University of Manitoba
Faculty of Science
Department of Mathematics

1 Course Details

Course Title & Number	SCI 2000 T03: Introduction to Encryption
Number of Credit Hours	3
Class Times	All lectures canceled, to be replaced with online notes and videos
Course Website	http://server.math.umanitoba.ca/~claya/crypto_2020.html
Pre-Requisites	Six credit hours of mathematics with a grade of B or better.

2 Instructor Contact Information

Instructor(s) Name	Adam Clay
Office Location	473 Machray Hall (currently not going to work)
Office Hours or Availability	Contact by email. I am mostly likely to answer after 7:30pm. I can also arrange WebEx calls if need be.
Office Phone Number	204-474-6849 (No longer in use)
Email	Adam.Clay@umanitoba.ca (Recommended)

3 Required material

The textbook for the class is The Mathematics of Encryption: An Elementary Introduction. ISBN: 978-0-8218- 8321-1. This textbook is required as all assignments and tutorial material will be sourced from this book.

Lecture notes will continue (after March 10, 2020) to be posted on the class website. Assignments 4, 5, and the final exam will be administered via Crowdmark. There are planned companion videos with the lecture notes.

4 Course Outline

This course will cover all of the material in the textbook, with an emphasis on the mathematical material rather than the historical development of encryption. There are, however, elements of the historical development of encryption that are very useful for framing the mathematics. While the historical context will sometimes be discussed in class, it will not be tested. The schedule on the course website is not being followed, as of March 10, 2020. The deadlines for assignments and exams are updated below.

Students are expected to learn all mathematical definitions in the book, as well as the relevant formulas and algorithms. All computations must be done without mechanical aids of any kind (E.g. phone, computer, calculator, slide rule, astrolabe, abacus). By the end of the term every student should be able to encrypt and decrypt messages by hand using all of the encryption schemes discussed in the book, understand permutations, combinations, and basic estimates of complexity of an encryption scheme, must be able to compute by hand all methods of attack covered in class (e.g. Euclidean algorithm as a means of cracking “KidRSA”). Basics of hashing, error correction, primality testing, and related by-hand computations. There will also be occasional proofs in this class. Students will be responsible for understanding any proofs presented in lectures and must be able to complete related/similar proofs of novel mathematical statements (i.e. things not covered in class) on assignments, tests and exams.

5 Attendance Policy

Students are expected to stay off campus and work from home as much as possible.

6 Course Evaluation Methods

There will be five assignments, two tests, and a final exam. Assignments 4 and 5 are to be uploaded to Crowdmark for evaluation (either scanning, or even taking a picture with your phone is fine as long as it is clear). Assignments 4 and 5 will be posted on the course website as well as mailed out via Crowdmark. Late assignments will be accepted, with a 20% penalty per day late.

The final exam will be a take-home exam, administered via Crowdmark. You will have 24 hours to complete it (the entire day of April 13th, the exam date originally assigned by the registrar’s office). It will be equal in difficulty and length to the planned 3-hour in-person exam, meaning that it should only take 3 hours of work (however you are welcome to invest 24 hours in the exam if you like). During the exam period (all of April 13) you are not permitted to communicate with anyone about the exam, even after you have completed your work.

Students MUST write the exam themselves. All work must be entirely that of the student writing the exam. Students are NOT allowed to share any of their work with others.

Violation of any of the above rules may be subject to penalties for academic dishonesty. These could include a mark of zero in the exam or a grade of F in the course, a record of academic dishonesty on your student record and/or your transcript, and/or suspension from taking courses in the Faculty of Science.

Due Date	Assessment Tool	Value of Final Grade
Feb. 6	Test 1	20%
March 12	Test 2	20%
Jan. 23, Feb. 13, Mar. 5, Mar. 29, Apr. 7	Assignments	20%
April 13	Final Exam	40%

7 Grading

The following letter grade cutoffs are preliminary and may be adjusted downwards at the end of the course (e.g. an A+ may become 90 and above).

Letter Grade	Minimum percentage to guarantee	Final Grade Point
A+	95	4.5
A	86	4.0
B+	80	3.5
B	72	3.0
C+	65	2.5
C	60	2.0
D	50	1.0

8 Assignment Grading Times

Assignments will always be returned before the next assignment is due.

9 Schedule of tests and quizzes and assignments

Dates outlined in the table above and in the tentative schedule posted on the class website.

10 Policy on missed or late assignments and tests

- There will be no deferred or make-up tests. If a student misses a test and is able to provide (within one week of the test) a medical note or other appropriate documentation excusing their absence, then the weight of that test will be moved onto the final exam.
- Late assignments will not be accepted and will be assigned a grade of zero–except for Assignments 4 and 5, where there is a 20% penalty per day late.

11 Course Technology

The main resource for this class is the website:

`http://server.math.umanitoba.ca/~claya/crypto_2020.html`. UM learn will not be used regularly, but will occasionally be updated with material that points to the website listed above.

It is the general University of Manitoba policy that all technology resources are to be used in a responsible, efficient, ethical and legal manner. The student can use all technology in classroom setting only for educational purposes approved by instructor and/or the University of Manitoba Student Accessibility Services. Student should not participate in personal direct electronic messaging / posting activities (e-mail, texting, video or voice chat, wikis, blogs, social networking (e.g. Facebook) online and offline "gaming" during scheduled class time. If student is on call (emergency) the student should switch his/her cell phone on vibrate mode and leave the classroom before using it. (© S Kondrashov. Used with permission)

12 Recording Class Lectures

Adam Clay and the University of Manitoba hold copyright over the course materials, presentations and lectures which form part of this course. No audio or video recording of lectures or presentations is allowed in any format, openly or surreptitiously, in whole or in part without permission of Adam Clay. Course materials (both paper and digital) are for the participant's private study and research.

13 Student Accessibility Services

If you are a student with a disability, please contact SAS for academic accommodation supports and services such as note-taking, interpreting, assistive technology and exam accommodations. Students who have, or think they may have, a disability (e.g. mental illness, learning, medical, hearing, injury-related, visual) are invited to contact SAS to arrange a confidential consultation.

> Student Accessibility Services http://umanitoba.ca/student/saa/accessibility/
> 520 University Centre
> 204 474 7423
> Student_accessibility@umanitoba.ca

14 Academic Integrity

The Department of Mathematics, the Faculty of Science and the University of Manitoba all regard acts of academic dishonesty in quizzes, tests, examinations or assignments as serious offences and may assess a variety of penalties depending on the nature of the offence.

Acts of academic dishonesty include bringing unauthorized materials into a test or exam, copying from another student, plagiarism and examination personation. Students are advised to read section 7 (Academic Integrity) and section 4.2.8 (Examinations: Personations) in the General Academic Regulations and Requirements of the current Undergraduate Calendar. Note, in particular, that cell phones and pagers are explicitly listed as unauthorized materials, and hence may not be present during tests or examinations.

Penalties for violation include being assigned a grade of zero on a test or assignment, being assigned a grade of ”F” in a course, compulsory withdrawal from a course or program, suspension from a course/program/faculty or even expulsion from the University. For specific details about the nature of penalties that may be assessed upon conviction of an act of academic dishonesty, students are referred to University Policy 1202 (Student Discipline Bylaw) and to the Department of Mathematics policy concerning minimum penalties for acts of academic dishonesty.

All students are advised to familiarize themselves with the Student Discipline Bylaw, which is printed in its entirety in the Student Guide, and is also available on-line or through the Office of the University Secretary. Minimum penalties assessed by the Department of Mathematics for acts of academic dishonesty are available on the Department of Mathematics web-page.