DEPARTMENT OF MATHEMATICAL AND COMPUTATIONAL SCIENCES
UNIVERSITY OF TORONTO MISSISSAUGA

MAT302H5F LEC0101
Introduction to Algebraic Cryptography
Course Outline - Fall 2019

Class Location & Time	Mon, 10:00 AM - 11:00 AM IB 250 Wed, 11:00 AM - 01:00 PM MN 3110
Instructor	Kaul Sonam Devgan
Office Location	DH 3019
Office Hours	
E-mail Address	sonam.kaul@utoronto.ca
Course Web Site	The course will be using Quercus for announcements, grades, course schedule, and assignments.
Teaching Assistant	Gilchrist Valerie
E-mail Address	valerie.gilchrist@mail.utoronto.ca

Course Description

(Cross list with CSC322H5) The course will take students on a journey through the methods of algebra and number theory in cryptography, from Euclid to Zero Knowledge Proofs. Topics include: block ciphers and the Advanced Encryption Standard (AES); algebraic and number-theoretic techniques and algorithms in cryptography, including methods for primality testing and factoring large numbers; encryption and digital signature systems based on RSA, factoring, elliptic curves and integer lattices; and zero-knowledge proofs. [36L, 12T]

Prerequisite: MAT224H5/MAT240H5, MAT301H5
Exclusion: CSC322H5, MATC16H3 (SCI)
Distribution Requirement: SCI

Students who lack a pre/co-requisite can be removed at any time unless they have received an explicit waiver from the department. The waiver form can be downloaded from here.

Learning Outcomes

Upon successful completion of this course, student will be able to
• Differentiate between symmetric key encryption and asymmetric key encryption.
• Define and analyze the different modes of operations used in encryption algorithms.
• Apply number theoretical concepts to encrypt and decrypt the data.
• Solve different algorithms and analyze their security aspects.
• Represent numbers on elliptical curves and generate cryptosystems based on elliptic curves
• Form encryption algorithms and digital signature protocols.
• Validate zero knowledge proofs.

Textbooks and Other Materials

Text book:

J. Hoffstein, J. Pipher, and J Silverman, An Introduction to Mathematical Cryptography, Second Edition (2014).

Other Reference Book:

D.R. Stinson, Cryptography Theory and Practice, Fourth Edition (2018).

Other materials may be used for selected topics, and all relevant references will be posted on the course website.

Assessment and Deadlines

Type	Description	Due Date	Weight

Assignment	Assignment 1	2019-09-23	8%
Assignment	Assignment 2	2019-10-07	8%
Assignment	Assignment 3	2019-10-28	8%
Assignment	Assignment 4	2019-11-11	8%
Assignment	Assignment 5	2019-11-25	8%
Term Test	Mid term test	2019-10-21	20%
Final Exam	End Term Examination	TBA	40%
		Total	100%

More Details for Assessment and Deadlines

1. Homework: Assignments are to be handed in on Mondays at the beginning of your tutorial. You are encouraged to work together on material related to the course, including discussing the written assignments. However, you must write up your own solutions independently.
2. Lectures: Students are expected to attend the lectures and tutorials regularly and to keep up with the material presented in the lecture and the assigned reading.
3. Tutorials: All students must be enrolled in a TUT. The main purpose of the tutorial is to give you an opportunity to ask questions and work through examples together with your TA. To get the most from your tutorial, you should review the lecture material and try the assigned problems before your tutorial. First Tutorial will be on Sept 16, 2019.
4. Mid Term Test: 50-minute written term test is scheduled on Oct 16, 2019 between 11:05 am and 11: 55 am in scheduled classroom location.
5. Quercus: Almost all course administration will take place on Quercus. Homework assignments, announcements, handouts and other important information will be posted there. We will also maintain a weekly schedule with the topics covered in the lectures and the assigned readings, that will get updated as we advance in the semester, so you should check it regularly. You will also be able to see your marks for the written homework assignments and tests on Quercus.

Penalties for Lateness

25% penalty for the first two days of lateness (that is, for homework submitted on Wednesday instead of Monday). Later submissions will receive 0%.

Procedures and Rules

Missed Term Work

To request special consideration, bring supporting documentation to the instructor in person during office hours at least one week in advance.

In case of illness, bring a U of T medical certificate to the instructor within one week of the missed work. The certificate must specify the exact period during which you were unable to carry out your academic work.

There will be no make-up test. In the event that a student misses the term test and provides acceptable documentation justifiying the absense, the 20% of the final mark normally associated to the term test will be reassigned to the final exam.

Missed Final Exam

Students who cannot write a final examination due to illness or other serious causes must file anonline petition **within 72 hours of the missed examination**. Original supporting documentation must also be submitted to the Office of the Registrar **within 72 hours of the missed exam**. Late petitions will **NOT** be considered. If illness is cited as the reason for a deferred exam request, a U of T Verification of Student Illness or Injury Form must show that you were **examined and diagnosed at the time of illness and on the date of the exam, or by the day after at the latest**. Students must also record their absence on ACORN on the day of the missed exam or by the day after at the latest. Upon approval of a deferred exam request, a non-refundable fee of $70 is required for each examination approved.

Academic Integrity

Honesty and fairness are fundamental to the University of Toronto's mission. Plagiarism is a form of academic fraud and is treated very seriously. The work that you submit must be your own and cannot contain anyone elses work or ideas without proper attribution. You are expected to read the handout How not to plagiarize (http://www.writing.utoronto.ca/advice/using-sources/how-

not-to-plagiarize) and to be familiar with the Code of behaviour on academic matters, which is linked from the UTM calendar under the link Codes and policies.

Final Exam Information

Duration:	3 hours
Aids Permitted:	Non-Programmable Calculators

Additional Information

Please see the syllabus posted on the course webpage for more information, including a week by week schedule.

Last Date to drop course from Academic Record and GPA is November 7, 2019.