# Winter 2023 CS489/689 Privacy, Cryptography, Network and Data Security

*This 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 class.*

This course provides an introduction to data privacy and security, using cryptography and related techniques in networks, distributed systems and data science. 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 in networks and (distributed) data science environments. In layman terms, this course shows you how to benefit from the Internet and machine learning and still preserve individuals' privacy. This course complements CS458 which provides a wider set of security and privacy techniques also in other areas, but doesn't study these techniques in the detail as this course does.

*Prerequisites: MATH135 or MATH145, Computer science students only co-requisites: CS454 or CS456, Antirequisites: None.*

**Lectures:** *Tuesday/Thursday 8:30-9:50am, MC4058*, content will also be posted to learn. It is your responsibility to keep up with all course-related information posted to LEARN.

**Textbooks and Readings:** There is no required textbook. Additional readings will be assigned, and will appear on the course website; readings marked as mandatory contain required material for the course. You must read these mandatory readings.

## Instructor Information


- Bailey Kacsmar, bkacsmar@uwaterloo.ca
- Thomas Humphries, thomas.humphries@uwaterloo.ca


**Instructor Office hours:** Tuesdays 10:30-11:30am in office TBA, Online available on request.

**Email:** Important course information will generally be posted to LEARN, but may also be sent to your uwaterloo.ca email address. For personal matters, such as an illness, please email the instructors directly. We will only reply back to email from your uwaterloo.ca email address, following privacy rules.

**Teaching Assistant's:** TBA, office hours posted to learn.

## Learning Outcomes

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

- Evaluate the use of cryptography to protect data assets in storage, transit, and use
- Analyze security and privacy threats to data assets, including the privacy level of various data release mechanisms, privacy-utility trade-offs, and statistical inference attacks to infer sensitive information
- Evaluate the use of network security hardware and software to protect data assets in transit and use.
- Compare various network security mechanisms, and articulate their advantages and limitations.

# Outline

**Foundation -Protected at rest**

- Intro security/privacy
- Ethics/policy relevant to this course
- Basics of cryptography
- Symmetric encryption
- Hash functions, MAC
- Public key encryption (RSA)
- Semantic security, etc.
- Advanced topics: Bilinear maps, identity-based encryption

**Networks-Protected in transit**

- Network Security Primer: Firewalls, Intrusion Detection, Honeypots
- Authentication Failures: Spoofs (IP, user ids), rerouting attacks (DNS, etc.)
- Authentication Primer (Needham-Schroeder/Kerberos, SAML, etc.), PAKE
- PKI, DH, DNSSEC
- Confidentiality Failures: Snooping, traffic analysis (frequency analysis), Web tracking (cookies), browser fingerprinting
- TLS, VPN, WPA2
- Tor, Mixes, Secure email and messaging (Signal, PGP, etc.)

**Data - Protected during computation**

- Data Security: Inference attacks (leakage from function output, background information, side channels)
- k-Anonymity, l-diversity, (t-plausibility)
- Differential privacy (Laplace, Stats Can, etc.)
- Local differential privacy (Randomized response, etc.)
- Private machine learning (DP-SGD)
- Blockchains
- Homomorphic encryption
- Intro to MPC, PSI (commutative encryption)
- PIR, SSE (ORAM as homework for grad students)

## Grading Scheme

- 10% participation in flipped classroom (short exercises/assignments, etc.)
- 45% three homework assignments
- 15% midterm exam
- 30% final exam
- For graduate students: the above scaled to 80% + 20% project/survey paper

**Midterm and Final Assessment:** The assessments will be available for a set time and date on Crowdmark. You must submit your responses within 2.5 hours of accessing the assessment, but not later than the indicated cutoff points. These assessments are written-only (no programming) but covers material from the whole term. There will be no assistance from course staff for these assessments.

**Research Survey Paper (CS 689)** Students registered in CS 689 must write a research survey paper on a topic related to data security or privacy. In writing your paper, you must become familiar with the research literature relevant to your topic. Your focus should be on academic venues, such as the USENIX Security Symposium, ACM CCS, IEEE Symposium on Security and Privacy, Privacy Enhancing Technologies Symposium (PETS) or the NDSS Symposium. You should email your topic, proposal, and paper to the instructors.

**Topic approval:** Your topic must be approved in advance by the instructors before you submit your proposal. Proposal: Your proposal should be one page in length and include at least 10 references, preferably including (but not limited to) papers from the aforementioned venues. It is recommended but not required that you discuss the proposal with the instructors first. Email your proposal to the instructors by February 21.

**Paper:** Your paper should be a summary of past and current work on your topic, as well as an overview of known open problems and potential future directions in the area. You should provide a concise summary of work, emphasizing major accomplishments, rather than a detailed accounting of individual pieces of research activity. Email your final paper to the instructors by April 10.

**Format:** Your proposal and paper paper should be formatted in the two-column ACM proceedings format, using one of the ACM SIG Proceedings Templates. Your paper should not be longer than six pages. The ACM templates include headings for "Categories and Subject Descriptors", "General Terms", and "Keywords", which you do not need to use.

# Course Policy Information

**Remarking Policy:** If you have an assignment that you would like to have reappraised, please follow the instructions given on learn to submit your request. Include a clear justification for your claims. The appeals deadline is **one week** after the respective graded item is first made available. If your appeal is concerned with a simple calculation error, please see the TA(s) during their office hours.

**Missed or Late Assessments:** Please start working on the assignments 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 1, 2, or 3 will be accepted only up to 72 hours after the original due date. There is no penalty for accepted late submissions. Assignments can be submitted multiple times, and the last one will be used for marking. Course personnel will not normally give assistance for assignments after their original due dates.

**Security Information:** In this course, you will be exposed to information about security problems and vulnerabilities with computing systems and networks. To be clear, you are not to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network without the express consent of the owner. In particular, you will comply with all applicable laws and UW policies, including, but not limited to, the following:

- UW Policy 33, Ethical Behaviour
- MFCF Account Usage Policy
- CSCF-Specific Policies

Violations will be treated severely, and with zero tolerance.

# University Policy Information

**Academic integrity:** In order to maintain a culture of academic integrity, members of the University of Waterloo community are expected to promote honesty, trust, fairness, respect and responsibility. [Check the Office of Academic Integrity for more information.]

**Grievance:** A student who believes that a decision affecting some aspect of their university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70, Student Petitions and Grievances, Section 4. When in doubt, please be certain to contact the department's administrative assistant who will provide further assistance.

**Discipline:** A student is expected to know what constitutes academic integrity to avoid committing an academic offence, and to take responsibility for their actions. [Check the Office of Academic Integrity for more information.] A student who is unsure whether an action constitutes an offence, or who needs help in learning how to avoid offences (e.g., plagiarism, cheating) or about "rules" for group work/collaboration should seek guidance from the course instructor, academic advisor, or the undergraduate associate dean. For information on categories of offences and types of penalties, students should refer to Policy 71, Student Discipline. For typical penalties, check Guidelines for the Assessment of Penalties.

**Appeals:** A decision made or penalty imposed under Policy 70, Student Petitions and Grievances (other than a petition) or Policy 71, Student Discipline may be appealed if there is a ground. A student who believes they have a ground for an appeal should refer to Policy 72, Student Appeals.

**Diversity:** It is our intent that students from all diverse backgrounds and perspectives be well served by this course, and that students' learning needs be addressed both in and out of class. We recognize the immense value of the diversity in identities, perspectives, and contributions that students bring, and the benefit it has on our educational environment. Your suggestions are encouraged and appreciated. Please let us know ways to improve the effectiveness of the course for you personally or for other students or student groups. In particular:

We will gladly honour your request to address you by an alternate/preferred name or gender pronoun. Please advise us of this preference early in the term so we may make appropriate changes to our records. We will honour your religious holidays and celebrations. Please inform of us these at the start of the course. We will follow AccessAbility Services guidelines and protocols on how to best support students with different learning needs.

**Note for students with disabilities:** AccessAbility Services, located in Needles Hall, Room 1401, collaborates with all academic departments to arrange appropriate accommodations for students with disabilities without compromising the academic integrity of the curriculum. If you require academic accommodations to lessen the impact of your disability, please register with AccessAbility Services at the beginning of each academic term.

**Mental Health Support:** The Faculty of Math encourages students to seek out mental health support if needed. On-campus Resources:

- Campus Wellness
- Counselling Services: email or 519-888-4567 ext 32655
- MATES: one-to-one peer support program offered by Waterloo Undergraduate Student Association (WUSA) and Counselling Services: email
- Health Services: located across the creek from the Student Life Centre, 519-888-4096

**Turnitin.com:** Text matching software (Turnitin®) may be used to screen assignments in this course. Turnitin® is used to verify that all materials and sources in assignments are documented. Students' submissions are stored on a U.S. server, therefore students must be given an alternative (e.g., scaffolded assignment or annotated bibliography), if they are concerned about their privacy and/or security. Students will be given due notice, in the first week of the term and/or at the time assignment details are provided, about arrangements and alternatives for the use of Turnitin in this course. It is the responsibility of the student to notify the instructor if they, in the first week of term or at the time assignment details are provided, wish to submit alternate assignment.