

COURSE OUTLINE

ECE 519C –Selected Topics In Secure Communications: Applied Cryptography

Term – SPRING 2020 (202001)

Instructor

Dr. Riham AlTawy
Phone: 250-721-8639
E-mail: raltawy@uvic.ca

Office Hours

Days: Tuesday and Friday
Time: 13:00 – 14:00
Location: EOW 431

Course Objectives

- Introduce the basic foundational concepts underlying classical and modern cryptography.
- Reason about how security is defined at the cryptographic level and how high level implementations affect the overall system security.
- Investigate common cryptanalytic methods and how to mitigate them.
- Apply appropriate cryptographic techniques to different security engineering problems.

Learning Outcomes

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

- Understand modern concepts related to cryptography and cryptanalysis.
- Analyze and use methods for cryptography and reflect about their limits and applicability.
- Implement some symmetric key ciphers and some toy examples (or textbook versions) of public key systems
- Reason about the details and design philosophy of modern symmetric and public key systems
- Have a better appreciation of the uses and limitations of the various categories of cryptographic algorithms and understand that great care is needed in their selection and use
- Reason that security is a systems problem, and that technical methods such as cryptography can only form part of the solution.

Syllabus

The following set of slides (will be available at Coursespaces) will be covered in the order below.

- Introduction and classical ciphers
- Block ciphers
- Introduction to Number theory
- RSA
- Stream ciphers
- Hash functions
- Other public key systems and signature schemes
- Odds and ends

A-Section(s): A01 / CRN 23960, A02 / CRN 23961

Days: Tuesday and Friday

Time: T: 14:30 – 16:20, F: 14:30 – 15:20

Location: ECS 125

Optional Text

Title: **Handbook of Applied Cryptography**

Author: Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone

Publisher: CRC press, ISBN: 0-8493-8523-7

Free copy of the book is available online www.cacr.math.uwaterloo.ca/hac

Assessment:

Assignments:	20%	Due Dates: 1 st (resp. 2 nd) assignment is due on Jan. 31 (resp. Mar. 20)
Mid-term 1	30%	Date: Feb. 11 (Tentative. See Notes)
Mid-term 2	20%	Date: Mar. 16
Quiz	10%	Date: Mar. 30
Project	20%	Due on the last day of classes (Apr. 3)

The final grade obtained from the above marking scheme for the purpose of GPA calculation will be based on the percentage-to-grade point conversion table as listed in the current Graduate Calendar.

<https://web.uvic.ca/calendar2020-01/grad/academic-regulations/grading.html>

Notes

- Mid-terms: The first midterm will be held after partially covering the RSA system. Exact time for the midterm, project presentations will be announced in class.
- There will be **NO** makeup for the 1st midterm. In the case of a serious illness or emergency, the weight of the midterm will be moved towards the second midterm and quiz proportionally. Be prepared to provide written documentation (e.g., a medical excuse from your doctor) to verify the emergency and its seriousness.
- **Late policy for assignments and project**
Cumulative of 10% times number of days late
 - 1 day late: lose 10%
 - 2 days late: lose 30% (10% + 20%)
 - 3 days late: lose 60% (30% + 30%)
 - Greater than 4 days late not accepted.

Note to Students:

Students who have issues with the conduct of the course should discuss them with the instructor first. If these discussions do not resolve the issue, then students should feel free to contact the Chair of the Department by email or the Chair's Secretary to set up an appointment.

Course Withdrawal Deadlines:

- January 19: Withdrawal with 100% reduction of tuition fees
- February 9: Withdrawal with 50% reduction of tuition fees
- February 29: Last day for withdrawal (no fees returned)

Accommodation of Religious Observance:

<https://web.uvic.ca/calendar2020-01/grad/registration/Registration.1.17.html#>

Policy on Inclusivity and Diversity:

<https://web.uvic.ca/calendar2020-01/general/policies.html>

Standards of Professional Behaviour:

You are advised to read the Faculty of Engineering document Standards for Professional Behaviour, which contains important information regarding conduct in courses, labs, and in the general use of facilities.

<http://www.uvic.ca/engineering/assets/docs/professional-behaviour.pdf>

Cheating, plagiarism and other forms of academic fraud are taken very seriously by both the University and the Department. You should consult the entry in the current Graduate Calendar for the UVic policy on academic integrity.

<https://web.uvic.ca/calendar2020-01/grad/academic-regulations/academic-integrity.html>

Equality:

This course aims to provide equal opportunities and access for all students to enjoy the benefits and privileges of the class and its curriculum and to meet the syllabus requirements. Reasonable and appropriate accommodation will be made available to students with documented disabilities (physical, mental, learning) in order to give them the opportunity to successfully meet the essential requirements of the course. The accommodation will not alter academic standards or learning outcomes, although the student may be allowed to demonstrate knowledge and skills in a different way. It is not necessary for you to reveal your disability and/or confidential medical information to the course instructor. If you believe that you may require accommodation, the course instructor can provide you with information about confidential resources on campus that can assist you in arranging for appropriate accommodation. Alternatively, you may want to contact the Centre for Accessible Learning located in the Campus Services Building. <https://www.uvic.ca/services/cal/>. The University of Victoria is committed to promoting, providing, and protecting a positive, and supportive and safe learning and working environment for all its members.

Course Lecture Notes:

Unless otherwise noted, all course materials supplied to students in this course have been prepared by the instructor and are intended for use in this course only. These materials are NOT to be re-circulated digitally, whether by email or by uploading or copying to websites, or to others not enrolled in this course. Violation of this policy may in some cases constitute a breach of academic integrity as defined in the UVic Calendar.

Sexualized Violence Prevention and Response at Uvic:

UVic takes sexualized violence seriously, and has raised the bar for what is considered acceptable behaviour. We encourage students to learn more about how the university defines sexualized violence and its overall approach by visiting www.uvic.ca/svp. If you or someone you know has been impacted by sexualized violence and needs information, advice, and/or support, please contact the sexualized violence resource office in Equity and Human Rights (EQHR). Whether or not you have been directly impacted, if you want to take part in the important prevention work taking place on campus, you can also reach out:

Where: Sexualized violence resource office in EQHR; Sedgewick C119

Phone: 250.721.8021

Email: svpcoordinator@uvic.ca

Web: www.uvic.ca/svp

Office of the Ombudsperson:

The [Office of the Ombudsperson](https://uvicombudsperson.ca/) is an independent and impartial resource to assist with the fair resolution of student issues. A confidential consultation can help you understand your rights and responsibilities. The Ombudsperson can also clarify information, help navigate procedures, assist with problem-solving, facilitate communication, provide feedback on an appeal, investigate and make recommendations. Phone: 250-721-8357; Email: ombuddy@uvic.ca; Web: <https://uvicombudsperson.ca/>