Course Outline

Final
Revised *September 16, 2014*

Meetings

Type	Section	Days	Time	Location
Lecture	COMP 4109-A	Mon & Wed	11:35am - 12:55pm	3165 ME

Instructor

Name	Email	Office	Office Hours
John Howat	jhowat@scs.carleton.ca	5380 HP	Mon & Wed, 2-4pm

Teaching Assistants

Name	Office	Office Hours
Adam Skillen	1170 HP	Mon & Tue, 1-2pm

Course Description

Practical aspects of cryptography. Pseudo random number generation, symmetric cryptography (stream and block ciphers), modes of operation, hash functions, message and entity authentication protocols, zero knowledge, pitfalls deploying public-key encryption and digital signatures, key distribution, secret-sharing.

Prerequisites

One of COMP 2402, SYSC 2100, and a MATH course at the 2000-level or above. Precludes additional credit for COMP 4103.

cuLearn

Students are expected to regularly check cuLearn for important announcements, assignments, references and readings, and grades.

Reading Materials

There are no required textbooks for this course. You may find *Cryptography Engineering* by Ferguson, Schneier and Kohno; *Cryptography and Network Security* by Stallings; and *Cryptography: Theory and Practice* by Stinson to be useful references.

Evaluation

Component	Weight	Date
Assignments	30%	Due Oct 1, Nov 5, Dec 3
Tests	30%	In class on Oct 20 and Dec 8
Proposal	5%	Due Oct 20
Presentation	5%	In class Nov 27 and Dec 1
Project	30%	Due Dec 8

Assignments

There will be 3 assignments, which will be due October 1, November 5, and December 3. Assignments should be submitted at the **beginning** of class. No late assignments will be accepted. You may **discuss the concepts** of your assignments with others, but your solutions must be **entirely your own**.

Project

You will be working on a project for the duration of the course. A proposal outlining your project's goals and deliverables is due October 20. A brief (5-minute) presentation of your project will take place in class on November 27 or December 1. The final project will be due December 8. Detailed expectations about the project will be given at the start of the semester. You may **discuss the concepts** of your project with others, but the project itself must be **entirely your own**.

Tests

There will be two in-class tests on October 20 and December 8.

Undergraduate Advisor

The Undergraduate Advisor for the School of Computer Science is available in Room 5302C HP, by telephone at 613-520-2600 x4364 or by email at undergraduate_advisor@scs.carleton.ca. The Undergraduate Advisor can assist with information about prerequisites and preclusions, course substitutions/equivalencies, understanding your academic audit and the remaining requirements for graduation. The Undergraduate Advisor will also refer students to appropriate resources such as the Science Student Success Centre, Learning Support Services and the Writing Tutorial Service.

University Policies

Student Academic Integrity Policy

Every student should be familiar with the Carleton University student academic integrity policy. A student found in violation of academic integrity standards may be awarded penalties which range from a reprimand to receiving a grade of F in the course or even being expelled from the program or University. Some examples of offences are: plagiarism and unauthorized co-operation or collaboration. Information on this policy may be found in the Undergraduate Calendar.

Plagiarism

As defined by Senate, "plagiarism is presenting, whether intentional or not, the ideas, expression of ideas or work of others as one's own." Such reported offences will be reviewed by the office of the Dean of Science. Unauthorized Co-operation or Collaboration Senate policy states that "to ensure fairness and equity in assessment of term work, students shall not co-operate or collaborate in the completion of an academic assignment, in whole or in part, when the instructor has indicated that the assignment is to be completed on an individual basis". Please refer to the course outline statement or the instructor concerning this issue.

Academic Accommodations for Students with Disabilities

The Paul Menton Centre for Students with Disabilities (PMC) provides services to students with Learning Disabilities (LD), psychiatric/mental health disabilities, Attention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorders (ASD), chronic medical conditions, and impairments in mobility, hearing, and vision. If you have a disability requiring academic accommodations in this course, please contact PMC at 613-520-6608 or pmc@carleton.ca for a formal evaluation. If you are already registered with the PMC, contact your PMC coordinator to send me your Letter of Accommodation at the beginning of the term, and no later than two weeks before the first in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, meet with me to ensure accommodation arrangements are made. Please consult the PMC website for the deadline to request accommodations for the formally-scheduled exam (if applicable) at:

http://www.carleton.ca/pmc/students/dates-and-deadlines/

Religious Obligation

Write to the instructor with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website:

http://www.carleton.ca/equity/

Pregnancy Obligation

Write to the instructor with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website:

http://www.carleton.ca/equity/

Medical Certificate

The following is a link to the official medical certificate accepted by Carleton University for the deferral of final examinations or assignments in undergraduate courses. To access the form, please go to:

http://www.carleton.ca/registrar/forms/