Course Syllabus

CP460 Applied Cryptography
Physics and Computer Science, Science, Waterloo
Fall | 2018

Instructor Information

Dr. Jianbing Ni | Science Building N2084A
519-888-4567 ext. 37466, jni@wlu.ca
Weekly Office Hours: Fridays: 1:00-3:00pm or By Appointment

Course Information

Algorithms and issues in applied cryptography. Topics include history of cryptography, stream ciphers, block ciphers, hash function, public-key encryption, digital signatures, secret sharing, and key management. Also, discussion of current issues in information security.

Prerequisites : MA121, CP213 or CP264.

Lecture: Monday, Wednesday, Friday 10:30 -11:20 am.
Room: Bricker Academic Building BA202

Course Overview and Approach

Overview: The course is an introduction to cryptographic algorithms, both historical and modern, and these algorithms are discussed in detail with encryption examples. There is an emphasis on security issues beyond confidentiality, e.g. authentication, nonrepudiation, integrity, and on the special properties common computer science tools like hash functions and random number generators need to have for cryptographic applications. The course provides an introduction to numerous applications, including digital signatures, secret sharing, and blockchain.

Course Topics: Introduction, Simple Ciphers, Cryptanalysis, Simplified DES, DES, Advanced Encryption Standard (AES), Public-key cryptography, RSA, Discrete Log, ElGamal, Signature Schemes, Elliptic curve cryptosystems, Hash functions, Secret sharing, Blockchain.

Learning Outcomes

By the end of this course, students should be able to:

- Understand fundamental cryptographic principles, including the types of cryptography and their properties.

- Understand some basic building blocks of computer security (encryption, authentication, hashing …).
- Understand and know some of the algorithms used to provide examples of those building blocks.
- Identify security problems in computer systems.
- Understand how to apply security algorithms to real-world applications.

Course Tools and Learning Materials

Text: Course Notes

Reference books:

--Cryptography: Theory and Practice. D. Stinson. 4nd edition. CRC Press, 2018.
--Cryptography and Network Security: Principles and Practices. William Stallings. 6rd edition. Prentice Hall, 2013.
--Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell, second edition, CRC Press, 2014.
--Cryptography Engineering. Niels Ferguson, Bruce Scheiner and Tadayoshi Kohno, Wiley, 2010.

Course Information:

Course information for CP460 is posted at https://ece.uwaterloo.ca/~j25ni/CP460. It is the student’s responsibility to check the webpage frequently for new information or updates.

Intellectual Property:

The educational materials developed for this course, including, but not limited to, lecture notes and slides, handout materials, examinations and assignments, and any materials posted to https://ece.uwaterloo.ca/~j25ni/CP460, are the intellectual property of the course instructor. These materials have been developed for students use only and they are not intended for wider dissemination and/or communication outside of a given course. Posting or providing unauthorized audio, video, or textual material of lecture content to third-party websites violates an instructor’s intellectual property rights, and the Canadian Copyright Act. Recording lectures in any way is prohibited in this course unless specific permission has been granted by the instructor. Failure to follow these instructions may be in contravention of the university’s Code of Student Conduct and/or Code of Academic Conduct, and will result in appropriate penalties. Participation in this course constitutes an agreement by all parties to abide by the relevant University Policies, and to respect the intellectual property of others during and after their association with Wilfrid Laurier University.

Student Evaluation (Total 100%)

Assessment	Weighting
4 Assignments	20%
Midterm Exam	30%
Final Exam	50%

Missed Tests, Late work, etc.: Tests missed *without a valid, documented excuse* will be assigned a mark of zero. Late work will not be accepted. Any work that is late without appropriate documentation (e.g. physician's note, death certificate, etc.) will receive zero.

University and Course Policies

1. **Special Needs:** Students with disabilities or special needs are advised to contact Laurier's Accessible Learning Centre for information regarding its services and resources. Students are encouraged to review the Academic Calendar for information regarding all services available on campus.

2. Plagiarism: The University has approved the following wording for inclusion on all course syllabi about the use of the institutionally supported plagiarism software tool. "Wilfrid Laurier University uses software that can check for plagiarism. If requested to do so by the instructor, students are required to submit their written work in electronic form and have it checked for plagiarism." (Approved by Senate May 14, 2002)

Academic Integrity: Laurier is committed to a culture of integrity within and beyond the classroom. This culture values trustworthiness (i.e., honesty, integrity, reliability), fairness, caring, respect, responsibility and citizenship. Together, we have a shared responsibility to uphold this culture in our academic and non-academic behaviour. The University has a defined policy with respect to academic misconduct. As a Laurier student you are responsible for familiarizing yourself with this policy and the accompanying penalty guidelines, some of which may appear on your transcript if there is a finding of misconduct. The relevant policy can be found at Laurier's academic integrity website along with resources to educate and support you in upholding a culture of integrity. Ignorance is not a defense.

3. Classroom Use of Electronic Devices: The use of electronic devices in the classroom is governed by WLU Policy 9.3: *Policy on the Classroom Use of Electronic Devices*. Details of this Policy and the consequences of breaches are stated in the Academic Calendar. Mobile devices are permitted in this course provided they do not detract from the learning of any student, for example by noise level or by the display of distracting or disturbing content. Responsibility for enforcing this rule rests with both the instructor and the students. Students who do not feel comfortable approaching another student can email or talk to the instructor in person. Students who fail to comply with this policy may receive a verbal and/or written warning, or may be asked to leave the classroom for all or part of the course.

4. Late Assignment Policy: Late assignments are not accepted without a valid, documented excuse.

5. Final Examinations: Students are strongly urged not to make any commitments (i.e., vacation) during the examination period. Students are required to be available for examinations during the examination periods of all terms in which they register. Refer to the Handbook on Undergraduate Course Management for more information.

6. **Foot Patrol, the Wellness Centre, and the Student Food Bank:** The University approved the inclusion of information about select wellness and safety services and supports on campus in the course

information provided to students. (Approved by Senate November 28, 2011.) Specific language (by campus) is provided below.

Multi-campus Resource:

- Good2Talk is a postsecondary school helpline that provides free, professional and confidential counselling support for students in Ontario. Call 1-866-925-5454 or through 2-1-1. Available 24-7.

Kitchener/Waterloo Resources:

- Waterloo Student Food Bank: All students are eligible to use this service to ensure they're eating healthy when overwhelmed, stressed or financially strained. Anonymously request a package online 24-7. All dietary restrictions accommodated.
- Waterloo Foot Patrol: 519.886.FOOT (3668). A volunteer operated safe-walk program, available Fall and Winter daily from 6:30 pm to 3 am. Teams of two are assigned to escort students to and from campus by foot or by van.
- Waterloo Student Wellness Centre: 519-884-0710, x3146. The Centre supports the physical, emotional, and mental health needs of students. Located on the 2nd floor of the Student Services Building, booked and same-day appointments are available Mondays and Wednesdays from 8:30 am to 7:30 pm, and Tuesdays, Thursdays and Fridays from 8:30 am to 4:15 pm. Contact the Centre at x3146, wellness@wlu.ca or @LaurierWellness. After hours crisis support available 24/7. Call 1-844-437-3247 (HERE247).

Brantford Resources:

- Brantford Student Food Bank: All students are eligible to use this service to ensure they're eating healthy when overwhelmed, stressed or financially strained. Anonymously request a package online 24-7. All dietary restrictions accommodated.
- Brantford Foot Patrol: 519-751-PTRL (7875). A volunteer operated safe-walk program, available Fall and Winter, Monday through Thursday from 6:30 pm to 1 am; Friday through Sunday 6:30 pm to 11 pm. Teams of two are assigned to escort students to and from campus by foot or by van.
- Brantford Wellness Centre: 519-756-8228, x5803. Students have access to support for all their physical, emotional, and mental health needs at the Wellness Centre. Location: Student Centre, 2nd floor. Hours: 8:30 am to 4:15 pm Monday through Friday. After hours crisis support available 24/7. Call 1-884-437-3247 (HERE247).