WILFRID LAURIER UNIVERSITY
LAURIER
Inspiring Lives.

CP 460 - Applied Cryptography

Course Outline

Department of Physics and Computer Science
Faculty of Science, Waterloo

Abbas Yazdinejad, Ph.D.

Fall 2024

Welcome Section, CP 460

- **Course Instructor**
  - **Abbas Yazdinejad, Ph.D.**
    - Designing the course content
    - Teaching: deliver lectures
    - Assessing student performance

Contact Information: ayazdinejad@wlu.ca

- **Instructional Assistant (IA)**

Froila Stephanie Penta Antony Raj
pent5530@mylaurier.ca

Lecture: Mondays- Wednesdays at 5:30 PM – 6:50 PM

Which contents will we cover in the course?

- **Introduction to Cryptography and Data Security**
- **Stream Ciphers**
- **The Data Encryption Standard (DES) and Alternatives**
- **The Advanced Encryption Standard (AES)**
- **More About Block Ciphers**
- **Introduction to Public-Key Cryptography**
- **The RSA Cryptosystem**
- **Elliptic Curve Cryptosystems**
- **Digital Signatures**
- **Message Authentication Codes (MACs)**
- **Key Establishment**

Course prerequisites, and Goals

- Pre-requisites : MA121, CP213 or CP264

Required Textbook(s):
Understanding Cryptography -A textbook for students and practitioners. C. Paar and J. Pelzl. Springer, 2010

Course Goals and Learning Outcomes
On the successful completion of this course, students will be able to:

- Understand the concept of block cipher, stream cipher, AES, RSA, Hash function, digital signature, authentication.
- Explain the differences and similarity between stream cipher and block cipher.
- Understand the algorithm of Data Encryption Standard
- Understand the algorithm of Advance Encryption Standard (AES) and its mathematical background.
- Understand the concept of mode of operations in symmetric key cryptography and its applications.
- Understand the mechanism of RSA.
- Explain the mechanism of digital signature algorithm and its applications.
- Explain the mechanism of authentication and authenticated encryption methods and compare their differences.
- Understand the concept of digital certificate and compare the difference between digital signature algorithm and digital certificate.
- Understand the mechanism of public-key infrastructures and its applications.

Course Schedule

Week	Topics	Data	Tentative Schedule
Week 1	Introduction to applied cryptography, Modular Arithmetic (Chapter 1); Stream cipher (Chapter 2)	Sep 9 - 11	
Week 2	Stream cipher (Chapter 2); Block cipher, DES (Chapter 3)	Sep 16 - 18	*Project Proposal, Sep 16*
Week 3	Field and its arithmetic operations, AES (Chapter 4)	Sep 23 - 25	*Project Proposal Due, Sep 25*
Week 4	RSA algorithm (Chapter 7)	Sep30–Oct 2	*Assignment 1, Sep30*
Week 5	Review previous content and Project discussion, Test 1	Oct 7 - 9	*Test 1 in class, Oct 9*
Week 6	Reading Week→ No class and no Lecture	Oct 14 - 16	
Week 7	Diffie-Helmen key exchange and Elgamal encryption, ECC (Chapter 8, 9)	Oct 21 - 23	*Assignment 1 Due, Oct 21*
Week 8	Mode of operations (Chapter 5)	Oct 28 - 30	
Week 9	Message authentication (Chapter 11, 12)	Nov 4 - 6	*Assignment 2, Nov 4*
Week 10	Digital signatures (Chapter 10); Key management (Chapter 13)	Nov 11 - 13	
Week 11	Public key infrastructure (Chapter 6)	Nov 18 - 20	*Assignment 2 Due, Nov 20*
Week 12	Makeup session, Test 2	Nov 25 - 27	*- Test 2 in class, Nov 25* *- Project Report Due, Nov 27*
Final Exam	**In Person**	**Dec 9**	

Any changes regarding the important dates will be announced on MyLS

Class Policy

You are expected to be familiar with the contents of the course syllabus

- Available on the course home page, MyLearning space
- If you haven’t read it, read it after this lecture

Final Examinations: Students are strongly urged not to make any commitments (e.g., 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.

Use of Artificial Intelligence (e.g., ChatGPT) in this course

The development of increasingly sophisticated AI systems such as ChatGPT poses potential threats to academic integrity. Unauthorized student use of AI systems undermines student learning, the achievement of learning outcomes and violates the University’s academic misconduct policies.

Course website

We will use MyLearning space

- The website will be updated regularly
- Syllabus, Calendar, lecture notes, Additional materials, assignments, announcements, policies, etc.
- It is your responsibility to keep up with the information on the course website.

- You must keep up with any information posted on MyLearning space

Plagiarism and academic offenses

University and Course Policies

Academic Calendars: Students are encouraged to review the Academic Calendar and MyLearning Space for information regarding all important dates, deadlines, announcement regarding the course and services available on campus.

- Read this and understand it
  - Ignorance is no excuse!
  - Questions should be brought to instructor
- Plagiarism applies to both text and code
- You are free (even encouraged) to exchange ideas, but no sharing code or text

Turnitin (Plagiarism detection software)

In this course, your instructor may be using Turnitin, integrated with the MyLearning space Dropbox tool, to detect possible plagiarism, unauthorized collaboration or copying as part of the ongoing efforts to maintain academic integrity at the University of Guelph. All submitted assignments will be included as source documents in the Turnitin.com reference database solely for the purpose of detecting plagiarism of such papers. Use of the Turnitin.com service is subject to the Usage Policy posted on the Turnitin.com site.

Plagiarism and academic offenses

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 MyLearning Space, are the intellectual property of the course instructors. These materials have been developed for student 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 course content to third-party websites violates instructors' 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 instructors. Failure to follow these instructions may be in contravention of the university's Student Non-Academic Code of 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 5

relevant University Policies, and to respect the intellectual property of others during and after their association with Wilfrid Laurier University.

Accessibility : Students requiring accommodation are advised to contact Laurier's Accessible Learning Centre Accessible Learning | Future Undergraduate Students | Wilfrid Laurier University (wlu.ca) for information regarding its services and resources.

Assignments

- Assignments/Labs/Project, etc. will be due at 11:59 PM
- Late submissions will be accepted up to 24 hours after due date with 20% Penalty.
- No assignment will be accepted after the 24-hour grace period

Late policy

- The purpose of the late policy is to deal with temporary problems occurring before the assignment due date
- If the problem occurs only during the 24 hours after the due date, you are out of luck
  - Submit early and submit often
- You must notify your instructor well before the due date of any severe, long-lasting problems that prevent you from completing an assignment on time

Student Assessment

To complete this course, students are required to participate in regular classes, complete the assignments and quizzes and develop a cryptography algorithm, present the project, write project reports, and complete the final exam. Please refer to the table below for details.

Assessment	Weighting
Assignments (2×10)	20%
Tests (2×10)	20%
Project	30%
Final Exam	30%
Total	100%

- See syllabus for late and reappraisal policies, academic integrity policy, and other details

Thank
You