Western Science

Department of Mathematics

MATH 3159A

Introduction to Cryptography

1 Course Information

Title: Introduction to Cryptography

Number: MATH 3159A

Term: Fall 2022

Times and Location: Tuesday 2:30–4:30 and Thursday 2:30–3:30 in TC-343

Prequisites: Mathematics 1600A/B and one of Mathematics 2120A/B, Mathematics 2124A/B, Mathematics 2151A/B, Mathematics 2155F/G, Mathematics 3150A/B, Applied Mathematics 2811A/B, or Computer Science 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.

2 Instructor

Instructor: Prof. Chris Hall

Office Hours: Monday 1:30–2:30 and Thursday 3:30–4:30 in MC-266

Email: `chall69@uwo.ca`

- Students must use their Western (uwo.ca) email addresses when contacting the instructor.
- Indicate the course (MATH 3159A) in your email.

3 Course Syllabus, Schedule, Delivery Mode

Course Content: Modern cryptological algorithms will be discussed with an emphasis placed on their mathematical foundation.

Main topics will include: basic number theory, complexity of algorithms, symmetric-key cryptosystems, public-key cryptosystems, RSA encryption, primality and factoring, discrete logarithms, elliptic curves and information theory.

Key Dates:

September 8, 2022	Classes begin
October 31 thru November 6, 2022	Fall Reading Week
December 8, 2022	Classes end
December 10–22, 2022	Exam period

COVID-19 Contingency plan: In the event of a COVID-19 resurgence during the course that necessitates the course delivery moving away from face-to-face interaction, affected course content will be delivered

entirely online, either synchronously (i.e., at the times indicated in the timetable) or asynchronously (e.g., posted on OWL for students to view at their convenience). The grading scheme will not change. Any remaining assessments will also be conducted online as determined by the course instructor.

4 Course Materials

Textbook: Students are strongly encouraged to acquire a copy of the second edition of *An Introduction to Mathematical Cryptography* by Hoffstein, Pipher, and Silverman. Lectures will loosely follow the text. Homework exercises may also be drawn from the text.

OWL statement: Students are responsible for checking the course OWL site (`http://owl.uwo.ca`) on a regular basis for news and updates. This is the primary method by which information will be disseminated to all students in the class.

All course material will be posted to OWL (`http://owl.uwo.ca`).

If students need assistance with the course OWL site, they can seek support on the OWL Help page. Alternatively, they can contact the Western Technology Services Helpdesk. They can be contacted by phone at 519-661-3800 or ext. 83800.

5 Methods of Evaluation

Breakdown:

Assignments (5)	40%	(Due: Sep 26, Oct 10, Oct 24, Nov 14, Nov 28)
Project Approval	5%	(Due: Oct 28)
Project	20%	(Due: Dec 2)
Final Exam	35%	Time and Location TBD

Assignments: Problem sets will be posted to OWL. Solutions must be submitted using `www.gradescope.ca` unless otherwise indicated. The lowest assignment score will be dropped, thus each remaining assignment will be worth 10%.

Assignments must be completed individually (as if it were an exam). Failure to do so may be regarded as a Scholastic Offence.

Project: The student should submit a presentation on a topic in cryptography. A typical presentation will be five or more written pages on a chosen topic. One could choose a theoretical topic and present it in a self-contained fashion. Alternatively one could choose a computational project and include code and calculations.

The student must first select a project and obtain instructor approval by the specified deadline. The completed project is due December 2 and must be submitted via gradescope.

Final Exam: The date, time, and location of the final exam will be posted to OWL once available. The exam is cumulative. The topics to be covered will be posted to OWL during the final week of class.

6 Student Absences

If you are unable to meet a course requirement due to illness or other serious circumstances, please follow the procedures below.

Assessments worth less than 10% of the overall course grade: Students who need a one-day extension for the project selection deadline should negotiate with the instructor. Students who need a longer extension should seek accommodation through their academic counsellor.

Assessments worth more than 10% of the overall course grade: For work totalling 10% or more of the final course grade, you must provide valid medical or supporting documentation to the Academic

Counselling Office of your Faculty of Registration as soon as possible. For further information, please consult the University's medical illness policy at
https://www.uwo.ca/univsec/pdf/academic_policies/appeals/accommodation_medical.pdf
The Student Medical Certificate is available at
https://www.uwo.ca/univsec/pdf/academic_policies/appeals/medicalform.pdf

Missed (homework) assignments with proper accommodation will be dropped and the remaining assignments will be reweighed accordingly.

An accommodation for the project will result in an extension of the deadline.

Absences from Final Examination: If you miss the Final Exam, please contact the Academic Counselling office of your Faculty of Registration as soon as you are able to do so. They will assess your eligibility to write the Special Examination (the name given by the University to a makeup Final Exam).

You may also be eligible to write the Special Exam if you are in a "Multiple Exam Situation" (e.g., more than 2 exams in 23-hour period, more than 3 exams in a 47-hour period).

Note: Missed work can only be excused through one of the mechanisms above. Being asked not to attend an in-person course requirement due to potential COVID-19 symptoms is not sufficient on its own.

7 Accommodation and Accessibility

Religious Accommodation: When a course requirement conflicts with a religious holiday that requires an absence from the University or prohibits certain activities, students should request accommodation for their absence in writing at least two weeks prior to the holiday to the course instructor and/or the Academic Counselling office of their Faculty of Registration. Please consult University's list of recognized religious holidays (updated annually) at:
https://multiculturalcalendar.com/ecal/index.php?s=c-univwo

Accommodation Policies: Students with disabilities are encouraged to contact Accessible Education, which provides recommendations for accommodation based on medical documentation or psychological and cognitive testing. The policy on Academic Accommodation for Students with Disabilities can be found at:
https://www.uwo.ca/univsec/pdf/academic_policies/appeals/AcademicAccommodation_disabilities.pdf

8 Academic Policies

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

In accordance with policy, https://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp113.pdf 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 their official university address is attended to in a timely manner.

No electronic devices will be allowed any the exam.

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

Remote Proctoring: In the event of health lock-down, tests and examinations in this course will be conducted using a remote proctoring service. By taking this course, you are consenting to the use of this software and acknowledge that you will be required to provide personal information (including some biometric data) and the session will be recorded. Completion of this course will require you to have a reliable internet connection and a device that meets the technical requirements for this service. More information about this remote proctoring service, including technical requirements, is available on Western's Remote Proctoring website at: https://remoteproctoring.uwo.ca.

9 Support Services

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

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

Western is committed to reducing incidents of gender-based and sexual violence and providing compassionate support to anyone who has gone through these traumatic events. If you have experienced sexual or gender-based violence (either recently or in the past), you will find information about support services for survivors, including emergency contacts at https://www.uwo.ca/health/student_support/survivor_support/get-help.html. To connect with a case manager or set up an appointment, please contact support@uwo.ca.

You may also wish to contact Accessible Education at http://academicsupport.uwo.ca/accessible_education/index.html if you have any questions regarding accommodations.

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