UNIVERSITY OF CALGARY
FACULTY OF SCIENCE
DEPARTMENT OF COMPUTER SCIENCE
COURSE OUTLINE

1. **Course:** CPSC 418, Introduction to Cryptography -- Fall 2017

   Lecture 01: (MWF, 15:00-15:50 in SA106)

Instructor Name	Email	Phone	Office	Hours
Renate Scheidler	rscheidl@ucalgary.ca	220-6628	MS 436	MW 16:00-17:00 or by appointment

   Course Site:

   D2L: CPSC 418 L01 & PMAT 418 L01-(Fall 2017)-Introduction to Cryptography
   (used only for online submission of assignments and posting of solutions)
   Course website: people.ucalgary.ca/~rscheidl/418.

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

2. **Prerequisites:**

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

   Either Computer Science 331 or both Computer Science 319 and 105, and one of Mathematics 271, 273, or Pure Mathematics 315.
   Credit for both Computer Science 418 and any of 429, 557, or Pure Mathematics 329 or 418 will not be allowed.
   Students who have completed Computer Science 319 instead of Computer Science 331, and who have been unable to complete Computer Science 105, should contact the Department of Computer Science for information about how to be prepared for, and eligible to take, Computer Science 418.

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 %
Assignments (4): due Oct. 6, Oct. 27, Nov. 17, Dec. 8	40%
Midterms (2): in class Oct. 20 and Nov. 24	30%
Final Exam	30%

   Each piece of work (reports, assignments, quizzes, midterm exam(s) or final examination) submitted by the student will be assigned a percentage score. The student's average percentage score for the various components listed above will be combined with the indicated weights to produce an overall percentage for the course, which will be used to determine the course letter grade.

   The conversion between a percentage grade and letter grade is as follows;

Letter Grade	A+	A	A-	B+	B	B-	C+	C	C-	D+	D
Minimum Percent Required	95	90	86	82	78	74	70	66	62	58	50

   A passing grade in the final exam (at least 50%) is essential if the student is to pass the course as a whole (grade of C- or better).

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

   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 himself/herself with these regulations. See also Section E.3 of the University Calendar

5. **Scheduled out-of-class activities:**

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

6. **Course Materials:**

   Recommended textbook: Nigel P. Smart, *Cryptography Made Simple,* Springer 2016. PDF version available for free download from SpringerLink Ebooks through the U of C library webpage (need to be logged into U of C).

   Additional course materials such as lecture slides, assignments, handouts and links to additional resources will be made available on the course website.

7. **Examination Policy:**

   Closed book. No aids of any kind 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:**

   In this course, the quality of the student's writing in the written problems on the homework assignments will be a factor in the evaluation of the assignments. See also Section E.2 of the University Calendar.

10. **Human studies statement:**

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

11. **OTHER IMPORTANT INFORMATION FOR STUDENTS:**

    a. **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.

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

    c. **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-accomodations-for-students-with-disabilities_0.pdf.

       Students needing an Accommodation in relation to their coursework or to fulfil 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.

    d. **Safewalk:** Campus Security will escort individuals day or night (www.ucalgary.ca/security/safewalk/) . Call 403-220-5333 for assistance. Use any campus phone, emergency phone or the yellow phones located at most parking lot pay booths.

    e. **Freedom of Information and Privacy:** This course is conducted in accordance with the Freedom of Information and Protection of Privacy Act (FOIPP). As one consequence, 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 also www.ucalgary.ca/legalservices/foip.

    f. **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: suvpaca@ucalgary.ca

    g. **Internet and Electronic Device Information:** You can assume that in all classes that you attend, your cell phone should be turned off unless instructed otherwise. Also, communication with other individuals, via

laptop computers, Blackberries or other devices connectable to the Internet is not allowed in class time unless specifically permitted by the instructor. If you violate this policy, you may be asked to leave the classroom. Repeated abuse may result in a charge of misconduct.

h. **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.

i. **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.

Department Approval: Electronically Approved **Date:** 2017-09-04 14:08

Course Outcomes

1. Describe the different services that cryptography provides and give examples of cryptographic mechanisms that provide a given service.
2. Verify that a cryptographic mechanism works properly, eg. that encryption followed by decryption is successful.
3. Describe the different attack models covered in the course and how they relate to each other.
4. Demonstrate competence with mathematical foundations of modern cryptographic primitives.
5. Apply mathematics to assess the security of cryptographic primitives.
6. Restate the main cryptographic protocols that are covered in the course and their different functions.
7. Write software that provides cryptographic services and integrate existing cryptographic software libraries and packages in this software.