UNIVERSITY OF REGINA
DEPARTMENT OF COMPUTER SCIENCE
CS 435/890BN - Cryptography and Network/Data Security (Fall 2020)

Information

Class time: 7:00 pm on Mondays and Wednesdays
Class location: Remote Learning
Instructor: Dr. Qian Yu
Email: Qian.Yu@uregina.ca
  (the best way to communicate with the instructor after class is by email)

Course Site: UR Courses
  (All the information and materials will be provided through UR Courses. Due to the
remote learning setting of the course, it is your responsibility to check UR Courses
frequently. Otherwise, you may miss important information or deadline)

Course delivery through Zoom:
  Zoom Info will be provided on UR Courses
Office Hours: through email or make appointment for a Zoom chat
Exam Date: TBD

Textbook


Reference Books (Optional)

A. Menezes, P. Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press
(All chapters are available for download for free at http://cacr.uwaterloo.ca/hac/)

Class Notes, Assignments and Projects

You can access course files, such as class notes, projects and assignments from UR Courses

Topics

1. Introduction
2. Classical Encryption Techniques
3. Modern Encryption Algorithms
4. Basic Concepts in Number Theory and Finite Fields, and AES
5. Public-key Cryptography and RSA
6. Message Authentication and Hash Functions
7. Digital Signature and Mutual Trust
(Note: This list of topics is subject to change, depending on the specific background of the students and time constraints.)

**Grading Scheme***

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Written Assignments</td>
<td>18%</td>
</tr>
<tr>
<td>Programming Assignment(s)</td>
<td>12%</td>
</tr>
<tr>
<td>Project</td>
<td>40%</td>
</tr>
<tr>
<td>Presentation</td>
<td>10%</td>
</tr>
<tr>
<td>Examination</td>
<td>20%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

* As this course is a 4th year undergraduate course cross-listed with a graduate course, there will be different expectations of these two groups of students. Those taking CS 890BN will be expected to develop a deeper understanding of the course topics than students taking CS 435. Although the distribution of grades is the same in both offerings, the requirements for the programming assignments, project, and examination will be different for CS 890BN students to reflect this difference in expected depth of knowledge.

* The grading scheme is subject to change later if found necessary. If there is a change, the instructor will let students know in class, as well as a note will be posted on the UR Courses.

**NOTES**

1. Instructor reserves the right to ADD or SUBTRACT up to 5% from the computed grade in the class, based upon instructor's subjective assessment of your participation and work.

2. The format of the exam(s) is not final confirmed, how to conduct the exam(s) will be communicated later.

3. DUE DATES for assignments and project will be given with the assignments and project. Late submissions without sufficient reason are NOT acceptable.

4. All assignments and projects need to be submitted electronically through UR Courses. Please make sure it is readable and clear for the submitted files.

5. Any student with a disability who may need accommodations should discuss these with the course instructor after contacting the Coordinator of the Disability Resource Office.

6. Cooperation on assignments or project is generally encouraged, but must be limited to verbal discussion. Refer to the section on Discipline Regulations in the General University Calendar.