

CS 4476/5413 Cryptography and Network Security

Winter, 2015

General information:

Instructor: Dr. Ruizhong Wei (AT 5021, Ex. 8227)

E-mail: rwei@lakeheadu.ca

Time and location: MW 10:00-11:30 am, AT 2006

Office hours: Wednesdays 1:30-2:30 pm, AT 5021

Prerequisite: CS 2412, CS 2477

Description:

This year the course will cover basic knowledge, technology and theory of cryptography and network security. Topics include conventional encryption, public-key cryptology, authentication and digital signatures, key distribution, email security, IP security, web security, etc. Several useful network security protocols and algorithms will also be investigated.

For CS 5413 students, the topics are the same, but more depth materials will be covered. The graduate students will expect to finish more reading materials.

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.

Assignments:

There will be 5 - 6 assignments in this term. Late assignments will be penalized and will not be accepted after 3 days. The assignments for CS 4476 and CS 5413 will be different.

Quizzes: There will be 3 - 4 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: 30%
- Quizzes: 10%
- Mid-term test: 20%
- Final exam: 40%

Course web page:

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

<http://peace.lakeheadu.ca/cs4476.html>

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