This version of the syllabus is a guideline for the course and does not superseded the officially posted one.

University of Alberta
CMPUT 496-A1 Cryptography for Digital Privacy
Fall 2025

Course Information

Instructor: Bailey Kacsmar
Office: UCOMM
E-mail: kacsmar@ualberta.ca
Instructor Office Hours: See Canvas
Lectures: See canvas or beartracks
TAs: Samuel Feldman and Sasha Dudiy
Teaching Assistant's Office Hours: TBA on Canvas

Course Communications: Important course information will generally be posted to **Canvas**, but may also be sent to your ualberta.ca email address. It is your responsibility to keep up with all course-related information. For personal matters, such as an illness, please email the instructor directly. We will only reply back to email from your ualberta.ca email address, following privacy rules.

Textbooks and Readings: There is no required textbook. Additional readings may be assigned; readings marked as mandatory contain required material for the course. You must read these mandatory readings.

Below are some recommended/supplemental materials you may find useful. The relevance will be discussed the first day of class.

- *Cryptography: Theory and Practice*, Douglas R. Stinson and Maura Paterson
- *Cryptography Made Simple (Information Security and Cryptography)*, Nigel Smart
- *A Pragmatic Introduction to Secure Multi-Party Computation* from Evans, Kolesnikov, and Rosulek.

Lecture Material: The slide decks will be posted at least 24 hours before class. Any recommended/required readings associated with this lecture will also be posted on Canvas. If a reading needs to be completed before a lecture, you will be notified the week before.

Course Description:

This course provides an introduction to data privacy and security, using cryptography and related techniques. It examines how data and meta-data can be protected at rest, in transit, and during computation. Students completing this course should be able to use and deploy data security and privacy protection technologies.

Prerequisites: CMPUT 272, CMPUT 204, MATH 125

Course Objectives and Expected Learning Outcomes:

By the end of this course students should be able to:

- Evaluate the use of cryptography to protect data assets for analysis and data science
- Analyze security and privacy threats to data assets across various use settings and while employing a range of data privacy mechanisms
- Compare various data security and privacy mechanisms and articulate their advantages and limitations, e.g., privacy-utility trade offs as well as risk calculations

Outline Below is an overview of topics within this course. At a high-level, we will cover three types of cryptographic techniques for digital privacy. Their security relies on either (i) computational guarantees, (ii) statistical guarantees, or (iii) information theoretic guarantees.

- Ethics/policy relevant to this course
- Basics of cryptography (CIA, adversarial thinking, cryptanalysis)
- Symmetric encryption
- Hash functions, MAC
- Public key encryption (RSA)
- Semantic security, etc.
- Secret Sharing
- Inference attacks (leakage from function output, background information, side channels)
- k-Anonymity, l-diversity, (t-plausibility)
- Differential privacy
- Local differential privacy (randomized response, etc.)
- Private machine learning (DP-SGD)
- Blockchains
- Homomorphic encryption
- MPC, PSI (commutative encryption)

Important Dates

- September 25th, 4pm MT, A1 due
- October 15th, in class, Midterm 1
- October 30th, 4pm MT, A2 due
- November 10-14th, reading week
- November 26th, in class, Midterm 2
- December 4th, 4pm MT, A3 due
- December, Date TBA by registrar's office, Final exam

Week	Topics
One:	Math preliminaries, Digital Privacy
Two:	Math preliminaries, Crypto. Fundamentals
Three:	Cryptography Fundamentals
Four: **(A1 Due)**	Cryptography Fundamentals
Five:	Cryptanalysis Fundamentals
Six: **Midterm 1**	MPC
Seven:	MPC
Eight: **(A2 Due)**	DP and HE
Nine:	Select private computations
Ten: **(Midterm 2)**	Private ML
READING WEEK NO CLASS - -	Reading Week - -
Eleven:	Inference Attacks
Twelve: **(A3 Due)**	Applied Crypto, Usable Crypto
Thirteen:	Misc topics, review, ...
Final Exam, date TBA by registrars office	

Grading Scheme

- 30% Assignments (three throughout the term, each worth ten percent)
- 25% Midterms (1 weighted 25% of the grade, the other weighted at 0% or used to replace the worst two assignment grades if the midterm grade is better)
- 39% Final exam
- 6% Weekly participation/thought exercises (One per week of instructional material, 12 total)

Assignments Assignment 1 and Assignment 2 consists of a written portion and a programming portion. The written portion includes proofs, conceptual questions, etc. The programming portion includes implementation, evaluation, experimental execution, etc. Assignment 3 will consists of a task to explain an advanced cryptography topic suitable for a beginner to get an understanding of it or do an assignment similar to the first two assignments.

Assignments are to be submitted to **Canvas** by the designated deadline. Assignments are to be completed individually. Students can expect the midterm and final examination to include questions that reflect the ones seen on the assignments. All assignments are due on their designated date in the calendar by 4pm Edmonton time.

Participation/Thought Exercises Each week there will be a prompt during one of the classes. This prompt will be in the slide deck, so if you miss that class you can still respond to the prompt. The response is to be submitted via **Canvas** in the designated place. In class, these prompts will be discussed among the attending students. If you discuss the prompt with someone in class, indicate who you discussed with in your submission. These will be graded on a trinary "best effort" metric. If you do not submit before the start of the next class (*NO EXTENSIONS ON THESE, NO EXCEPTIONS*), you get zero, if you submit on time, something at all relevant to the prompt, you will get one, and if you submit something good, definitively engaging with the prompt you get two.

Midterms The midterms question distributions includes multiple-choice, true and false, short answer, proofs, etc. Both midterms are comprehensive (covers all material from the course up to that point). They are closed book, no notes or cheat sheets permitted. No calculators allowed (and they also are not necessary). There are two midterms. Your best performing midterm is

your midterm grade (the 25% in the syllabus). The other midterm, if the grade is better than your worst two assignments, can replace your grade for those assignments. This replacement option is because the assignments may tend towards being difficult, as they are intended to help you learn the material such that you could do well on the examinations.

Final Exam The final exam will be similar to the midterms in terms of question distributions (can include multiple-choice, true and false, short answer, proofs, etc.). The final exam is comprehensive (covers all material from the course). It is closed book, no notes or cheat sheets permitted. No calculators allowed (and they also are not necessary). See course policy section on deferred final exams in the page below for this info.

IMPORTANT - SUBJECT TO RANDOM TEST All graded components of the course are subject to an oral test at the discretion of the instructor. A random subset of submissions (and any selection of ones based on the instructor/TAs determination) will be evaluated this way. The performance of the student on the oral test will effect the students grade on that submission. If the student is reasonably able to explain their submission, the oral test will *not* impact their original grade. If the student cannot reasonably explain their submission (are not sufficiently familiar with it), the oral test mark will result in a decrease in their original grade. While students may be referring to internet materials and solutions or discussing assignments with friends; they must do the assignment by themselves and acknowledge any sources used. Further, they must be able to defend/explain their submissions (e.g., how they arrived at the solution, why that solution works etc.). Be aware that any suspected cheating will be reported to the Faculty of Science.

Course Policy Information

Missed or Late Assessments: Please start working on the material in advance of the deadlines. To motivate you to do so, we may require you to submit milestones for some or all of them. Late submissions for assignments and project reports will be accepted only up to 72 hours after the original due date. They **will not be accepted at all after this 72 hours has ended**. All other graded components (participation/thought exercises and A3 proposals) must be done on time. There is no penalty for accepted late submissions within the 72 hour window. Course personnel will not normally give assistance after the original due dates.

Missed Midterm: If only one of the two midterms is missed the other midterm will serve as the midterm grade. If both midterms are missed, the weight may be shifted to the final exam at the discretion of the instructor after communication with the student.

Missed Term Work or Final Exam Due to Non-medical Protected Grounds (e.g., religious beliefs): When a term assessment or final exam presents a conflict based on non-medical protected grounds, students must apply to the Academic Success Centre for accommodations via their Register for Accommodations website. Students can review their eligibility and choose the application process specific for Accommodations Based on Non-medical Protected Grounds.

It is imperative that students review the dates of all course assessments upon receipt of the course syllabus, and apply AS SOON AS POSSIBLE to ensure the timely application of the accommodation. Students who apply later in the term may experience unavoidable delays in the processing of the application, which can affect the accommodation.

Missed Term Work Type 2:
A student who cannot complete assignment type assessments due to incapacitating illness, severe

domestic affliction or other compelling reasons must contact the instructor within two working days of missing the assessment, or as soon as possible, to request an excused absence. If an excused absence is granted, then the student will be presented with an option of re-weighting the grade to a different portion of the class as defined by the instructor. An excused absence is a privilege and not a right. There is no guarantee that an absence will be excused. Misrepresentation of facts to gain an excused absence is a serious breach of the Code of Student Behaviour. In all cases, instructors may request adequate documentation to substantiate the reason for the absence at their discretion.

Deferred Final Examination: A student who cannot write the final examination due to incapacitating illness, severe domestic affliction or other compelling reasons can apply for a deferred final examination. Such an application must be made to the student's Faculty office within two working days of the missed examination and must be supported by appropriate documentation or a Statutory Declaration (see calendar on Attendance). Deferred examinations are a privilege and not a right; there is no guarantee that a deferred examination will be granted. The Faculty may deny deferral requests in cases where less than 50% of term work has been completed. Misrepresentation of facts to gain a deferred examination is a serious breach of the Code of Student Behaviour.

Deferred final exam for this course is scheduled for **January 20, 2026**

Remarking Policy: If you have an assignment that you would like to have reappraised, please **email the instructor** (Dr. Bailey Kacsmar) to submit your request. Include a clear justification for your claims. Note that reevaluation **can result in the grade going up or down**. Not providing a clear justification is reason for the instructor to decline the reappraisal. The appeals deadline is **ONE WEEK** after the respective graded item is first made available. Appeals will not be considered after this date; so be sure to review your assessments in advance of this. If your appeal is concerned with a simple calculation error, please email Dr. Kacsmar directly or speak with her during office hours.

University Policy Information

Academic Integrity and Student Conduct: The University of Alberta is committed to the highest standards of academic integrity and honesty, as well as maintaining a learning environment that fosters the safety, security, and the inherent dignity of each member of the community, ensuring students conduct themselves accordingly. Students are expected to be familiar with the standards of academic honesty and appropriate student conduct, and to uphold the policies of the University in this respect.

Students are particularly urged to familiarize themselves with the provisions of the Student Academic Integrity Policy and the Student Conduct Policy, and avoid any behaviour that could potentially result in suspicions of academic misconduct (e.g., cheating, plagiarism, misrepresentation of facts, participation in an offence) and non-academic misconduct (e.g., discrimination, harassment, physical assault). Academic and non-academic misconduct are taken very seriously and can result in suspension or expulsion from the University.

All students are expected to consult the Academic Integrity website for clarification on the various academic offences. All forms of academic dishonesty are unacceptable at the University. Unfamiliarity of the rules, procrastination or personal pressures are not acceptable excuses for committing an offence. Listen to your instructor, be a good person, ask for help when you need it, and do your own work – this will lead you toward a path to success. Any academic integrity concern in this course will be reported to the College of Natural and Applied Sciences. Suspected

cases of non-academic misconduct will be reported to the Dean of Students. The College, the Faculty, and the Dean of Students are committed to student rights and responsibilities, and adhere to due process and administrative fairness, as outlined in the Student Academic Integrity Policy and the Student Conduct Policy. Please refer to the policy websites for details on inappropriate behaviours and possible sanctions.

The College of Natural and Applied Sciences (CNAS) has created an Academic Integrity for CNAS Students eClass site. Students can self enroll and review the various resources provided, including the importance of academic integrity, examples of academic misconduct & possible sanctions, and the academic misconduct & appeal process. They can also complete assessments to test their knowledge and earn a completion certificate.

Re-examination: There is no possibility of a re-examination in this course.

University of Alberta Grading Policy Grades reflect judgements of student achievement made by instructors and must correspond to the associated descriptor. These judgements are based on a combination of absolute achievement and relative performance in a class. Faculties may define acceptable grading practices in their disciplines. Such grading practices must align with the University of Alberta Assessment and Grading Policy and its procedures. The descriptors are Excellent: A+, A, A-, Good: B+, B, B-, Satisfactory: C+, C, C-, Poor: D+, Minimal Pass: D, Failure: F or F4.

Grades are unofficial until approved by the Department and/or Faculty offering the course. The break points are not predetermined but generally (+ or - not specified) 50's is D range, 60's is C range, 70's is B range, and 80's is A range. You need over 90% for A+ and a minimum of 50% to pass. There is no curve or special/fixed break points. This information will not be released.

Contract Cheating and Misuse of University Academic Materials or Other Assets: Contract cheating describes the form of academic dishonesty where students get academic work completed on their behalf, which they submit for academic credit as if they had created it themselves. Contract cheating may or may not involve the payment of a fee to a third party, who then creates the work for the student.

Examples include:

1. Getting someone to write an essay or research paper for you.
2. Getting someone to complete your assignment or exam for you.
3. Posting an essay, assignment, or exam question to a tutorial or study website; the question is answered by a "content expert", then you copy it and submit it as your own answer.
4. Posting your solutions to a tutorial/study website, public server, or group chat and/or copying solutions that were posted to a tutorial/study website, public server, or group chat.
5. Sharing your login credentials to the course management system (e.g., Canvas) and allowing someone else to complete your assignment or exam remotely.
6. Using an artificial intelligence bot or text generator tool to complete your essay, research paper, assignment, or exam solutions for you (without the instructor's permission).
7. Using an online grammar checker to "fix" your essay, research paper, assignment, or exam solutions for you (without the instructor's permission).

Contract cheating companies thrive on making students believe that they cannot succeed without their help; they attempt to convince students that cheating is the only way to succeed.

Uploading the instructor's teaching materials (e.g., course outlines, lecture slides, assignment, or exam questions, etc.) to tutorial, study, or note-sharing websites or public servers is a copyright infringement and constitutes the misuse of University academic materials or other assets. Receiving assignment solutions or answers to exam questions from an unauthorized source puts you at risk of receiving inaccurate information.

Appropriate Collaboration: Students are not permitted to copy solutions on homework assignments. Here are some tips to avoid copying on assignments:

1. Do not write down something that you cannot explain to your instructor.
2. When you are helping other students, avoid showing them your work directly. Instead, explain your solution verbally. Students whose work is copied also receive academic sanctions.
3. If you find yourself reading another student's solution, do not write anything down. Once you understand how to solve the problem, remove the other person's work from your sight and then write up the solution to the question yourself. Looking back and forth between someone else's paper and your own paper is almost certainly copying and will result in academic sanctions for both you and your fellow student.
4. If the instructor or TA writes down part of a solution in order to help explain it to you or the class, you cannot copy it and hand it in for credit. Treat it the same way you would treat another student's work with respect to copying, that is, remove the explanation from your sight and then write up the solution yourself.
5. There is often more than one way to solve a problem. Choose the method that makes the most sense to you rather than the method that other students happen to use. If none of the ideas in your solution are your own, there is a good chance it will be flagged as copying.

Exam Conduct: Please refer to the Examinations section of the Academic Calendar for more details on Conduct of Exams.

- Your student photo ID is required at exams to verify your identity.
- Students must arrive at the specified time to take the exam. Once the exam has started, students must remain in the physical in-person or remote environment for at least 30 minutes. Students who arrive more than 30 minutes late for an in-person exam will not be permitted to take the exam. Students who arrive more than 30 minutes late for an online exam may have their exam attempt removed or disqualified by the instructor. In both cases, students may apply for a deferred examination.
- All cell phones must be turned off and stored in your bags.

Accommodations for Students: In accordance with the University of Alberta's Discrimination, Harassment, and Duty to Accommodate policy, accommodation support is available to eligible students who encounter limitations or restrictions to their ability to perform the daily activities necessary to pursue studies at a post-secondary level due to medical conditions and/or non-medical protected grounds. Accommodations are coordinated through the Academic Success Centre, and students can learn more about eligibility on the Register for Accommodations website.

It is recommended that students apply **AS SOON AS POSSIBLE** in order to ensure sufficient time to complete accommodation registration and coordination. Students are advised to review

and adhere to published deadlines for accommodation approval and for specific accommodation requests (e.g., exam registration submission deadlines). Students who request accommodations less than a month in advance of the academic term for which they require accommodations may experience unavoidable delays or consequences in their academic programs, and may need to consider alternative academic schedules.

Recording and/or Distribution of Course Materials: Audio or video recording, digital or otherwise, of lectures, labs, seminars or any other teaching environment by students is allowed only with the prior written consent of the instructor or as a part of an approved accommodation plan. Student or instructor content, digital or otherwise, created and/or used within the context of the course is to be used solely for personal study, and is not to be used or distributed for any other purpose without prior written consent from the content authors.

Past or Representative Evaluative Material: Sample exam questions will be provided in the form of questions from the instructor or suggestions for similar styles of questions to practice. Exams include questions based on assignment questions, thus those are a recommended study source.

Learning and Working Environment: The Faculty of Science is committed to ensuring that all students, faculty and staff are able to work and study in an environment that is safe and free from discrimination, harassment, and violence of any kind. It does not tolerate behaviour that undermines that environment. This includes virtual environments and platforms.

If you are experiencing harassment, discrimination, fraud, theft or any other issue and would like to get confidential advice, please contact any of these campus services:

- Office of Safe Disclosure & Human Rights: A safe, neutral and confidential space to disclose concerns about how the University of Alberta policies, procedures or ethical standards are being applied. They provide strategic advice and referral on matters such as discrimination, harassment, duty to accommodate and wrong-doings. Disclosures can be made in person or online using the Online Reporting Tool.
- University of Alberta Protective Services: Peace officers dedicated to ensuring the safety and security of U of A campuses and community. Staff or students can contact UAPS to make a report if they feel unsafe, threatened, or targeted on campus or by another member of the university community.
- Office of the Student Ombuds: A confidential and free service that strives to ensure that university processes related to students operate as fairly as possible. They offer information, advice, and support to students, faculty, and staff as they deal with academic, discipline, interpersonal, and financial issues related to student programs.
- Office of Student Success and Experience: They can assist students in navigating services to ensure they receive appropriate and timely resources. For students who are unsure of the support they may need, are concerned about how to access services on campus, or feel like they may need interim support while you wait to access a service, the Dean of Students office is here to help.

Faculty of Science Student Services: The Faculty of Science Student Services office is located on the main floor of the Centennial Centre for Interdisciplinary Sciences (CCIS). This office can assist with the planning of Your Academics, and provide information related to Student Life & Engagement, Internship and Careers, and Study Abroad opportunities. Please visit Advising for more information about what Faculty Academic Advisors can assist you with.

Academic Success Centre: The Academic Success Centre provides professional academic support to help students strengthen their academic skills and achieve their academic goals. Individual advising, appointments, and group workshops are available year round in the areas of Accessibility, Communication, Learning, and Writing Resources. Modest fees may apply for some services.

Feeling Stressed, Anxious, or Upset? It's normal for us to have different mental health experiences throughout the year. Know that there are people who want to help. You can reach out to your friends and access a variety of supports available on and off campus at the Need Help Now webpage or by calling the 24-hour Distress Line: 780-482-4357 (HELP).

Course Outlines: Policy about course outlines can be found in the Academic Regulations, Evaluation Procedures and Grading section of the University Calendar.

Disclaimer: Any typographical errors in this syllabus are subject to change and will be announced in class and/or posted on the course website. The date of final examinations is set by the Registrar and takes precedence over the final examination date reported in the syllabus.