# COMP 4140 Introduction to Cryptography and Cryptosystems

## 1. General Information

- Instructor: Noman Mohammed
- Email: 
- Office location: 
- Lecture time and location: 
- Office hours: 
- Course website: 

## 2. Course Description

**Summary:** Description and analysis of cryptographic methods used in the authentication and protection of data. Classical cryptosystems and cryptanalysis, symmetric cryptosystems, and asymmetric (or public-key) cryptosystems.

**Prerequisites:** COMP 2130 (Discrete Mathematics for Computer Science), Students must be registered in fourth year of a Major or Honours programme in the Department of Computer Science

## 3. Textbook and Other Readings

- **Required Textbook:**

- **Recommended optional textbooks:**

## 4. Grading

1. Assignments: 40%
2. Midterm exam: 20% (tentative date: sometime in the last two weeks of October)
3. Final exam: 40%

- The final grade is based on curving the overall performance. There is no direct mapping between numerical percentage grades and final letter grades for this course.
5. Administrative Policy

- There will be 4 assignments: 2 before the midterm and 2 after the midterm. All the assignments will be due in class (unless otherwise specified). Late submissions suffer a penalty rate of 20% per day, up to 5 days (weekends count).
- The midterm and final are closed-book exams. The midterm covers all material presented up to that point in the course. The final exam covers material from the whole term, with emphasis on the second half of the course. Detailed information about the midterm will be released at a later time.
- There is no makeup to a missing midterm, so make sure that you write the midterm at the scheduled time. In the case of a serious illness or emergency, the weight of the midterm will be moved towards the final exam.
- Final exam make-up is possible ONLY under a university-approved condition, such as sickness with a doctor's note. Be prepared to provide written documentation (e.g., a medical excuse from your doctor) to verify the emergency and its seriousness.
- Students are expected to attend every class. Some material may only be covered in class and not made available on the course note/website. Students are expected to read the assigned materials and to actively participate in class discussions.
- In the event of extraordinary circumstances beyond the University's control, the content and/or evaluation scheme in this course is subject to change.

6. Course Topics (subject to change)

- Introduction
- Stream Ciphers
- The Advanced Encryption Standard (AES)
- More About Block Ciphers
- Introduction to Public-Key Cryptography
- The RSA Cryptosystem
- Public-Key Cryptosystems Based on the Discrete Logarithm Problem
- Digital Signatures
- Hash Functions
- Message Authentications Codes (MACs)
- Key Establishment
- A Few Other Topics

7. Student Resources

A list of University governing documents pertaining to students can be found here.

Academic Recourses

Various academic resources are available to students including the Science and Technology Library and various departmental help centers.
Health & Mental Health Resources

Students with Health and/or Mental Health issues may seek advice and/or help from Student Counselling Center, Student Accessibility Services, and University Health Services.

Copyright and Intellectual Property Resources

Copyrights and intellectual property must be respected by all students. For more information, please refer to the copyright office.

Academic Integrity Resources

The Faculty of Science takes academic integrity very seriously. Any evidence of academic dishonesty on assignments, labs and/or tests will be forwarded to the appropriate authorities for potential disciplinary actions.

The University Student Discipline By-Law may be accessed at: http://umanitoba.ca/admin/governance/governing_documents/students/student_discipline.html. Information from the Faculty of Science regarding Cheating and Plagiarism can be found at http://umanitoba.ca/faculties/science/undergrad/resources/webdisciplinedocuments.html.

Respectful Behavior Resources

Students are expected to act in a respectful manner. Policies regarding respectful work and learning environment and sexual assault can be found here.

Final Examinations, Grades and Grade Appeals Resources

Final examination and grades policies can be found here. For more resources about examinations, see here.

Students wishing to appeal their term work grade can do so through the Registrar’s office. A fee is charged for each appeal. More information can be found here.

To view your final examination, please check with the department offering the course for policies. More information can be found here.

To appeal your final grade, you can initiate the process at the Registrar’s office. A fee will be charged for each appeal. See the Registrar’s office for more information.

Limited Access and VW Resources

Students who fail or VW from a course will be subject to limited access to that course in future terms. That is, students will not be able to register for a course (for which they have VWed or failed) during the limited access registration period. For more information, please see the policy document for repeated courses.