University of Alberta
CMPUT 496-A1 Cryptography for Digital Privacy
Fall 2024

Course Information

Instructor: Bailey Kacsmar
Office: Athabasca Hall
E-mail: kacsmar@ualberta.ca
Instructor Office Hours: TBA
Lectures: MWF 2pm-2:50pm
TAs: Steven Hai
Teaching Assistant's Office Hours: TBA

This document is for **reference only in advance of the course start date.** *This version of the syllabus is a guideline for the course and not a contract. As such, its terms may be altered when doing so is, in the opinion of the instructor(s), in the best interests of the students*

Course Communications: Important course information will generally be posted to **TBA**, 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.

- *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.

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.

Recommended background: 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

DRAFT

- 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)

Grading Scheme

- 36% Assignments (three throughout the term, each worth twelve percent)
- 22% Midterms (1 weighted 22% of the grade, the other weighted at 0% or 12% as it can be used to replace the worst assignment grade)
- 36% Final exam
- 6% Weekly participation/thought exercises (14 weeks, so 14 total)

Assignments Assignment 1 and Assignment 2 consists of a written portion and a programming portion. The written portion can include proofs, conceptual questions, etc. The programming portion can include 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.

Assignments are to be submitted to **TBA** 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.

DRAFT

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 **TBA** 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), 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 (can include 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 20% in the syllabus). The other midterm, if the grade is better than your worst two assignments, can replace your grade for those assignments. Note you cannot replace both A3 and A4 this way. 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).

EVALUATION 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.

DRAFT

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 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 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.

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 me directly or speak with me during my office hours.

DRAFT

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 Code of Student Behaviour 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) 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. Any suspected academic offence 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 of Science, and the Dean of Students are committed to student rights and responsibilities, and adhere to due process and administrative fairness, as outlined in the Code of Student Behaviour and the Student Conduct Policy. Anyone who is found in violation is likely to receive a sanction. Typical sanctions for academic misconduct include conduct probation, a mark reduction or a mark of 0 on an assessment, a grade reduction or a grade of F in a course, a remark on the transcript, and a recommendation for suspension or expulsion. Sanctions for non-academic misconduct include conduct conditions, fines, suspension of essential or non-essential University services and resources, and suspension or expulsion from the University.

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.

DRAFT

Students Eligible for Accessibility-Related Accommodations:

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 early 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.

Academic Success Center: The Academic Success Centre (ASC) provides services to support University of Alberta students in the areas of accommodations, learning, and writing. The ASC coordinates reasonable accommodations to eligible students who encounter medical or non-medical restrictions to their ability to perform the daily activities necessary to pursue studies at a post-secondary level. To that end, they work with students to coordinate disability-related accommodation needs for participation in University programs. For more information, and to register for services, visit the Academic Accommodations webpage.

The ASC also provides peer-based and professional academic support in the areas of learning and writing. They offer individual appointments, group workshops, and online courses to students in all University of Alberta programs, and at all levels of achievement and study.

At Writing Services, undergraduate students can work with a peer tutor to get feedback on a draft of their paper. Graduate students can book an appointment with a graduate writing advisor to get feedback on their documents. For more information, please visit the Writing Services webpage.

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 & Careers, and Study Abroad opportunities. Please visit Advising for more information about what Faculty Academic Advisors in the Student Services Office can assist you with.

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 author(s).

DRAFT