MATH 3159B Course Outline

1. Course Information

Title: Introduction to Cryptography
Number: MATH 3159B
Term: Winter 2025

Prerequisite(s): 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 you have either the requisites for this course or written special permission from your Dean's Designate (Department/Program Counsellors and Science Academic Advisors) 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 Information

Instructors	Email	Office	Office Hours
Dr. Hyun Jong Kim	hkim2293@uwo.ca	MC 119	MW 1:30 – 2:30 P.M. (Office hours are subject to change) or by appointment

Students must use their Western (@uwo.ca) email addresses when contacting the instructor. Students are encouraged to contact the instructor to discuss more personalized questions/accommodations (e.g. about assessment flexibilities as they pertain to their own personal situations). Students should use the course page on Owl Brightspace (https://westernu.brightspace.com/) to ask questions pertaining to the course contents (e.g. questions on math problems) or non-personal course logistics commonly applicable to students (e.g. questions about general course policies)

Students are encouraged to send the instructor reminder emails if the instructor has not responded to an email within 2 business days. Students are also encouraged to send the instructor reminder emails for *urgent matters* if the instructor has not responded within 24 hours.

3. Course Syllabus, Schedule, Delivery Mode

Course Description: 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

Rough course schedule (the following schedule may change and the topics of some weeks may blend into prior or following weeks)

Week Number	Dates	Topic	Chapters	Assignment due and/or Midterm
1	Jan 6 – Jan 10	An Introduction to Cryptography	Chapter 1	
2	Jan 13 – Jan 17	Discrete Logarithms and Diffie-Hellman	Chapter 2.1-2.4	
3	Jan 20 – Jan 24	Discrete Logarithms and Diffie-Hellman	Chapter 2.5-2.7	Assignment 1 due Jan 22
4	Jan 27 – Jan 31	Integer Factorization and RSA	Chapter 3.1-3.5	Assignment 2 due Jan 29
5	Feb 3 – Feb 7	Integer Factorization and RSA	Chapter 3.9-3.10	**Midterm 1 tentatively (time and location TBA) on Feb 5, to focus on the material of Weeks 1 – 4.**
6	Feb 10 – Feb 14	Probability Theory and Information Theory	Chapter 4.1, 4.3, 4.4, 4.7	Assignment 3 due Feb 12
7	Feb 17 – Feb 21	**Reading week**		
8	Feb 24 – Feb 28	Elliptic Curves	Chapter 5.1-5.4	
9	Mar 3 – Mar 7	Elliptic Curves	Chapter 2.10.4, 5.7-5.10	Assignment 4 due Mar 5
10	Mar 10 – Mar 14	Lattices and Cryptography	Chapter 6.3-6.8	Assignment 5 due Mar 12
11	Mar 17 – Mar 21		(Left blank for the time being)	**Midterm 2 tentatively on Mar 19 (time and location TBA), to focus on the material of Weeks 5 – 10**
12	Mar 24 – Mar 28	Digital Signatures	Chapter 7.1-7.2	

13	Mar 31 – Apr 4		(Left blank for the time being)	Assignment 6 due Apr 2

Here are some Key Sessional Dates for the course:
Classes begin: January 6, 2025
Midterm 1 (Tentative Date): Wednesday, February 12
Spring Reading Week: February 15 – 23, 2025
Midterm 2 (Tentative Date): Wednesday, 12
Classes end: April 4, 2025
Exam period: April 7 – 30, 2025

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. The cost of such a copy depends on the format (e.g. physical, electronic, hardcover, paperback); copies were recently seen offered at around CAD 80 – 130 online (before taxes and shipping and handling). Lectures will loosely follow the text, and lecture notes will be uploaded on OWL Brightspace roughly after the end of each week. Homework exercises may also be drawn from the text.

An errata to the text is available at https://www.math.brown.edu/johsilve/MathCryptoHome.html

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

Students are responsible for checking the course OWL site (https://westernu.brightspace.com/) 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 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.

Technical Requirements
The use of SageMath, an open-source mathematics software system, will be required for course assignments (but not any of the exams). As such, a computer with either stable internet connection (for access to https://sagecell.sagemath.org/ or https://cocalc.com/, the latter of which requires at least a free account) or an installation of SageMath is required.

5. Methods of Evaluation

Grading Scheme and Assessment Dates

The overall course grade will be calculated as listed below:
Assignments (5) 35%

Midterm 1	20%
Midterm 2	20%
Final Exam	25%

Assignments will typically be released at least one week before they are due and will be due on the Wednesday of the week that they are due.

See Section 3 for assignment due dates and tentative midterm dates.

Tentatively, Makeup Midterm 1 will be held on Feb 7 and Makeup Midterm 2 will be held on Mar 21, time and location TBA

Requirements on Assessment Submissions

Writings on assignment, midterm, and final exam submissions must be clear and legible to receive full credit. Assignment submissions on Gradescope (See section 4) must be as PDF files. Students are encouraged, but not required, to submit assignments using typesetting software/software that displays mathematical notations LaTeX, TeX, and/or MathJax. Handwritten submissions that are scanned, photocopied, and/or photographed are also acceptable as long as they are clear and legible.
we
Unless otherwise specified, solutions to assignments, midterms, and the final exam must be justified and/or calculations must be shown as appropriate to receive full credit.

On the beginning of all assignment submissions, students must compile any sources other than the required or recommended textbooks (See Section 4) and lecture contents that they may have consulted in formulating their solutions. Such sources may include, but are not limited to: collaborations/discussions with other people (including, but not limited to, the instructor and other students), Internet resources, articles or textbooks other than those listed in Section 4, AI or ML models or interfaces thereof (students are advised, however, that AI or ML models often generate inaccurate and even incoherent statements and that students are responsible for all statements that they include in their assignment submissions), and computer software (such as SageMath). The compilation of these sources should include a brief description of how to identify these sources. The following is a list recommending students on how to identify the aforementioned potential sources:

- For collaborations/discussions with other people: describe who these people are, say by listing their names (Unless an individual wishes to remain anonymous) and relationship to the submitter of the assignment (e.g. friend, classmate, instructor).
- For Internet resources: write out/copy and paste the URL of the web page consulted.
- For articles or textbooks other than those listed in Section 4: indicate the title, author, and journal/publisher as available, along with identifying information on which parts were specifically consulted (e.g. page number, theorem number, section number) .
- For AI or ML models or interfaces thereof: indicate which AI or ML models (e.g. GPT3.5, GPT4, Llama3.1) or interfaces (ChatGPT, perplexity.ai) were used, and summarize what prompts were inputted into said models or interfaces and what responses were outputted.
- For computer software (such as SageMath): summarize what kinds of computations were performed or include a screenshot of relevant code.

Here is a sample statement that compiles sources:

> Sources consulted: I collaborated with classmates A, B, along with a friend who wishes to remain anonymous. I also consulted the following webpages: https://www.blahblahblah.com/weeemathisfun, https://www.numbertheoryismindnumbing.com/lalalala . I also consulted Section 1.1.1 of the second edition of Hoffstein, Pipher, and Silverman's *An introduction to mathematical cryptography*. I also consulted perplexity.ai with the following prompt "Can negative numbers be prime numbers?" to which it responded that "…negative numbers cannot be prime numbers…" and listed reasons why, and yet suggested that "researchers might explore concepts like 'negative primes' with modified definitions". Lastly, I used the following code via SageMath: `Integer(1001).next_prime()` to find the next prime number after 1001.

If no sources were consulted in formulating the solutions to the assignment submission, then the compilation must indicated as such, for example by stating "**Sources consulted: None**".

All solutions in assignment submissions must be formulated in the submitter's "own words", no matter what sources may have been consulted. Failure to submit a compilation of sources and/or plagiarism on any given assignment **may result in a grade of zero on that assignment and/or treated as "Scholastic Offence"** (see Section 6).

General 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://www.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/
All requests for Academic Consideration must be made within 48 hours after the assessment date or submission deadline.

All Academic Consideration requests normally must include supporting documentation; however, recognizing that formal documentation may not be available in some extenuating circumstances, the policy allows students to make one Academic Consideration request **without supporting documentation** in this course. However, the following assessments are excluded from this, and therefore always require formal supporting documentation:

- Examinations scheduled during official examination periods (Defined by policy)
- Midterm (Designated by the instructor as the one assessment that always requires documentation when requesting Academic Consideration)

When a student *mistakenly* submits their one allowed Academic Consideration request **without supporting documentation** for the assessments listed above or those in the **Coursework with**

Assessment Flexibility section below, the request cannot be recalled and reapplied. This privilege is forfeited.

Evaluation Scheme for Missed Assessments

Midterm 1 submissions will not be accepted after Feb 7 and Midterm 2 submissions will not be accepted after Mar 21, even with Academic Consideration granted. A missed midterm will be reweighted to the student's percentage grade of the final exam.

When a student misses the Final Exam and their Academic Consideration has been granted, they will be allowed to write the Special Examination (the name given by the University to a makeup Final Exam). See the Academic Calendar for details (under Special Examinations), especially for those who miss multiple final exams within one examination period.

Coursework with Assessment Flexibility
By policy, instructors may deny Academic Consideration requests for the following assessments with built-in flexibility:

Flexible Completion
Assignments. This course has 6 assignments, and the 5 assignments with the highest marks are counted towards your final grade. Should extenuating circumstances arise, students do not need to request Academic Consideration for the first 1 missed assignments. Academic consideration requests will be denied for the first 1 missed assignments. Academic Consideration requests may be granted when students miss more than 1 assignments, and these additional (2^{nd} , 3^{rd}…) missed assignments will be reweighted to the final exam.

Deadline with a No-Late-Penalty Period
Assignments. Students are expected to submit each of the 6 assignments by the deadline listed. Should extenuating circumstances arise, students do not need to request Academic Consideration and they are permitted to submit their assignment up to 48 hours past the deadline without a late penalty. Should students submit their assessment beyond 48 hours past the deadline, a late penalty of 25% per day will be applied. Academic Consideration requests may be granted only for extenuating circumstances that started before the deadline and lasted longer than the No-Late-Penalty Period (48 or 72 hours).

6. Additional Statements

Religious Accommodation
When conflicts with a religious holiday that requires an absence from the University or prohibits certain activities, students should request an accommodation for their absence in writing to the course instructor and/or the Academic Advising office of their Faculty of Registration. This notice should be made as early as possible but not later than two weeks prior to the writing or the examination (or one week prior to the writing of the test).

Please visit the Diversity Calendars posted on our university's EDID website for the recognized religious holidays:

https://www.edi.uwo.ca.

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.

Academic Policies
The website for Registrar Services is https://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 permitted on exams.

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:

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

Support Services
Please visit the Science & Basic Medical Sciences Academic Advising webpage for information on adding/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.

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 Accessible Education at

http://academicsupport.uwo.ca/accessible_education/index.html

if you have any questions regarding accommodations.

Learning-skills counsellors at Learning Development and Success (https://learning.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.

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/.

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