Math 3159A: Introduction to Cryptography (Fall 2020)

Essential information

This is an online course.

- **Lectures:** TuTh 2:30-4
- **Office hours:** Th 4-5 on Zoom, anytime on Discord, or by appointment
- **Instructor:** Chris Kapulkin
- **Email:** kkapulki (at) uwo.ca
- **Office:** MC 116 (not that it matters...)
- **Teaching assistants:** Udit Mavinkurve and Mohabat Tarkeshian
- **Website:** http://uwo.ca/math/faculty/kapulkin/courses/2020-3159A
- **Prerequisites:** Math 1600A/B and (at least) one of: Math 2120A/B, 2124A/B, 2151A/B, 2155F/G, 3150A/B, ApplMath 2811B, or CompSci 2214A/B. Unless you have either the requisites for this course or written special permission from your Dean to enroll in it, you may be removed from this course and it will be deleted from your record. This decision may not be appealed. You will receive no adjustment to your fees in the event that you are dropped from a course for failing to have the necessary prerequisites.

Delivery

The course is delivered entirely **online, via Zoom**. The Zoom information is shared with students via OWL.

Students are required to attend the lectures under their *full legal name* and to have their *webcams on*. If a student is unable to do so, they must obtain prior written permission of the instructor.

Technical requirements: computer with working microphone and webcam, stable internet connection, and scanner or alternative (e.g., iPad). It is the student's responsibility to ensure that their device meets the system requirements for Zoom.

The course is delivered *synchronously* and *not recorded*. Producing and/or distributing audio/video recordings of the lectures will be considered an academic offense and handled accordingly.

Textbook

The course will follow:

- Hoffstein, Pipher, Silverman, *Introduction to Mathematical Cryptography*, 2nd Edition, 2014.

The entire book is available for free download in pdf format from Western library. Students are also welcome to consult:

- Koblitz, *A Course in Number Theory and Cryptography*, 2nd Edition, 1994.

Recommended homework problems

Section	Problems
1.2	6, 10, 11, 12, 14
1.3	15, 19, 20, 21, 22, 23
1.4	28, 29, 31
1.5	35, 36, Challenge: 37, 38
2.2	3, 4a
2.3	6, 7
2.4	9, 10
2.5	12, 15
2.6	16
2.7	17a
2.8	18a, 20, 24, Challenge: 22 and 25
2.9	26, 27, 28
2.10	30, 31, 34, 35, 37, Challenge: 29 and 41
3.1	1a, 4, 5
3.2	10, 11
3.3	12
3.4	15a, 16, 19, 21
3.5	22a
3.6	26ab
3.9	37, 38, 39a, 40, 41
3.10	42ab
4.2	1, 2, 4
4.3	5, 6, 7, 8, 9, 10
6.1	1, 2, 3
6.2	5, 6ab, 7ab
6.3	8, 9, 10, 11a
6.4	14, 15, 16, 19
6.6	21a
6.8	29, 31, 32, 33, Challenge: 30
6.10	48

Content

The topics will include:

- Elementary Number Theory
- Introduction to Computational Complexity
- Discrete Logarithm Problem and Diffie-Hellman Key Exchange
- RSA Encryption, Primality Test, Factorization Algorithms, and Quadratic Reciprocity
- Elliptic Curve Cryptography
- Post-Quantum Cryptography (time permitting)

Evaluation

The final grades will be based on the following components:

- assignments: 25%
- group assignment: 25%
- midterm exam: 25%
- final exam: 25%

Assignments

There will be five assignments, each worth 5% of the final grade, released according to the following schedule:

- Assignment 1: released Sep 17, due Sep 22 at 2 PM;
- Assignment 2: released Oct 1, due Oct 6 at 2 PM;
- Assignment 3: released Oct 15, due Oct 20 at 2 PM;
- Assignment 4: released Nov 12, due Nov 17 at 2 PM;
- Assignment 5: released Nov 26, due Dec 1 at 2 PM.

Late assignments will not be accepted.

Each assignment will consist of two problems: one requiring proof writing and one requiring code writing, and each student should choose one for submission. The solutions need to be prepared in LaTeX, using the template provided by the instructor. All programs must be written in 64bit version of Python3.

While working on on assignment, you are allowed to use the course textbook and notes. You are also allowed to discuss the problem with your fellow students. If necessary, you can ask the instructor or the teaching assistants for clarification.

However, you are **not allowed** to discuss the assignment with anyone else nor are you allowed to use any additional resources (other texts or online resources). You are also **not allowed** to share your solution with your fellow students.

Group assignments

There will be five group assignments, each worth 5% of the final grade, released according to the following schedule:

- Assignment 1: released Sep 24, due Sep 29 at 2 PM;
- Assignment 2: released Oct 8, due Oct 13 at 2 PM;
- Assignment 3: released Oct 22, due Oct 27 at 2 PM;
- Assignment 4: released Nov 19, due Nov 24 at 2 PM;
- Assignment 5: released Dec 3, due Dec 8 at 2 PM.

In order to participate in each group assignment, students will need to fill out a **survey** distributed 48 hours ahead of the assignment's release time. Students will have 24 hours to fill out this survey and the results will be used to determine their roles.

Late assignments will not be accepted.

Each assignment will consist of a single problem, requiring both proof writing and coding. Group assignments will be completed in groups of 4-5 students with roles assigned by the instructor:

- **Manager.** The manager is responsible for arranging and running group meetings. They should find convenient times for everyone to meet, set up Zoom calls, and coordinate discussions. In particular, they ensure that each group member understands all steps of the solution and that they have all proofread the draft produced by the scribe.
- **Programmer.** The programmer will write the Python program required as part of the submission. All programs must be written in 64bit version of Python3.
- **Reporter.** The front page of each submission consists of a report how the group meetings went, including: how many times the group met with the exact times of when each group member joined and disconnected from each call, and what difficulties and successes (with the subject matter or otherwise) the group have had. If there are disagreements about the solution, the report should sketch dissenting opinions and proposed alternatives. If a group consists of 4 members, then the reporter takes on the role of the secretary.
- **Scribe.** The scribe is responsible for writing up the final version of the submission - this is the only version that will be accepted and graded. The submission must include the report, the mathematical solution, and the program with its output.
- **Secretary.** During group meetings, the secretary is tasked with producing a record of all ideas discussed by the group. These notes are then used by the scribe and the programmer to prepare their parts of the submission.

The solutions need to be prepared in LaTeX, using the template provided by the instructor.

Midterm exam

The midterm exam will be on **October 29** (Thursday), 2020, from **2:30-3:45 PM**.

Students will have 60 minutes to solve problems and 15 minutes to scan and upload their solutions.

A mock exam, worth 1% of the midterm grade, will be conducted on October 27 (Tuesday), 2020, at 3:45 PM (end of class time). Students will be asked to upload a short non-mathematical submission, produced using the same technology that they intend to use during the exam.

Final exam

The final exam will be on **December 14** (Monday), 2020, from **9-11 AM**.

Students will have 100 minutes to solve problems and 20 minutes to scan and upload their solutions.

The final exam will be cumulative.

Course Websites

Students should check OWL (http://owl.uwo.ca) and the course website on a regular basis for news and updates for all of the courses in which they are enrolled. This is the primary method by which information will be disseminated to all students in each class. Students are responsible for checking OWL on a regular basis.

Accommodation and Accessibility

Accommodation Policies

Students with disabilities work with Accessible Education (formerly SSD) which provides recommendations for accommodation based on medical documentation or psychological and cognitive testing. The Academic Accommodation for Students with Disabilities policy can be found at:

https://www.uwo.ca/univsec/pdf/academic_policies/appeals/Academic Accommodation_disabilities.pdf

Academic Consideration for Student Absence

Students will have up to two (2) opportunities during the regular academic year to use an on-line portal to self-report an absence during the semester, provided the following conditions are met: the absence is no more than 48 hours in duration, and the assessment for which consideration is being sought is worth 30% or less of the student's final grade. Students are expected to contact their instructors within 24 hours of the end of the period of the self-reported absence, unless

noted on the syllabus. Students are not able to use the self-reporting option in the following circumstances:

- for exams scheduled by the Office of the Registrar (e.g., December and April exams)
- absence of a duration greater than 48 hours,
- assessments worth more than 30% of the student's final grade,
- if a student has already used the self-reporting portal twice during the academic year.

If the conditions for a Self-Reported Absence are *not* met, students will need to provide a Student Medical Certificate if the absence is medical, or provide appropriate documentation if there are compassionate grounds for the absence in question. Students are encouraged to contact their Faculty academic counselling office to obtain more information about the relevant documentation.

Students should also note that individual instructors are not permitted to receive documentation directly from a student, whether in support of an application for consideration on medical grounds, or for other reasons. **All documentation required for absences that are not covered by the Self-Reported Absence Policy must be submitted to the Academic Counselling office of a student's Home Faculty.**

For policy on Academic Consideration for Student Absences - Undergraduate Students in First Entry Programs, see:

https://www.uwo.ca/univsec/pdf/academic_policies/appeals/Academic_Consideration_for_absences.pdf

and for the Student Medical Certificate (SMC), see:

http://www.uwo.ca/univsec/pdf/academic_policies/appeals/medicalform.pdf

Religious Accommodation

Students should consult the University's list of recognized religious holidays, and should give reasonable notice in writing, prior to the holiday, to the Instructor and an Academic Counsellor if their course requirements will be affected by a religious observance. Additional information is given in the Western Multicultural Calendar:

https://multiculturalcalendar.com/ecal/index.php?s=c-univwo

You may also be eligible to write the Special Exam if you are in a "Multiple Exam Situation" (see http://www.registrar.uwo.ca/examinations/exam_schedule.html).

If a student fails to write a scheduled Special Examination, the date of the next Special Examination (if granted) normally will be the scheduled date for the final exam the next time this course is offered. The maximum course load for that term will be reduced by the credit of the

course(s) for which the final examination has been deferred. See Academic Calendar for details (under Special Examinations).

Academic Policies

The website for Registrarial Services is http://www.registrar.uwo.ca.

In accordance with policy, http://www.uwo.ca/its/identity/activatenonstudent.html, the centrally administered e-mail account provided to students will be considered the individual's official university e-mail address. It is the responsibility of the account holder to ensure that e-mail received from the University at his/her official university address is attended to in a timely manner.

Participants in this course are not permitted to record the sessions, except where recording is an approved accommodation, or the participant has the prior written permission of the instructor.

Scholastic offences are taken seriously and students are directed to read the appropriate policy, specifically, the definition of what constitutes a Scholastic Offence, at the following Web site:

http://www.uwo.ca/univsec/pdf/academic_policies/appeals/scholastic_discipline_undergrad.pdf.

Completion of this course will require you to have a reliable internet connection and a device that meets the system requirements for Zoom. Information about the system requirements are available at the following link:

https://support.zoom.us/hc/en-us

Please note that Zoom servers are located outside Canada. If you would prefer to use only your first name or a nickname to login to Zoom, please provide this information to the instructor in advance of the test or examination.

Support Services

Please visit the Science & Basic Medical Sciences Academic Counselling webpage for information on add/drop courses, academic considerations for absences, appeals, exam conflicts, and many other academic related matters: https://www.uwo.ca/sci/counselling/

Please contact the course instructor if you require lecture or printed material in an alternate format or if any other arrangements can make this course more accessible to you. You may also wish to contact Student Accessibility Services (SAS) at (519) 661-2147 if you have any questions regarding accommodations.

Western University is committed to a thriving campus as we deliver our courses in the mixed model of both virtual and face-to-face formats. We encourage you to check out the Digital Student Experience website to manage your academics and well-being: https://www.uwo.ca/se/digital/.

Learning-skills counsellors at the Student Development Centre (http://www.sdc.uwo.ca) are ready to help you improve your learning skills. They offer presentations on strategies for improving time management, multiple-choice exam preparation/writing, textbook reading, and more. Individual support is offered throughout the Fall/Winter terms in the drop-in Learning Help Centre, and year-round through individual counselling.

Students who are in emotional/mental distress should refer to Mental Health@Western (http://www.health.uwo.ca/mental_health) for a complete list of options about how to obtain help.

Additional student-run support services are offered by the USC, http://westernusc.ca/services.