• Prof. Claude Crépeau
• McConnell 110N
• (514) 398-4716

• Office Hours: Mondays 12:00-15:30
• For all class matters please use:
  crepeau@cs.mcgill.ca
Mr. Krtin KUMAR
McConnell
(514) 398-7071

Office Hours: Wednesdays 12:00-15:00
For all class matters please use:
krtin.kumar@mail.mcgill.ca
### COMP-547 Winter 2017 — Weekly Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Claude TR-2110</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon 11:30</td>
<td>Mon 11:30</td>
<td>10:00</td>
<td>11:30</td>
<td>10:00</td>
<td>10:00</td>
</tr>
<tr>
<td>Tue 10:00</td>
<td>Tue 10:00</td>
<td>10:30</td>
<td>11:00</td>
<td>10:30</td>
<td>10:30</td>
</tr>
<tr>
<td>Wed 11:30</td>
<td>Wed 11:30</td>
<td>12:00</td>
<td>12:00</td>
<td>12:30</td>
<td>12:30</td>
</tr>
<tr>
<td>Thu 11:30</td>
<td>Thu 11:30</td>
<td>12:00</td>
<td>12:00</td>
<td>12:30</td>
<td>12:30</td>
</tr>
<tr>
<td>Fri 10:00</td>
<td>Fri 10:00</td>
<td>10:30</td>
<td>10:30</td>
<td>12:00</td>
<td>12:00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Claude MC-110N</th>
<th>Tue</th>
<th>Thu</th>
<th>Thu</th>
<th>Fri</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon 15:30</td>
<td>Mon 15:30</td>
<td>14:30</td>
<td>14:30</td>
<td>14:30</td>
<td>14:30</td>
</tr>
<tr>
<td>Tue 14:30</td>
<td>Tue 14:30</td>
<td>15:00</td>
<td>15:00</td>
<td>15:00</td>
<td>15:00</td>
</tr>
<tr>
<td>Wed 14:30</td>
<td>Wed 14:30</td>
<td>15:00</td>
<td>15:00</td>
<td>15:00</td>
<td>15:00</td>
</tr>
<tr>
<td>Thu 14:30</td>
<td>Thu 14:30</td>
<td>15:30</td>
<td>15:30</td>
<td>15:30</td>
<td>15:30</td>
</tr>
<tr>
<td>Fri 14:00</td>
<td>Fri 14:00</td>
<td>13:00</td>
<td>13:00</td>
<td>13:00</td>
<td>13:00</td>
</tr>
</tbody>
</table>

**Office Hours:**

- Claude TR-2110 (Mon 11:30)
- Claude MC-110N (Mon 15:30)
- Comp 547 (Mon 16:00)

**MC = MCENG = McConnell • TR = ENG**

**Krtin MC-TBA**

**MC = MCENG = McConnell • TR = Trottier**
Computer Science COMP-547B
Cryptography and Data Security

Winter 2017,
Schedule: Monday-Wednesday 10:00-11:30 ENGTR 2110

Instructor: Prof. Claude Crépeau

T.A.: Krtin KUMAR

Office Hours: Claude : Monday 11:30-14:30, McConnell 110N.

<table>
<thead>
<tr>
<th>TASKS</th>
<th>ENCRYPTION</th>
<th>AUTHENTICATION</th>
<th>IDENTIFICATION</th>
<th>QUANTUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURITY</td>
<td>MILLER-VERNAM ONE-TIME PAD</td>
<td>WEGMAN-CARTER UNIVERSAL HASH</td>
<td>SIMPLE SOLUTIONS</td>
<td>QUANTUM KEY DISTRIBUTION</td>
</tr>
<tr>
<td>SYMMETRIC INFORMATIONAL</td>
<td>FROM PRBG DES, AES, ETC</td>
<td>FROM PRBG DES, AES, ETC</td>
<td>FROM PRBG DES, AES, ETC</td>
<td>QUANTUM ATTACKS, Q-SAFETY</td>
</tr>
<tr>
<td>SYMMETRIC COMPUTATIONAL</td>
<td>RSA, ELGAMMAL, BLUM-GOLDWASSER</td>
<td>RSA, DSA, ETC</td>
<td>GUILLOUX-QUISQUATER, SCHNOR, ETC</td>
<td>QUANTUM ATTACKS, Q-SAFETY</td>
</tr>
<tr>
<td>ASYMMETRIC COMPUTATIONAL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HOMEWORKS:

http://crypto.cs.mcgill.ca/~crepeau/COMP547/
COMP-547
Cryptography and Data Security

• Description: (4 credits; 3 hours) This course presents an in-depth study of modern cryptography and data security. We investigate four important subjects of cryptography: data encryption, data authentication, user identification and key distribution. The basic information theoretic and computational security of classical and modern cryptographic systems are analyzed. The course is self-contained and all necessary math background will be explicitly covered.
Mandatory textbook:

Errata

Mandatory use of MAPLE:
Available labs with maple 16 installed: lab2-X, open-X, lab6-X, lab7-X, lab9-X, where X is from 1 to approximately 25.
Any student taking a cs course either has or can create a CS account.

useful books:

Doug Stinson.

Cryptography - Theory and Practice (third edition)
Your final grade will be calculated as follows:

- 50% for 5 assignments (10% each)
- 50% for the final exam
- The exam is open book, no electronic device will be allowed (this includes noise-cancelling headphones).
Policy on collaborations

- We greatly encourage you to discuss the assignment problems with each other.

- However, these discussions should not go so far that you are sharing code or giving away the answer.

- A rule of thumb is that your discussions should be considered public in the sense that anything you share with a friend should be sharable with any student in the class.

- We ask you to indicate on your assignments the names of the persons with whom you collaborated or discussed your assignments (including the TA’s and instructor).
Policy on re-grading

- If you wish us to re-grade a question on an exam (or assignment), we will do so. However, to avoid grade ratcheting, we reserve us the right to re-grade other questions on as well.

Policy on final grades

- We will use the same rules and formula for calculating the final grade for everyone. We understand that your performances may be influenced by many factors, possibly out of your control. However, that is the only way we can be fair. The only exceptions will be medical exceptions. In that case, I will require a medical note, which has to be also reported to McGill, and to be informed as early as possible. Failure to comply to these rules, may results in the impossibility to invoke a medical exception.
Policy on Assignments

• Due date/time, location/mode for returning your solutions, and accepted formats will be announced in class and indicated on the course web page.

• Failure to return your assignment in time will result in penalties or even absence of grading. Late submission of 24h or less will receive a penalty of 20%. In all other cases, your assignment will be refused and not graded.

• Importantly, solutions that do not follow the requested format will receive a penalty. By default, we only accept PDF or TEXT files. Images (if any) must be embedded in a PDF. Do not compress your files. All files must open on LINUX SOCS workstations.

• The quality of the presentation of your solution is very important. Unreadable material, cryptic notations, or bad organization of the material will result in penalties, and potentially even an absence of grading. If you scan your hand-written solutions, it is your responsibility to ensure that you submit a high-quality image (i.e. excellent luminosity, contrast, focus and resolution). The clarity of your explanations will also be an integral part of your final grade.
McGill Policies

• In accordance with McGill University’s Charter of Students’ Rights, students in this course have the right to submit in French as well as in English any written work that is to be graded.

• McGill University values academic integrity. Therefore, all students must understand the meaning and consequences of cheating, plagiarism and other academic offenses under the Code of Student Conduct and Disciplinary Procedures. See this link: http://www.mcgill.ca/students/srr/
Winter 2017  COMP-547
Cryptography and Data Security
Prof. Claude Crépeau