

CS 4476 Cryptography and Network Security

Winter, 2025

General information:

Instructor: Dr. Ruizhong Wei

E-mail: rwei@lakeheadu.ca

Time and location: MW 1:00 - 2:30 pm, OA 2008

Office hours: Wednesdays 3:00 - 4:00 pm, OR 1024.

Prerequisite: COMP 2412, 1008, 1011, Math 1271

Description:

This course covers fundamental concepts in cryptography and network security which includes basic knowledge, technology and theory of cryptography and network security. Topics of cryptography include conventional encryption, public-key cryptology, message authentications and digital signatures. Then some important topic of network security will be investigated including key distributions, remote access control, email security, IP security, web security, transaction security. Useful network security protocols and algorithms will be introduced and common security attacks will be analyzed.

Materials:

Based on lecture notes which can be downloaded from course webpage. However, the lecture notes and related materials will be updated from time to time. Therefore, the materials are determined by the lecture classes.

Some extra materials will be from Internet or other resources and distributed later.

Reference books:

- W. Stallings, Network and internetwork security, Prentice Hall.
- D.R. Stinson, Cryptography: Theory and practice, CRC Press.

Note: The reference books are for students who want further study the topics of this course. This course has no required textbook costs.

Assignments:

There will be 4 - 5 assignments in this term. Late assignments will be penalized and will not be accepted after 3 days.

Quizzes: There will be 4 - 5 short quizzes during lectures. The purpose of a quiz is for understanding lecture materials.

Examinations:

The regulation of examinations and related matters is described on university Calendar.

Course grade:

To determine the final grade of the course, the following weights will be applied:

- Assignments: 35%
- Quizzes: 30%
- Final exam: 35%

Course web page:

Some course information, supplemental materials and lecture notes will be put on D2L or the following page:

<http://ccc.cs.lakeheadu.ca/cs4476.html> (The web only can be accessed on campus or through the university's VPN)

Students are recommended to reference the web from time to time.

Note (University's *Academic Dishonesty Regulations* provide more details):

The University takes a most serious view of offences against academic honesty such as plagiarism, cheating and impersonation. Penalties for dealing with such offences will be strictly enforced.

The following rules shall govern the treatment of candidates who have been found guilty of attempting to obtain academic credit dishonestly.

- The minimum penalty for a candidate found guilty of plagiarism, or of cheating on any part of a course will be a zero for the work concerned.

- A candidate found guilty of cheating on a formal examination or a test, or of serious or repeated plagiarism, or of unofficially obtaining a copy of an examination paper before the examination is scheduled to be written, will receive zero for the course and may be expelled from the University.