Course Name Number (ECE519C) – SELECTED TOPICS IN SECURE COMM: Cryptography

Term – Spring 2019 (201901)

Instructor
Dr. Morteza Esmaeili
Phone: 778-650-3910
E-mail: mesmaeil@engr.uvic.ca

Office Hours
Days & Time: Mondays 1:30—2:30
Thursdays 12:30—1:30
Location: EOW 419

Course Objectives
*Introduction and studying security related issues in computer and communication technology.
*Studying fundamental concepts and techniques of modern cryptography.
*To study some of the most recent techniques of cryptography used in technology from both the theory and engineering perspectives.

Learning Outcomes
As per the course objectives, students who successfully pass the course, would have a good understanding of security issues in communications engineering, and have the basic knowledge to work in this subfield of communications theory in any related project.

Syllabus
Classical cryptography; Security and Information Theory; Block ciphers and their security potential (including AES and DES); Some known attacks on block ciphers; RC4 and LFSR-based stream ciphers and their security; Principle of public-key cryptography; Hybrid cryptography and its applications.

A-Section(s): 24041 ECE 519C A01 / 24042 ECE 519C A02
Days: Mon-Th
Time: M-3:30-4:50 & Th-2:30-3:50
Location: Mon: Cornett Building A129
          Th: Elliott Building 061

Required Text
Title: Cryptography: Theory & Practice, 4th edition
Author: D.R. Stinson & M.B. Paterson
Publisher: CRC press
Year: 2018

Optional Text
Title: Introduction to Modern Cryptography
Author: J. Katz & Y. Lindell
Publisher: CRC press
Year: 2015

References: The mentioned texts and journal papers
Assessment:
Assignments: 20%  
Due Dates: : Jan 28, Feb 11, Feb 25, March 11, March 25
Project 15%
Mid-term 30%  
Date: Feb 21
Final Exam 35%

Note: Failure to pass the final exam will result in a failing grade for the course.

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/calendar2019-01/grad/academic-regulations/grading.html

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 Assistant to set up an appointment.

Accommodation of Religious Observance:  
https://web.uvic.ca/calendar2019-01/grad/registration/Registration.1.17.html#

Policy on Inclusivity and Diversity:  
https://web.uvic.ca/calendar2019-01/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.  
https://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/calendar2019-01/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 Resource Centre for Students with a Disability located in the Campus Services Building.

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

Updated November 20, 2018
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](http://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](mailto:svpcoordinator@uvic.ca)
- **Web:** [www.uvic.ca/svp](http://www.uvic.ca/svp)