CSI 4108
Cryptography

Outline (Fall 2018)

| Lectures:       | Tuesday             | 10:00 to 11:30     | LPR 154 |
|                | Thursday            | 08:30 to 10:00     | LPR 285 |
| Office Hours:   | By appointment      | By appointment     | SITE 5035 |

Teaching assistant: Weiyun Lu (WLU058@uottawa.ca)

Course description (from calendar):

Prerequisites: CSI 3105  Design and Analysis of Algorithms I
MAT 2377  Probability and Statistics for Engineers

General objective for course: to present a broad overview of the field of cryptography.

Specific objectives: students should learn how and when to use particular cryptographic algorithms and protocols. For each algorithm/protocol covered in the course, students should have a good understanding of its strengths & limitations, how it works, what security service(s) it is intended to provide, and how well it achieves the intended security.

Teaching methods: in-class lectures (mostly at the board) with some topic outlines and other materials made available electronically via the course website (http://www.site.uottawa.ca/~cadams/courses/CSI4108.html).
Textbooks


Grading Scheme

Assignments [to be submitted electronically]:
- Assignment 1 (due September 21, before 16:00) 8%
- Assignment 2 (due October 5, before 16:00) 8%
- Assignment 3 (due November 9, before 16:00) 8%
- Assignment 4 (due November 30, before 16:00) 8%
Midterm examination (October 16): 20%
Final examination: 50%
**General Policies and Procedures**

**Plagiarism and Academic Integrity**
- Zero percent for work in which cheating is detected.
- Other penalties (including course failure and expulsion) are also possible.
- See [https://www.uottawa.ca/about/sites/www.uottawa.ca.about/files/plagiarism.pdf](https://www.uottawa.ca/about/sites/www.uottawa.ca.about/files/plagiarism.pdf) or [https://www.uottawa.ca/about/sites/www.uottawa.ca.about/files/plagiat.pdf](https://www.uottawa.ca/about/sites/www.uottawa.ca.about/files/plagiat.pdf)

**Academic Fraud**
- see the following link for important information:
  - [http://www.uottawa.ca/academic/info/regist/crs/0305/home_5_ENG.htm](http://www.uottawa.ca/academic/info/regist/crs/0305/home_5_ENG.htm) or [http://www.uottawa.ca/academic/info/regist/crs/0305/home_5_FR.htm](http://www.uottawa.ca/academic/info/regist/crs/0305/home_5_FR.htm)

**Course Policies**
- Zero percent for late work.
- In a 4th-year course, it is unreasonable to expect that all testable material will be covered in class (real life is not like this!). Make use of the suggested textbooks and reading material, as well as any other relevant material.
- **Electronic devices are not to be used in class without explicit permission from the instructor.**

**University of Ottawa Academic Regulations**
- [https://www.uottawa.ca/administration-and-governance/policies-and-regulations](https://www.uottawa.ca/administration-and-governance/policies-and-regulations) or [https://www.uottawa.ca/administration-et-gouvernance/politiques-et-reglements](https://www.uottawa.ca/administration-et-gouvernance/politiques-et-reglements)

**Specific University of Ottawa Academic Regulations**
- Class attendance is mandatory. As per academic regulations, students who do not attend at least 80% of the classes may not be allowed to write the final examination.
- Students must be registered in order to take the class. Students who are not officially registered cannot receive a mark.
- All components of the course (i.e., assignments, exams) must be fulfilled otherwise students may receive an INC as a final mark (equivalent to an F). This also holds for students taking a course for the second time.

Detailed Outline (Tentative)

Week

Introduction [Ch. 1]
1:
overview, model of attacker, cryptographic strength

Classical Encryption Techniques [Ch. 2]
2:
Caesar, Playfair, Hill, Vigenere, Vernam, rotor machine

Entering the Modern Era of Symmetric Ciphers [Ch. 3]
3 – 4:
SP-Network, DES, linear/differential cryptanalysis, CAST-128

Modern Symmetric Ciphers [Ch. 4-7]
5 – 6:
finite fields, AES, modes of operation, stream ciphers

Midterm (October 16)

Asymmetric (Public-Key) Encryption [Ch. 8-10]
7 – 9:
number theory, PK cryptography, trap-door function, RSA, ECC

Cryptographic Keys [Ch. 7, 10, 14]
10:
PRNG, key management, D-H protocol, ECDH

Message Authentication and Hash Functions [Ch. 11-12]
11:
MACs, hash functions, one-way functions, HMAC, SHA

Digital Signatures and Cryptographic Protocols [Ch. 13]
12:
digital signatures, RSA, DSA, bit commitment, zero-knowledge

Additional Algorithms, Protocols, and Techniques
13:
additional topics in cryptography (as time permits)

Semester Review
Dec. 4:
review of course material

Dec. 8-21 Fall semester final examinations
(specific exam date to be determined)