INSE 6110 Foundations of Cryptography (4 credits)

1 General Information

- Course name: INSE6110 Foundations of Cryptography
- Lecture time & location: Tuesdays, 20:30-23:00, H-431 (Hall building)
- Instructor: Mohammad Mannan, Concordia Institute for Information Systems Engineering, ENCS.
- Office: EV6.221 (EV building, 6th floor)
- Email: mmannan@ciise.concordia.ca
- Office hours: Tuesdays from 13:00-14:30
- Course website (general info): http://www.encs.concordia.ca/~mmannan/teaching/inse6110-winter2012.html
- Course materials: **accessible only on Moodle (via MyConcordia.ca)**

2 Course Description

- This course is an introduction to the basic theory of cryptographic techniques used for information security. It is intended for graduate students with basic computer science/engineering background and is a prerequisite for (INSE6120, INSE6130, INSE6140, and INSE6150).
- The following topics will be covered (if time allowed): Cryptography and cryptanalysis, mathematical background: complexity theory, number theory, abstract algebra, finite fields. Number theoretic reference problems: the integer factorization problem, the RSA problem, the quadratic residuosity problem, computing square roots in Zn, the discrete logarithm problem, the Diffie-Hellman problem, pseudorandom bits and sequences, stream ciphers: feedback shift registers, LFSRs, RC4. Block ciphers: SPN and Fiestel structures, DES, AES, linear cryptanalysis, differential cryptanalysis, side channel attacks; public key encryption: RSA, Rabin, ElGamal, McEliece, elliptic curves cryptography; hash functions: un-keyed hash functions, MACs, attacks; digital signatures: RSA, Fiat-Shamir, DSA, public key infrastructure; key management, efficient implementation of ciphers.
- Prerequisites: This course has no formal prerequisites, however you are assumed to be competent in basic mathematical algebra, manipulation of formulae and simple polynomial arithmetic.

3 Learning Outcomes

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

1. Understand modern concepts related to cryptography and cryptanalysis.
2. Analyze and use methods for cryptography and reflect about limits and applicability of these methods.
3. Implement some symmetric key ciphers and some toy examples (or textbook versions) of public key systems.
4. Reason about the details and design philosophy of modern symmetric and public key systems.
5. 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.
6. Reason that security is a systems problem, and that technical methods such as cryptography can only form part of the solution.

4 Tentative Schedule

The following set of slides (available from the Moodle course site) will be covered in the order below.

1. Introduction and classical ciphers
2. Block ciphers
3. Stream ciphers
4. Hash functions
5. Message Authentication Codes (MACs)
6. Public key cryptography
7. RSA encryption
8. Other public key systems and signature schemes
9. Authentication, secret sharing, key establishment & miscellaneous topics

The midterm will be held close to mid-February. Exact time for the midterm, the project presentations/report submission and the final exam will be announced in class. The final exam will be scheduled by the University examination office during the final exam period.

5 Course Materials

1. Optional Textbook: Handbook of Applied Cryptography,
   - Authors: 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
   - A copy of the book is available in the library. The library also has a very good selection of many introductory books to the subject.
2. Optional Textbook: Cryptography and Network Security: Principles and Practice, fifth edition
   - Authors: William Stallings.
   - Publisher: 978-0-13-609704-4
   - Older editions (e.g., 3e) are fine (much cheaper than 5e, see Amazon.com)

6 Marks Distribution

1. **35%**: Assignments/Projects (may include programming, report writing and presentations)
2. **25%**: Midterm exam
3. **40%**: Final exam

Late Assignments: All assignments/projects will be due in class (unless otherwise specified). Late assignments suffer a penalty rate of 20% per day, up to 5 days (weekends count).

Midterm Makeup: There will be NO makeup for the midterm. In the case of a serious illness or emergency, the weight of the midterm will be moved towards the final exam. Be prepared to provide written documentation (e.g., a medical excuse from your doctor) to verify the emergency and its seriousness.

7 Academic Code of Conduct

Any form of cheating, plagiarism, impersonation, falsification of a document as well as any other form of dishonest behaviour by a student is an academic offence under the Academic Code of Conduct and may lead to severe academic penalties up to and including suspension and expulsion. As examples only, you are not permitted to:

- Copy from anywhere without indicating where it came from
- Let another student copy your work and then submit it as his/her own
- Hand in the same assignment in more than one class
- Have unauthorized material or devices in an exam. Note that you do not have to be caught using them just having them is an offence
- Copy from someones else exam
- Communicate with another student during an exam
- Add or remove pages from an examination booklet or take the booklet out of an exam room
- Acquire exam or assignment answers or questions
- Write an exam for someone else or have someone write an exam for you
- Submit false documents such as medical notes or student records
- Falsify data or research results

For details of the Academic Code of Conduct, see: provost.concordia.ca/academicintegrity/

8 Students' Responsibilities

1. Students are expected to attend every class. Some material may only be covered in class and not made available on the course website. Students are expected to read the assigned material and to actively participate in class discussions.
2. Students are expected to be respectful of other peoples opinions and to express their own views in a calm and reasonable way. Disruptive behaviour will not be tolerated. Students are expected to be familiar with the Code of Rights and Responsibilities: http://rights.concordia.ca
3. If you cannot attend class for any reason, unforeseen or not, you are to come and talk or write to me as soon as possible.

9 Student Services

1. Concordia Counselling and Development offers career services, psychological services, student learning services, etc. http://cdev.concordia.ca
2. The Concordia Library Citation and Cycle Guides: http://library.concordia.ca/help/howto/citations.html
3. Advocacy and Support Services: http://supportservices.concordia.ca
4. Student Transition Centre: http://stc.concordia.ca
5. New Student Program: http://newstudent.concordia.ca
6. Office for Students with Disabilities: http://supportservices.concordia.ca/disabilities/
7. The Academic Integrity Website: http://provost.concordia.ca/academicintegrity/

10 Disclaimer

In the event of extraordinary circumstances beyond the University's control, the content and/or evaluation scheme in this course is subject to change.