06-88-566-01 Data Security and Cryptography

Course Syllabus

Faculty of Engineering, Department of Electrical and Computer Engineering

University of Windsor, Canada

Fall 2014

Please note: This syllabus will be discussed during the first class meeting, and an electronic copy will be available at CLEW course website.

Course, Instructor/Professor, and Graduate Assistant (GA) Details

Class Hours: 1:00—3:50pm, Tue., CEI 2100 (The 1st class is on Sept 9, 2013)
Professor: Dr. Huapeng Wu
Office: CEI 3049, Phone: 519-253-3000 Ext. 2568
Email: hwu@uwindsor.ca (E-mail anytime is welcomed. Please add [88-566] to your email subject.)
Office Hours: 1:30pm-2:30pm, every Monday and Wednesday between Sept 8 and Dec 3. Office Hours during final exam period will be announced later in class and on CLEW.
Midterm: Closed-book, two-page of formula sheets allowed (single-side, letter size), Date: Oct. 14**.**
Final Examination: Closed-book, four-page of formula sheets (single-side, letter size), Date: Dec 11.
Graduate Assistant: TBA, responsible for grading assignments and projects**.**
Course Website: CLEW website

Course Description

This is an introductory course on the techniques, algorithms, architectures and tools used for data security and cryptography. The theoretical aspects of data security and cryptographic algorithms and protocols are firstly reviewed. Then we show how these techniques can be integrated to provide solutions to particular data and communication security problems. The course contents are of use to computer and communication engineers who are interested in embedding security services into an information system, and thus providing integrity, confidentiality and authenticity of the data to the communicating parties. Main contents: classical cryptography techniques; mathematical foundations; secret key cryptography; public key cryptography; authentication and digital signature; network cryptographic protocols.
Prerequisite: Graduate Student Status, ***Programming skill with a major computer language*** and substantial knowledge on computer/communication networks.
3 lecture hours a week. Credit Weight 3.

Objective:

Network security, especially wireless network security, has been paid much attention recently because of the prevailing use of the Internet and the increasing importance of the networks in our daily life. Cryptographic techniques have enabled various network security services that provide most secure

networking protocols today. This course is an introduction to the techniques, algorithms, architectures and tools of cryptography and data security. It is intended to be offered to the graduate students who will work in network security, communication, computer, and DSP areas, although it is also beneficial to the students in electrical engineering and computer science in general.

Textbook (Required):

Understanding Cryptography, by C.Paar and J.Pelzl, ISBN 978-3-642-04100-6, e-ISBN: 978-3-642-04101-3, Springer-Verlag, 2010 (required)
Introduction to Cryptography with Coding Theory, 2nd Edition, (hardcover), by Wade Trappe and Lawrence C. Washington, Pearson/Prentice Hall, New Jersey, 2006. ISBN: 0-13-186239-1(optional)

Learning Outcomes

In this course, students will be able to

1	Obtain an in-depth knowledge of contemporary cryptography, understand the electrical and computer software behavior of security schemes and design building blocks of security schemes.
2	Identify design problems of security schemes, read research articles in this area and evaluate research studies as well as conducting independent research projects.
3	Explain the behavior of advanced cryptography systems, describe their performance parameters, and examine security scheme design methodologies.
4	Interpret the terminology related to contemporary cryptography and use software tools to simulate, optimize and validate the design parameters of security schemes.
5	Get involved in team works and independent studies through course assignments and projects.
6	Improve interpersonal skills and communications by presenting their projects and interacting with the instructor and other students.
7	The course includes a group based project requiring teamwork and collaboration skills.
8	Be creative to develop new idea in the area of contemporary cryptography, ability to critically apply knowledge of security scheme design to problems, write technical reports in a professional manner.
9	Realize the importance of contemporary cryptography and data security and establish the foundation for further study in this area.

This course will develop the following CEAB Graduate Attributes Criteria via Learning Outcomes:

CEAB Graduate Attributes Criteria	Course Learning Outcomes
1. A knowledge base for engineering ***Demonstrated competence in University level mathematics, natural sciences, engineering fundamentals, and specialized engineering knowledge appropriate to the program.***	1,2,3,4,8
2. Problem analysis ***An ability to use appropriate knowledge and skills to identify, formulate, analyze, and solve complex engineering problems in order to reach substantiated conclusions.***	1,2,3
3. Investigation ***An ability to conduct investigations of complex problems by methods that include appropriate experiments, analysis and interpretation of data, and synthesis of information in order to reach***	1,2,3,6

valid conclusions.	
4. Design ***An ability to design solutions for complex, open-ended engineering problems and to design systems, components or processes that meet specified needs with appropriate attention to health and safety risks, applicable standards, economic, environmental, cultural and societal considerations.***	2,3,8
5. Use of engineering tools ***An ability to create, select, apply, adapt, and extend appropriate techniques, resources, and modern engineering tools to a range of engineering activities, from simple to complex, with an understanding of the associated limitations.***	1,2,4
6. Individual and team work ***An ability to work effectively as a member and leader in teams, preferably in a multi-disciplinary setting.***	5,6,7
7. Communication skills ***An ability to communicate complex engineering concepts within the profession and with society at large. Such abilities include reading, writing, speaking and listening, and the ability to comprehend and write effective reports and design documentation, and to give and effectively respond to clear instructions.***	6,7,8
8. Professionalism ***An understanding of the roles and responsibilities of the professional engineer in society, especially the primary role of protection of the public and the public interest.***	9
9. Impact of engineering on society and the environment ***An ability to analyse social and environmental aspects of engineering activities. Such abilities include an understanding of the interactions that engineering has with the economic, social, health, safety, legal, and cultural aspects of society; the uncertainties in the prediction of such interactions; and the concepts of sustainable design and development and environmental stewardship.***	9
10. Ethics and equity ***An ability to apply professional ethics, accountability, and equity.***	8,9
11. Economics and project management ***An ability to appropriately incorporate economics and business practices including project, risk and change management into the practice of engineering, and to understand their limitations.***	5,7,9
12. Life-long learning ***An ability to identify and to address their own educational needs in a changing world, sufficiently to maintain their competence and contribute to the advancement of knowledge.***	9

Course Schedule

The following course schedule is approximate.

Week	Date	Subject, activity, assignment, etc.	Textbook Chapter or Readings
1		Discussion on syllabus, Chapter 1. Introduction to Data Security and Applications	Courseware

2		Chapter 2. Classical Ciphers	Courseware
3		Chapter 2. Classical Ciphers Chapter 3. Mathematical Preliminaries	Courseware
4		Chapter 3. Mathematical Preliminaries	Courseware
5		Chapter 3. Mathematical Preliminaries Chapter 4. Steam Ciphers	Courseware
6		Chapter 5. AES: Advanced Encryption Standard	Courseware
7		Chapter 6. RSA: Public Key System	Courseware
8		Chapter 6. RSA: Public Key System	Courseware
9		Chapter 7. Hash Function and Signature	Courseware
10		Chapter 7. Hash Function and Signature Chapter 8. Key Establishment	Courseware
11		Chapter 9. Security Protocols	Courseware
12		Chapter 10. Post-Quantum Cryptography A Brief Review of the Course Information on the Final Exam	Courseware
13		n.a.	Courseware

Lab/Tutorial Schedule

- Solution to assignments will be posted on the course CLEW website usually on the fourth day after the submission deadline.
- The first 20 minutes of the first lecture after the assignment marked and returned will be used as tutorial time to discuss the common issues in solving the assignment problems.

Evaluation Methods

The course grade will be evaluated as follows:

Method of Evaluation	% of Final Grade	Due Dates*	Related Learning Outcomes
Assignments or reports Approximately 4 (Individual)	10%	Click here to enter a date.	2,4,5,6,7,8,9
Midterm exam (Closed-book)	20%	15/10/2013	1,2,5,6,7
About 2 Projects (one team-work, and the other (Individual)	25%	Click here to enter a date.	1,2,3,4,5,6,7,8
Final exam (Closed-book)	45%	10/12/2013	1,2,5,6,7

*** According to Bylaw 51, Section 1.1.2 and 1.1.3 respectively,**

http://athena.uwindsor.ca/units/senate/main.nsf/947f0bc672983a17852568b60051f690/bf28934998d7c7c3852578c3006e22d7/$FILE/Bylaw%2051%20-%20Examination%20Procedures%20(Amended%20091209).pdf

"**Two to three hour examination slots** will normally be scheduled in the formal final examination periods in each semester for all courses which terminate in that semester. All final testing procedures (written test, oral interview, essay, take home test, etc.) shall take place (or fall due, as the case may be) during the two to three-hour final examination slot so scheduled. The actual duration of testing procedures during the scheduled final examination slot may be less than the scheduled time, at the discretion of the individual instructor" (Bylaw 51, Section 1.1.2).

"The last seven calendar days prior to, and including, the last day of classes in each period of instruction of twelve (or greater) weeks in duration must be free from any procedures for which a mark will be assigned, including the submission of assignments such as essays, term papers, and take home examinations. Courses that are presented by a specialized teaching method, where the testing procedures are an integral part of the instructional process, shall be exempt from this regulation subject to approval of the Dean of the Faculty in which the course is given" (Bylaw 51, Section 1.1.3).

Grading

Grades for the course will be consistent with the following table, per the University of Windsor Policy P1: Standardization of Percentages Across the University

http://athena.uwindsor.ca/units/senate/main.nsf/947f0bc672983a17852568b60051f690/3c87fa97b5f64f7c852578ef006c00be/$FILE/Policy%20P1%20-%20Standardization%20of%20Percentages%20Across%20the%20University.pdf

☐ Graduate Course:

Numerical	90-100	85-89.9	80-84.9	77-79.9	73-76.9	70-72.9	67-69.9	63-66.9	60-62.9	35-59.9	00-34.9
Letter	A+	A	A-	B+	B	B-	C+	C	C-	F	F-

Assessment Considerations

Assignments:

There are four assignments. All assignments should be submitted through the course CLEW website. No email submission or hardcopy submission is allowed. If a student is experiencing difficulty meeting a deadline, he/she is encouraged to contact the course instructor as soon as possible to discuss the situation in advance of the deadline. Late assignments will be deducted 10% per day up to 3 days (after which they will receive 0 marks).

Projects:

There are two projects, one is individual based and the other is group based. For group based project, a group up to two students should be formed and emailed to the GA within one week after the project information is posted at the course CLEW website. All project reports should be submitted through the course CLEW website. No email submission or hardcopy submission is allowed. If a student is experiencing difficulty meeting a deadline, he/she is encouraged to contact the course instructor as soon as possible to discuss the situation in advance of the deadline. Late project reports will be deducted 10% per day up to 3 days (after which they will receive 0 marks).

Midterm:

Mid-term examination is closed-book, but two pages (single-side, letter size) of formula sheets are allowed. No electronic devices except for a non-programmable calculator are allowed in the examination. Missing midterm with legitimate reason will be treated that the weight of midterm will be moved to the final examination.

Final Exam:

Final examination is closed-book, but four pages (single-side, letter size) of formula sheets are allowed. No electronic devices except for a non-programmable calculator are allowed in the examination.

Calculators

Only non-programmable is allowed during tests/exams.

Other Electronic Devices Aside from Calculators

- ■ Electronic devices aside from calculators are **NOT** permitted during exams.
- □ Other electronic devices aside from calculators are permitted during Tests / exams / both?. Acceptable electronic devices include: Please state

The Student Evaluation of Teaching (SET)

The SET will be administered in the course during the last two weeks of the semester.

Exams and fire alarms

Pulling a fire alarm (e.g. during an exam) is a serious offence. The Criminal Code of Canada dictates that initiating a false alarm is a **criminal offence**. Such an offence could result in a criminal record, a large fine, as well as disciplinary action under the University of Windsor Bylaw 31 where serious consequences would be likely (see Appendices for student misconduct).

In the event that a fire alarm disrupts an exam session, the decision on how to proceed or not proceed with the exam will be made by the instructor. Therefore, if students are evacuated from the building due to a fire alarm they should wait outside and receive instructions from the instructor.

Supplemental Privileges

- ■ A supplemental examination is **NOT** allowed in this course.
- □ A supplemental examination is allowed in this course.

.

General Class Expectations

Attendance and punctuality

Attendance in classes and labs is critical to student success; students should seize the opportunity to share and discuss information in labs, tutorials, and classes. The course is designed to move swiftly and efficiently.

Communication

Students are encouraged to utilize office hours to ask questions. Emails will be responded to within 24 hours Monday to Friday. Only emails sent from a uwindsor email address will be responded to. Emails should include "[88-566]" in the subject.

Group work

Project may require group work. A group up to two students should be formed within one week after the project information is posted at the course CLEW website. It should be indicated who is going to submit the project report on behalf of the group.

Academic Integrity

Per the University of Windsor Bylaw 31: Student Affairs and Integrity

http://athena.uwindsor.ca/units/senate/main.nsf/947f0bc672983a17852568b60051f690/06e37bd761de3505852578c30069a8f8/$FILE/Bylaw%2031%20-%20Student%20Affairs%20Amended%2020080110%20-%20RW%20reviewed%20Sept%2028,%202011.pdf

Plagiarism: *the act of copying, reproducing or paraphrasing portions of someone else's published or unpublished material (from any source, including the internet), without proper acknowledgement. Plagiarism applies to all intellectual endeavours: creation and presentation of music, drawings, designs, dance, photography and other artistic and technical works. In the case of oral presentations, the use of material that is not one's own, without proper acknowledgment or attribution, constitutes plagiarism and, hence, academic dishonesty. (Students have the responsibility to learn and use the conventions of documentation as accepted in their area of study.)*

For more information on academic integrity and student misconduct please see the appendices.

CEAB Hours

Subject Areas	**Accreditation Units** One hour of lecture (corresponding to 50 minutes of activity) = 1AU One hour of laboratory or scheduled tutorial = 0.5 AU
Mathematics	9
Natural Sciences	-

Engineering Science	9
Engineering Design	18
Complementary Studies	-

Will there be a laboratory experience and safety procedures instruction? ☐ Yes ■No

Services Available to Students at the University of Windsor

Students are encouraged to discuss any disabilities, including questions and concerns regarding disabilities, with the course instructor. Let's plan a comfortable and productive learning experience for everyone. The following services are also available to students:

- Student disability services: http://www.uwindsor.ca/disability
- Skills to enhance personal success (S.T.E.P.S):
    - http://www.uwindsor.ca/lifeline/steps-skills-to-enhance-personal-success
- Student counseling centre: http://www.uwindsor.ca/scc
- Academic advising centre: http://www.uwindsor.ca/advising/