# MATH 3159A Course Outline

## 1. Course Information

**Course Information**

**List of Prerequisites**
Mathematics 1600A/B or Mathematics 1700A/B and one of Mathematics 2124A/B, Mathematics 2151A/B, Mathematics 2155F/G, Mathematics 2700A/B, Mathematics 3150A/B, Computer Science 2214A/B, the former Applied Mathematics 2811A/B, the former Mathematics 2120A/B.

Unless students have either the prerequisites for this course or written special permission from the Department of Mathematics to enroll in it, they may be removed and withdrawn from this course in accordance with university policy. This may be done after the add/drop deadline of the academic term, and the course will be marked as withdrawn (WDN) on their academic record. This decision may not be appealed.

## 2. Instructor Information

| Instructors | Email | Office | Office Hours |
|---|---|---|---|
| Chris Hall, Associate Professor | chall69@uwo.ca | | |

Students must use their Western (@uwo.ca) email addresses when contacting the instructor. Mathematical questions sent by email are unlikely to receive a response. They should be posed in office hours or in person after class.

Office hours will be in person. Times are tentative; changes will be posted on OWL Brightspace.

# 3. Course Syllabus, Schedule, Delivery Mode

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

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

**Learning Outcomes**

A successful student in the course should be able to do the following:
- use elementary number theory and modular arithmetic in cryptographic calculations;
- explain the distinction between symmetric-key and public-key cryptosystems;
- perform and analyze RSA encryption and decryption;
- apply elementary primality-testing and factoring algorithms;
- formulate and work with discrete-logarithm problems;
- carry out basic elliptic-curve computations and explain their cryptographic use.

**Key Dates**

Classes begin: September 9, 2026
Fall Reading Week: October 10 – 18, 2026
Classes end: December 9, 2026
Exam period: December 11 – 22, 2026

**Delivery Mode**

This course is delivered in person.

# 4. Course Materials

**Required textbook:** Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *Introduction to Cryptography*, 2nd ed. The textbook is available through Western Libraries at no cost to students; no purchase is required.

All course material will be posted to OWL Brightspace: https://westernu.brightspace.com/.

Students are responsible for checking the course OWL Brightspace site regularly for news and updates. This is the primary method by which information will be disseminated to all students in the class.

If students need assistance with the course OWL Brightspace site, they can seek support on the OWL Brightspace 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

**Grading Scheme and Assessment Dates**

The overall course grade will be calculated as listed below:

| | |
|---|---|
| Assignments | 10% |
| Midterm Test 1 | 25% |
| Midterm Test 2 | 25% |
| Final Exam | 40% |

There will be five written homework assignments. Starting Friday, September 18 assignments will be posted to Brightspace and due seven days later. The tentative dates are:

| Assignment | open | due |
|---|---|---|
| 1 | Sep 18 | Sep 25 |
| 2 | Oct 2 | Oct 9 |
| 3 | Oct 23 | Oct 30 |
| 4 | Nov 6 | Nov 13 |
| 5 | Nov 20 | Nov 27 |

Completed assignments should be uploaded to Gradescope.

There are two midterm tests tentatively scheduled for Wednesday, October 21 and Monday, November 16. They will take place during usual class time but will be in a *different* room. Details will be posted to Brightspace.

**Essential Learning Requirements**

Demonstrating satisfactory achievement on the cumulative final examination is an essential learning requirement of this course. To pass MATH 3159A, a student must satisfy both of the following conditions:

1. obtain a calculated final course grade of at least 50%; and
2. obtain a grade of at least 50% on the final examination.

A student whose calculated final course grade is at least 50% but whose final-examination grade is below 50% will not pass the course. In that case, the student's recorded final course grade will be 49%. Automatic reweighting of assignments or midterm tests to the final examination does not remove this requirement. For a student authorized to write a Special Examination, the Special Examination grade will be used for purposes of this requirement.

**Information about Missed Coursework**

Students must familiarize themselves with the *University Policy on Academic Consideration – Undergraduate Students in First Entry Programs,* posted on the Academic Calendar: https://uwo.ca/univsec//pdf/academic_policies/appeals/academic_consideration_Sep24.pdf,

This policy does not apply to requests for Academic Consideration submitted for **attempted or completed work**, whether online or in person. The policy also does not apply to students experiencing longer-term impacts on their academic responsibilities. These students should consult Accessible Education.

For procedures on how to submit Academic Consideration requests, please see the information posted on the Office of the Registrar's webpage: https://registrar.uwo.ca/academics/academic_considerations/.

Academic Consideration requests are not required and will not be accepted for missed in-term tests or assignments in this course. Missed in-term assessments are handled automatically through the flexible-completion and reweighting arrangements described below. The only absence requiring documentation and submission through the Student Absence Portal is the final examination.

**Midterms and Tests**

This course has two midterm tests and a **cumulative** final exam. There is **no** makeup test for a missed midterm. If you miss a midterm test, its 25% weight will shift automatically to the final examination. You do not need to submit an Academic Consideration request. In addition, after the final examination is graded, if your final-examination percentage is higher than your percentage on either midterm, the 25% weight of that midterm will shift automatically to the final examination, whether or not you wrote the midterm.

The only exception is an early sitting, offered when the scheduled test conflicts with another scheduled class, laboratory, or tutorial; a university-sanctioned varsity or institutional event; or a religious holiday or religious commitment. For a university-sanctioned scheduling conflict, the student must notify the instructor in writing no later than one week before the test. For a religious accommodation, the student must submit the request through the Student Absence Portal no later than one week before the test, as described in Section 6.1. No other circumstance, including illness, qualifies for an early sitting or makeup; these are addressed through the automatic reweighting described above.

**Assignments**

There will be five written assignments, each worth 2% of the final course grade. Each assignment will have a stated deadline followed by an automatic 48-hour no-late-penalty period. A submission received during that period will receive no late penalty. No submission will be accepted after the end of the no-late-penalty period.

If an assignment is not submitted by the end of its no-late-penalty period, no Academic Consideration request is required or accepted. The 2% weight of that assignment will shift automatically to the final examination.

Students may not request Academic Consideration on the basis of circumstances that began only after the original assignment deadline.

**Deadlines: The 48-Hour No-Late-Penalty Period**

All take-home assignments with a stated due date include an automatic 48-hour period after the deadline during which students may still submit without a late penalty. For example, if an assignment is due on

November 5, they may submit it until November 7 without penalty. After this 48-hour period, no further submissions will be accepted, and students do not need to request Academic Consideration for a missed deadline; their grade for this component will be calculated as described above.

**Final Exam and Special Examination**

Per university policy, an absence from the final examination requires an Academic Consideration request with supporting documentation submitted through the Student Absence Portal. If Academic Consideration is granted, the student will be permitted to write the Special Examination. Students should consult the Academic Calendar under "Special Examinations" for information about this process and its scheduling.

If the student misses their SPC exam and is approved for Academic Consideration, they will be withdrawn from the course without academic penalty. If they experienced extenuating circumstances such as prolonged illness, they may appeal to the Associate Dean (Academic), on a case-by-case basis, for the opportunity to write the final exam the next time the course is offered. An outstanding SPC will reduce their course load for the term in which the exam is deferred, as outlined in the Definitions of Types of Examinations policy.

If the student misses their SPC exam and Academic Consideration is not approved, or was not requested, they will receive a grade of zero on the exam.

# 6. Additional Statements

### 6.1 Religious Accommodation

When a recognized religious holiday either requires a student to be absent from the University, or requires or prohibits an activity that makes it impossible for them to complete an academic requirement scheduled that day, they are entitled to accommodation. No student will be penalized for an absence for religious reasons, and an alternative means of satisfying the requirement will be arranged. This accommodation is provided in accordance with the University's policy on Accommodation for Religious Holidays:
https://www.uwo.ca/univsec/pdf/academic_policies/appeals/accommodation_religious.pdf

The student should submit their requests through the Student Absence Portal (SAP), identifying the conflict and the specific course component(s) affected (e.g., test, midterm, exam).

> **Midterms and Tests**: If a religious observance conflicts with a midterm test, they must submit their request no later than **one week** before the test. Their instructor will arrange an early sitting of the test. As set out above, no makeup test is offered for any other reason; this early sitting is available specifically for this accommodation.
>
> **Final Examinations**: If a religious observance conflicts with the final examination, the student must submit the request through the Student Absence Portal no later than **two weeks** before the examination. If the request is approved, a Special Examination will be arranged in accordance with University and Faculty procedures. Students should consult the Academic Calendar under "Special Examinations" for information about scheduling.

Students are responsible for finding out what was covered in any class they miss due to a religious observance, and for taking the appropriate steps to keep up with the course.

If a suitable arrangement cannot be reached between a student and their instructor, they should consult the Undergraduate Chair of the department offering the course, and if necessary, the Associate Dean (Academic) of the Faculty of Science.

For a list of recognized religious observances, please visit the calendars posted on the Equity, Diversity & Inclusion website - https://www.edi.uwo.ca (About Us – Resources – Additional Resources – Calendars).

### 6.2 Academic 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/Academic Accommodation_disabilities.pdf.

### 6.3 General Academic Policies

The website for Registrar Services is https://www.registrar.uwo.ca/.

**Use of @uwo.ca email:** 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 email address. It is the responsibility of the account holder to ensure that emails received from the University at their official university address are attended to in a timely manner.

### Requests for Relief from Academic Decisions

Policy on Request for Relief from Academic Decision:
https://uwo.ca/univsec//pdf/academic_policies/appeals/requests_for_relief_from_academic_decisions.pdf

Procedures on Request for Relief from Academic Decision (Undergraduate):
https://uwo.ca/univsec//pdf/academic_policies/appeals/undergrad_requests_for_relief_procedure.pdf

### 6.4 Scholastic Offences

Policy on Scholastic Offences:
https://uwo.ca/univsec//pdf/academic_policies/appeals/scholastic_offences.pdf

Procedures on Scholastic Offences (Undergraduate):
https://uwo.ca/univsec//pdf/academic_policies/appeals/undergrad_scholastic_offence_procedure.pdf

### Use of Software for Assessments

All required papers may be subject to submission for textual similarity review to the commercial plagiarism detection software under license to the University for the detection of plagiarism. All papers submitted for such checking will be included as source documents in the reference database for the purpose of detecting plagiarism of papers subsequently submitted to the system. Use of the service is subject to the licensing agreement, currently between The University of Western Ontario and Turnitin.com (http://www.turnitin.com).

### Use of Electronic Devices During Assessments

In courses offered by the Faculty of Science, the **possession** of unauthorized electronic devices during any in-person assessment (such as tests, midterms, and final examinations) is strictly prohibited. This includes, but is not limited to: mobile phones, smart watches, smart glasses, hidden cameras, wireless earbuds, or headphones.

Unless explicitly stated otherwise in advance by the instructor, the presence of any such device at a student's desk, on their person, or within reach during an assessment will be treated as a scholastic offence, **even if the device is not in use**.

Effective September 2026, the typical penalty for this offence is a failing grade in the course AND a 12-month prohibition on retaking the course.

Only devices expressly permitted by the instructor (e.g., non-programmable calculators) may be brought into the assessment room. It is each student's responsibility to review and comply with these expectations.

**Use of Generative AI Tools**

Unless otherwise stated, the use of generative AI tools (e.g., ChatGPT, Microsoft Copilot, Google Gemini, or similar platforms) is **not permitted** in the completion of any course assessments, including but not limited to: assignments, lab reports, presentations, tests, and final examinations.

Using such tools for content generation, code writing, problem solving, translation, or summarization—when not explicitly allowed—will be treated as a **scholastic offence**.

If the use of generative AI is permitted for a particular assessment, the conditions of use will be specified by the instructor in advance. If no such permission is granted, students must assume that use is prohibited. It is the student's responsibility to seek clarification before using any AI tools in academic work.

### 6.5 Support Services

**Academic Advising.** Please visit the Science & Basic Medical Sciences Academic Advising webpage for information on adding/dropping courses, academic considerations for absences, requests for relief, exam conflicts, and many other academic-related matters: https://www.uwo.ca/sci/advising/.

**Mental Health Support.** 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.

**Gender-Based and Sexual Violence.** Western is committed to reducing incidents of gender-based and sexual violence (GBSV) and providing compassionate support to anyone who has gone through these traumatic events. If a student has experienced GBSV (either recently or in the past), they can 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.

**Accessibility for Coursework.** A student may contact the course instructor if they require lecture or printed material in an alternate format or if any other arrangements can make this course more accessible to them. If they have any questions regarding accommodations, they may also contact Accessible Education at http://academicsupport.uwo.ca/accessible_education/index.html

**Learning Development and Success.** Learning-skills counsellors at Learning Development and Success (https://learning.uwo.ca) are ready to help students improve their learning skills. The facility offers 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.

**Student Councils.**
Student-run support services are offered by the University Students' Council (https://westernusc.ca) and the Science Students' Council (https://www.westernssc.ca).