrolment Services. See Section I.3 of the University Calendar.

12. **Other Important Information For Students:**

    a. **Mental Health** The University of Calgary recognizes the pivotal role that student mental health plays in physical health, social connectedness and academic success, and aspires to create a caring and supportive campus community where individuals can freely talk about mental health and receive supports when needed. We encourage you to explore the mental health resources available throughout the university community, such as counselling, self-help resources, peer support or skills-building available through the SU Wellness Centre (Room 370, MacEwan Student Centre, Mental Health Services Website) and the Campus Mental Health Strategy website (Mental Health).

    b. **SU Wellness Services:** For more information, see www.ucalgary.ca/wellnesscentre or call 403-210-9355.

    c. **Sexual Violence:** The Sexual Violence Support Advocate, Carla Bertsch, can provide confidential support and information regarding sexual violence to all members of the university community. Carla can be reached by email (svsa@ucalgary.ca) or phone at 403-220-2208. The complete University of Calgary policy on sexual violence can be viewed at (https://www.ucalgary.ca/policies/files/policies/sexual-violence-policy.pdf)

    d. **Misconduct:** Academic integrity is the foundation of the development and acquisition of knowledge and is based on values of honesty, trust, responsibility, and respect. We expect members of our community to act with integrity. Research integrity, ethics, and principles of conduct are key to academic integrity. Members of our campus community are required to abide by our institutional Code of Conduct and promote academic integrity in upholding the University of Calgary's reputation of excellence. Some examples of academic misconduct include but are not limited to: posting course material to online platforms or file sharing without the course instructor's consent; submitting or presenting work as if it were the student's own work; submitting or presenting work in one course which has also been submitted in another course without the

instructor's permission; borrowing experimental values from others without the instructor's approval; falsification/fabrication of experimental values in a report. Please read the following to inform yourself more on academic integrity:

Student Handbook on Academic Integrity
Student Academic Misconduct Policy and Procedure
Research Integrity Policy

Additional information is available on the Student Success Centre Academic Integrity page

e. **Academic Accommodation Policy:** Students needing an accommodation because of a disability or medical condition should contact Student Accessibility Services in accordance with the procedure for accommodations for students with disabilities available at procedure-for-accommodations-for-students-with-disabilities.pdf.

Students needing an accommodation in relation to their coursework or to fulfill requirements for a graduate degree, based on a protected ground other than disability, should communicate this need, preferably in writing, to the Associate Head of the Department of Computer Science, Nelson Wong by email nelson@cpsc.ucalgary.ca or phone 403-210-8483. Religious accommodation requests relating to class, test or exam scheduling or absences must be submitted no later than **14 days** prior to the date in question. See Section E.4 of the University Calendar.

f. **Freedom of Information and Privacy:** This course is conducted in accordance with the Freedom of Information and Protection of Privacy Act (FOIPP). Students should identify themselves on all written work by placing their name on the front page and their ID number on each subsequent page. For more information, see Legal Services website.

g. **Student Union Information:** VP Academic, Phone: 403-220-3911 Email: suvpaca@ucalgary.ca. SU Faculty Rep., Phone: 403-220-3913 Email: sciencerep@su.ucalgary.ca. Student Ombudsman, Email: ombuds@ucalgary.ca.

h. **Surveys:** At the University of Calgary, feedback through the Universal Student Ratings of Instruction (USRI) survey and the Faculty of Science Teaching Feedback form provides valuable information to help with evaluating instruction, enhancing learning and teaching, and selecting courses. Your responses make a difference - please participate in these surveys.

i. **Copyright of Course Materials:** All course materials (including those posted on the course D2L site, a course website, or used in any teaching activity such as (but not limited to) examinations, quizzes, assignments, laboratory manuals, lecture slides or lecture materials and other course notes) are protected by law. These materials are for the sole use of students registered in this course and must not be redistributed. Sharing these materials with anyone else would be a breach of the terms and conditions governing student access to D2L, as well as a violation of the copyright in these materials, and may be pursued as a case of student academic or non-academic misconduct, in addition to any other remedies available at law.

Course Outcomes:

- Describe the different services that cryptography provides and give examples of cryptographic mechanisms that provide a given service.
- Verify that a cryptographic mechanism works properly, eg. that encryption followed by decryption is successful.
- Describe the different attack models covered in the course and how they relate to each other.
- Demonstrate competence with mathematical foundations of modern cryptographic primitives.
- Apply mathematics to assess the security of cryptographic primitives.
- Restate the main cryptographic protocols that are covered in the course and their different functions.
- Write software that provides cryptographic services and integrate existing cryptographic software libraries and packages in this software.

Electronically Approved - Dec 22 2020 11:50

Department Approval

Electronically Approved - Apr 07 2021 09:41

Associate Dean's Approval