UNIVERSITY OF CALGARY
FACULTY OF SCIENCE

Department of Computer Science
ICT 602
403 220-6015
cpsc@cpsc.ucalgary.ca

COURSE OUTLINE

1. **Course:** CPSC 601.98, Special Topics in Computer Science - Fall 2019, Topic: Intro. to Modern Crypto

   Lecture 03: TR 15:30 - 16:45 in ST 126

Instructor	Email	Phone	Office	Hours
Dr Reyhaneh Safavi-Naeini	rei@ucalgary.ca	403 210-5492	ICT 636	By Appointment

   Course Site:

   D2L: CPSC 601.98 L03-(Fall 2019)-Special Topics in Computer Science

   Note: Students must use their U of C account for all course correspondence.

2. **Requisites:**

   See section 3.5.C in the Faculty of Science section of the online Calendar.

3. **Grading:**

   The University policy on grading and related matters is described in F.1 and F.2 of the online University Calendar. In determining the overall grade in the course the following weights will be used:

Component(s)	Weighting %	Date
Assignments (2-3)	20%	
Paper presentations	30%	
Course project	50%	

   Each of the above components will be given a letter grade using the official university grading system. The final grade will be calculated using the grade point equivalents weighted by the percentages given above and then converted to a final letter grade using the official university grade point equivalents.

   This course has a registrar scheduled final exam.

4. **Missed Components Of Term Work:**

   In the event that a student misses the midterm or any course work due to illness, supporting documentation, such as a medical note or a statutory declaration will be required (see Section M.1; for more information regarding the use of statuary declaration/medical notes, see FAQ). Absences must be reported within 48 hrs.

   The regulations of the Faculty of Science pertaining to this matter are found in the Faculty of Science area of the Calendar in Section 3.6. It is the student's responsibility to familiarize themselves with these regulations. See also Section E.3 of the University Calendar.

5. **Scheduled Out-of-Class Activities:**

   There are no scheduled out of class activities for this course.

6. **Course Materials:**

   1. Book (online): Introduction to Modern Cryptography. Katz and Lindell

   2. Online notes: Lecture Notes on Cryptography, Shafi Goldwasser and Mihir Bellare, 2008

   3. Online notes: Introduction to Modern Cryptography. M. Bellare and P. Rogaway.

7. **Examination Policy:**

   No aids are allowed on tests or examinations.

   Students should also read the Calendar, Section G, on Examinations.

8. **Approved Mandatory And Optional Course Supplemental Fees:**

   There are no mandatory or optional course supplemental fees for this course.

9. **Writing Across The Curriculum Statement:**

   For all components of the course, in any written work, the quality of the student's writing (language, spelling, grammar, presentation etc.) can be a factor in the evaluation of the work. See also Section E.2 of the University Calendar.

10. **Human Studies Statement:**

    Students will not participate as subjects or researchers in human studies.

    See also Section E.5 of the University Calendar.

11. **Reappraisal Of Grades:**

    A student wishing a reappraisal, should first attempt to review the graded work with the Course coordinator/instructor or department offering the course. Students with sufficient academic grounds may request a reappraisal. Non-academic grounds are not relevant for grade reappraisals. Students should be aware that the grade being reappraised may be raised, lowered or remain the same. See Section I.3 of the University Calendar.

    a. **Term Work:** The student should present their rationale as effectively and as fully as possible to the Course coordinator/instructor within **10 business days** of either being notified about the mark, or of the item's return to the class. If the student is not satisfied with the outcome, the student shall immediately submit the Reappraisal of Graded Term work form to the department in which the course is offered. The department will arrange for a re-assessment of the work if, and only if, the student has sufficient academic grounds. See sections I.1 and I.2 of the University Calendar

    b. **Final Exam:**The student shall submit the request to Enrolment Services. See Section I.3 of the University Calendar.

12. **Other Important Information For Students:**

    a. **Mental Health** The University of Calgary recognizes the pivotal role that student mental health plays in physical health, social connectedness and academic success, and aspires to create a caring and supportive campus community where individuals can freely talk about mental health and receive supports when needed. We encourage you to explore the mental health resources available throughout the university community, such as counselling, self-help resources, peer support or skills-building available through the SU Wellness Centre (Room 370, MacEwan Student Centre, Mental Health Services Website) and the Campus Mental Health Strategy website (Mental Health).

    b. **SU Wellness Center:** The Students Union Wellness Centre provides health and wellness support for students including information and counselling on physical health, mental health and nutrition. For more information, see www.ucalgary.ca/wellnesscentre or call 403-210-9355.

    c. **Sexual Violence:** The University of Calgary is committed to fostering a safe, productive learning environment. The Sexual Violence Policy (https://www.ucalgary.ca/policies/files/policies/sexual-violence-policy.pdf) is a fundamental element in creating and sustaining a safer campus environment for all community members. We understand that sexual violence can undermine students' academic success and we encourage students who have experienced some form of sexual misconduct to talk to someone about their experience, so they can get the support they need. The Sexual Violence Support Advocate, Carla Bertsch, can provide confidential support and information regarding sexual violence to all members of the university community. Carla can be reached by email (svsa@ucalgary.ca) or phone at 403-220-2208 .

    d. **Misconduct:** Academic misconduct (cheating, plagiarism, or any other form) is a very serious offence that will be dealt with rigorously in all cases. A single offence may lead to disciplinary probation or suspension or expulsion. The Faculty of Science follows a zero tolerance policy regarding dishonesty. Please read the sections of the University Calendar under Section K. Student Misconduct to inform yourself of definitions, processes and penalties. Examples of academic misconduct may include: submitting or presenting work as if it were the student's own work when it is not; submitting or presenting work in one course which has also been submitted in another course without the instructor's permission; collaborating in whole or in part without prior agreement of the instructor; borrowing experimental values from others without the instructor's

approval; falsification/ fabrication of experimental values in a report. **These are only examples**.

e. **Assembly Points:** In case of emergency during class time, be sure to FAMILIARIZE YOURSELF with the information on assembly points.

f. **Academic Accommodation Policy:** Students needing an accommodation because of a disability or medical condition should contact Student Accessibility Services in accordance with the procedure for accommodations for students with disabilities available at procedure-for-accommodations-for-students-with-disabilities.pdf.

   Students needing an accommodation in relation to their coursework or to fulfill requirements for a graduate degree, based on a protected ground other than disability, should communicate this need, preferably in writing, to the Associate Head of Undergraduate Affairs of the Department of Computer Science, Nathaly Verwaal by email nmverwaa@ucalgary.ca or phone 403-220-8485. Religious accommodation requests relating to class, test or exam scheduling or absences must be submitted no later than **14 days** prior to the date in question. See Section E.4 of the University Calendar.

g. **Safewalk:** Campus Security will escort individuals day or night (See the Campus Safewalk website). Call 403-220-5333 for assistance. Use any campus phone, emergency phone or the yellow phones located at most parking lot pay booths.

h. **Freedom of Information and Privacy:** This course is conducted in accordance with the Freedom of Information and Protection of Privacy Act (FOIPP). Students should identify themselves on all written work by placing their name on the front page and their ID number on each subsequent page. For more information, see Legal Services website.

i. **Student Union Information:** VP Academic, Phone: 403-220-3911 Email: suvpaca@ucalgary.ca. SU Faculty Rep., Phone: 403-220-3913 Email: sciencerep@su.ucalgary.ca. Student Ombudsman, Email: ombuds@ucalgary.ca.

j. **Internet and Electronic Device Information:** Unless instructed otherwise, cell phones should be turned off during class. All communication with other individuals via laptop, tablet, smart phone or other device is prohibited during class unless specifically permitted by the instructor. Students that violate this policy may be asked to leave the classroom. Repeated violations may result in a charge of misconduct.

k. **Surveys:** At the University of Calgary, feedback through the Universal Student Ratings of Instruction (USRI) survey and the Faculty of Science Teaching Feedback form provides valuable information to help with evaluating instruction, enhancing learning and teaching, and selecting courses. Your responses make a difference - please participate in these surveys.

l. **Copyright of Course Materials:** All course materials (including those posted on the course D2L site, a course website, or used in any teaching activity such as (but not limited to) examinations, quizzes, assignments, laboratory manuals, lecture slides or lecture materials and other course notes) are protected by law. These materials are for the sole use of students registered in this course and must not be redistributed. Sharing these materials with anyone else would be a breach of the terms and conditions governing student access to D2L, as well as a violation of the copyright in these materials, and may be pursued as a case of student academic or non-academic misconduct, in addition to any other remedies available at law.

Department Approval: Electronically Approved Date: 2019-08-29 17:31