People

<table>
<thead>
<tr>
<th>Instructor</th>
<th>M. Jason Hinek (contact info)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teaching Assistant</td>
<td>tba</td>
</tr>
</tbody>
</table>

Course Information

<table>
<thead>
<tr>
<th>Classroom</th>
<th>Building: Southam Hall  Room: 313</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Times</td>
<td>Days: Wednesday and Friday   Time: 08:35am - 09:55am</td>
</tr>
<tr>
<td>Course Website</td>
<td><a href="https://www.scs.carleton.ca/content/comp4109f13">https://www.scs.carleton.ca/content/comp4109f13</a></td>
</tr>
<tr>
<td>Piazza (Course Forum)</td>
<td><a href="https://piazza.com/carleton.ca/fall2013/comp4109a">https://piazza.com/carleton.ca/fall2013/comp4109a</a></td>
</tr>
<tr>
<td>culearn</td>
<td><a href="https://www.carleton.ca/culearn/">https://www.carleton.ca/culearn/</a></td>
</tr>
</tbody>
</table>

Calendar 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 COMP2402, SYSC2100, and a MATH course at the 2000-level or above.
Precludes additional credit for COMP 4103 (no longer offered).

Textbooks

There is no required textbook for the course. However, material from the following supplemental textbooks (all freely available online) will be used:

- **Cryptography, An Introduction** by N. Smart (online)
- **Handbook of Applied Cryptography** by A. J. Menezes, P. C. van Oorschot and S. A. Vanstone (online)
- **A Computational Introduction to Number Theory and Algebra**, by V. Shoup (online)

Evaluation

<table>
<thead>
<tr>
<th></th>
<th>Assignments</th>
<th>30%</th>
<th>three assignments tba</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Midterm Exam</td>
<td>20%</td>
<td>tba</td>
</tr>
<tr>
<td>P</td>
<td>Project</td>
<td>20%</td>
<td>tba</td>
</tr>
<tr>
<td>F</td>
<td>Final Exam</td>
<td>30%</td>
<td>tba</td>
</tr>
</tbody>
</table>

Note: There will be a computational aspect to some of the assignment problems (and most likely your project). This may involve programming with a C++ library like NTL or using software that does symbolic computation (CAS software).
Note: You must pass the weighted average of your midterm (M) and final exam (F) in order to pass the course. Your final grade will be determined using the following:

```c
/* A - assignment grade between 0 and 30 */
/* P - project grade between 0 and 20 */
/* M - midterm exam grade between 0 and 20 */
/* F - final exam grade between 0 and 30 */

if (M+F >= 25) then
    final grade is A+P+M+F
else // (M+F < 25)
    final grade is min(2*(M+F), A+P+M+F)
```

Note: Your assignments and project must be typeset. My suggestion is to use \LaTeX or some other similar variant (such as \XeLaTeX if you want to easily use nice fonts).

**Collaboration Policy**

You may collaborate at the conceptual/problem-solving level of assignments and tutorials, but you must write your own solutions and code. I expect that you will work together on the assignments. On each assignment, you must declare which problems you solved collaboratively and who you worked with. I expect you to work in pairs for the project (submitting a single project).

Posting assignment solutions on discussion boards before the due date and time is also prohibited.

**Undergraduate Academic Advisor**

The Undergraduate Advisor for the School of Computer Science is available in Room 5302C HP, by telephone at 520-2600, ext. 4364 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 Services.

**University Policies**

Full academic regulations are found in the University’s calendar [link]. Some excerpts are below.

**Academic Integrity**

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 is presenting, whether intentional or not, the ideas, expression of ideas or work of others as one's own. Plagiarism includes reproducing or paraphrasing portions of someone else's published or unpublished material, regardless of the source, and presenting these as one's own without proper citation or reference to the original source.

In cases where an investigation determines that a violation of the Academic Integrity Policy has occurred, sanctions may be applied by the Faculty Dean, the Provost and Vice President (Academic), or by Senate Executive.

Sanctions may include but are not limited to completion of a remediation process, a written reprimand, assignment of a failing grade, withdrawal from a course, suspension from a program, suspension or expulsion from the university.

**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://www2.carleton.ca/pmc/new-and-current-students/dates-and-deadlines/](http://www2.carleton.ca/pmc/new-and-current-students/dates-and-deadlines/)

**Religious Obligations**

Carleton University accommodates students who, due to religious obligation, must miss an examination, test, assignment deadline, laboratory, or other compulsory event. The University has a Senate-approved policy on religious accommodation that forms part of its Human Rights Policy, available at: [http://www2.carleton.ca/equity/](http://www2.carleton.ca/equity/)

Accommodation will be worked out directly and on an individual basis between the student and the instructor(s) involved. Students should make a formal written request to the instructor(s) for alternative dates and/or means of satisfying requirements. Such requests should be made during the first two weeks of any given academic term, or as soon as possible after a need for accommodation is known to exist, but in no case later than the penultimate week of classes in that term.

**Pregnancy Obligation**

Write to me 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://www2.carleton.ca/equity/](http://www2.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/](http://www.carleton.ca/registrar/forms/)