CS 4476 Cryptography and Network Security

Fall, 2021

General information:

Instructor: Dr. Ruizhong Wei

E-mail: `rwei@lakeheadu.ca`

Time and location: MW 8:30 - 10:00 am

Office hours: Wednesdays 2:00-3:00 pm

Prerequisite: COMP 2412, 2477 (or COMP 1008, 1011, 2412)

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.

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 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: 25%

- Final exam: 40%

Course web page:

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

`http://ccc.cs.lakeheadu.ca/cs4476.html` (Currently the web server does not work. Main teaching materials will be post on D2L)

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