CO 485/685: The Mathematics of Public-Key Cryptography **Fall 2020**

Instructor: **David Jao** djao@math.uwaterloo.ca
Teaching assistant: **Andrew Jena** ajjena@uwaterloo.ca

Lectures: MWF 12:30pm–1:30pm

Course web page: https://www.math.uwaterloo.ca/~djao/co485/

Discussion forum: https://campuswire.com/c/G0FD0B7CE/
Participation in the Campuswire forum is **mandatory**, in the following sense: although no part of your grade depends directly on forum participation, important administrative messages about the course will be posted on the forum from time to time, and you are expected to keep up to date with these messages. There is no monetary cost to sign up for Campuswire.

Course Outline. An in-depth study of public-key cryptography and number-theoretic problems related to the efficient and secure use of public-key cryptographic schemes. Topics to be covered will be drawn from the following partial list.

- *Algorithmic number theory*: Primality testing, integer factorization problem, discrete logarithm problem, elliptic curve discrete logarithm problem.
- *Public-key encryption*: RSA, ElGamal.
- *Signature schemes*: RSA, Schnorr, ECDSA.
- *Key establishment*: Diffie-Hellman and variants.
- *Provable security*: Security definitions, security models, security proofs.
- *Additional topics*: Pairing-based cryptography, isogeny-based cryptography, lattice-based cryptography.

References. The course textbook is:

- Jeffrey Hoffstein, Jill Pipher, and Joseph Silverman, *An Introduction to Mathematical Cryptography*, second edition, Springer-Verlag, 2014. The book can be downloaded online via the library web site (https://proxy.lib.uwaterloo.ca/login?url=https://link.springer.com/book/10.1007/978-1-4939-1711-2).

You might also find the following books interesting or useful.

- Boaz Barak, *Intense Crypto*, https://intensecrypto.org/.
- Dan Boneh and Victor Shoup, *A Graduate Course in Applied Cryptography*, https://toc.cryptobook.us/.

Marking scheme	**Option 1**	**Option 2**
Assignments:	100%	70%
Course project:	—	30%

This course normally has exams; however, because of the special circumstances brought about by online instruction, there are no exams this term. You have a choice of one of two marking schemes:

1. 100% assignments: Ten assignments, each worth 10% of your grade, due weekly on Friday from September 18 to November 27, except for Reading Week, or

2. 70% assignments, 30% project: If you choose this option, your assignment average will be based on your seven best assignments (each worth 10% of your grade). The course project is to implement a cryptographic primitive, protocol, attack, or construction, in such a way that your implementation improves upon available implementations in some way. Details will be discussed individually with students who are considering this option. The project is due on Friday, December 18.

All deadlines and due dates are strict and no extensions will be provided for any reason. If you need to skip an assignment, then choose the project option (which allows you to skip any three assignments without penalty). If you choose the project option, you must inform me of your choice by November 27; otherwise, I will assume you choose the 100% assignments option.

Policies.

Academic Integrity: 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 his/her 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 his/her 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 the 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 he/she has a ground for an appeal should refer to Policy 72, Student Appeals.

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.