UNIVERSITY OF CALGARY
FACULTY OF SCIENCE

Department of Mathematics & Statistics
MS 476
403 220-5210
math@ucalgary.ca

COURSE OUTLINE

1. **Course:** MATH 318, Introduction to Cryptography - Fall 2021

   Lecture 01: MWF 16:00 - 16:50 in ES 162

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

In Person Delivery Details:

Lectures will take place in-person. Technology permitting, lectures will be live-streamed via Zoom from the classroom and recorded. Students may attend in-person or online.

All U of C safety protocols and requirements are in effect for in-person instructional components at all times.

Re-Entry Protocol for Labs and Classrooms:

To limit the spread of COVID-19 on campus, the University of Calgary has implemented safety measures to ensure the campus is a safe and welcoming space for students, faculty and staff. The most current safety information for campus can be found here.

Course Site:

https://people.ucalgary.ca/~rscheidl/crypto/

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

2. **Requisites:**

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

Prerequisite(s):
Mathematics 211 or 213; and Mathematics 271 or 273.

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

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: October 7, November 4, December 8
Midterm Exam (1)	30	In-person, November 18, 19:15-20:45 pm
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 University of Calgary offers a flexible grade option, Credit Granted (CG) to support student's breadth of learning and student wellness. Faculty units may have additional requirements or restrictions for the use of the CG grade at the faculty, degree or program level. To see the full list of Faculty of Science courses where CG is not eligible, please visit the following website: https://science.ucalgary.ca/current-students/undergraduate/program-advising/flexible-grading-option-cg-grade

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, one possible arrangement is that the percentage weight of the legitimately missed assignment could also be pro-rated among the components of the course. This option is at the discretion of the coordinator and may not be a viable option based on the design of this course.

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

The following out of class activities are scheduled for this course.

Activity	Location	Date and Time	Duration
Midterm	On-Campus, room to be announced	Thursday, November 18, 2021 at 7:15 pm	1.5 Hours

REGULARLY SCHEDULED CLASSES HAVE PRECEDENCE OVER ANY OUT-OF-CLASS-TIME-ACTIVITY. If you have a conflict with the out-of-class-time-activity, please contact your course coordinator/instructor no later than **14 days prior** to the date of the out-of-class activity so that alternative arrangements may be made.

6. **Course Materials:**

Recommended Textbook(s):

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

Purchase of the textbook is entirely optional. Older editions of this textbook are obsolete and missing modern material. They should not be used.

Additional course materials such as lecture slides, tutorial materials, assignments, practice problem sets, 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:**

Examinations are conducted in-person and are closed-book. No aids of any kind are allowed on the midterm or the final 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/legal-services/sites/default/files/teams/1/Policies-Sexual-and-Gender-Based-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:**

It is the student's responsibility to request academic accommodations according to the University policies and procedures listed below. The student accommodation policy can be found at: https://www.ucalgary.ca/legal-services/sites/default/files/teams/1/Policies-Student-Accommodation-Policy.pdf

Students needing an accommodation because of a disability or medical condition should communicate this need to Student Accessibility Services in accordance with the Procedure for Accommodations for Students with Disabilities: https://www.ucalgary.ca/legal-services/sites/default/files/teams/1/Policies-Accommodation-for-Students-with-Disabilities-Procedure.pdf.

Students needing an accommodation in relation to their coursework or to fulfil requirements for a graduate degree, based on a Protected Ground other than Disability, should communicate this need, by filling out the Request for Academic Accommodation Form and sending it to Mark Bauer by email bauerm@ucalgary.ca preferably 10 business days before the due date of an assessment or scheduled absence.

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.
- Use mathematical reasoning to rigorously prove security properties of various cryptographic primitives.

Electronically Approved - Sep 08 2021 16:45

Department Approval

Electronically Approved - Sep 08 2021 16:48

Associate Dean's Approval