Cryptography and Network Security
Computer Science Department
Winter 2023

Instructor Information

Instructor: Osama Amjad
Office Location: RL 1012
E-mail: oamjad@lakeheadu.ca
Office Hours: Monday-Friday, by appointment

Teaching Assistant (TA) Information: TBD

Course Identification:

Course Number: CS 4476
Course Name: Cryptography and Network Security
Class Times: Tuesday, Thursday, 2:30-4:00 pm (Thunder Bay)
Class Times: Monday, Wednesday, 8:30-10:00 pm (Orillia)

Course Description:

This course introduces the fundamental principles of the network security domain. The course starts by introducing required cryptographic techniques for secure (confidential) communication of two parties over an insecure (public) channel and verification of the authenticity and integrity of a message. Then, introducing several topics related to network security architecture and design of selected protocols including access control, application layer security protocols, transport layer security, network layer security, wireless security, Data link layer security, firewall, and Intrusion Detection Systems (IDS). Topics include conventional encryption, public-key cryptology, authentication and digital signatures, key distribution, IP security, web security, and network management security.

Course Learning Objectives (Student Learner Outcomes, SLOs)

At the end of the course, students will be able to:

1. Identify the necessary concepts in network security and the required cryptographic techniques for secure data communication.
2. Practice authentication and integrity techniques required to provide related network security objectives.
3. Apply encryption and authentication approaches for maintaining and protecting the privacy of the information in the network under investigation.
4. Analyze common network vulnerabilities and attacks, security weaknesses, and defense mechanisms against network attacks.
5. Write an extensive analysis report on network security product or related concerns and issues.

Course Resources

Course Website:

- myCourseLink

Text Books:

- W. Stallings, **Cryptography and Network Security: Principles and Practices**, 7th edition, Prentice Hall, 2017.

References:

- W. Stallings, Network Security Essentials: Applications and Standers, 6th edition, Prentice Hall, 2017.
- C. Kaufman, R. Perlman, and M. Speciner, Network Security: Private Communication in a Public World, 2nd Edition. Prentice Hall, 2002.
- Paar, Christof, and Jan Pelzl. **Understanding cryptography**: a textbook for students and practitioners. Springer Science & Business Media, 2009.

Course Schedule/Outline

1. Introduction to Network Security
2. symmetric encryption: Data Encryption Standard & Advanced Encryption Standard
3. Public-Key Cryptography and Digital signature.
4. Message Authentication CODES
5. User Authentication: Identification, key-distribution centers &CA & PKI
6. Network Access Control and Cloud Security
7. Transport-Level Security: SSL, TLS, more on attacks and other protocols
8. Electronic Mail Security
9. Application Layer Security: Kerberos, Secure HTTP (HTTPS), SSH
10. IP SECURITY and VPN
11. Firewalls and Intrusion Detection Systems (IDS)
12. Malicious Software
13. Wireless Security and Data Link Layer security

Assignments and Evaluations

Item	Weight (%)
Quizzes, Assignment	20%
Research Project	10%
Mid Term Exam	20%
Final Exam	50%

Course Policy

- Attendance in lectures is required to ensure your success for this course. The instructor is available for help but you need to ask questions in class. Polite Emails to instructors are fine and the instructor will try his best to answer within 24 hours.
- Group work/collaboration during studying for the course is encouraged. The instructor is willing to be available at reasonable mutually convenient hours to facilitate such group study on a voluntary as needed basis.
- Test and Exam are individual with possibly individualized question paper and the following academic integrity statement must be followed by each student:

Assignments

Homework will be assigned regularly. It will be due at the beginning of class on the specified due date.

Academic Integrity Statement:

I understand and agree that:

(1) Unless otherwise allowed by the course instructor, I must complete the assignments in this course without the assistance of anyone else.
(2) Unless otherwise allowed by the course instructor, I must not access any sources or materials (in print, online, or in any other way) to complete any course exam.

I further understand and agree that, if I violate either of these two rules, or if I provide any false or misleading information about my completion of course assignments or exams, I may be prosecuted under the Lakehead University Student Code of Conduct – Academic Integrity, which requires students to act ethically and with integrity in academic matters and to demonstrate behaviors that support the University's academic values.

Copyright

Students should be aware that all instructional, reference, and administrative materials prepared for this course are protected in their entirety by copyright. Students are expected to comply with this copyright by only accessing and using the course materials for personal educational use related to the course, and that the materials cannot be shared in any way, without the written authorization of the course instructor. If this copyright is infringed in anyway, students may be prosecuted under the Lakehead University Student Code of Conduct – Academic Integrity, which requires students to act ethically and with integrity in academic matters and to demonstrate behaviors that support the University's academic values.

Regulations

It is the responsibility of each student registered at Lakehead University to be familiar with, and comply with all the terms, requirements, regulations, policies and conditions in the Lakehead University Academic Calendar. This includes, but is not limited to, Academic Program

Requirements, Academic Schedule of Dates, University and Faculty/School Policies and Regulations and the Fees and Refund Policies and Schedules (Lakehead University Regulations webpage, 2020-21).

Academic Integrity

A breach of Academic Integrity is a serious offence. The principle of Academic Integrity, particularly of doing one's own work, documenting properly (including use of quotation marks, appropriate paraphrasing and referencing/citation), collaborating appropriately, and avoiding misrepresentation, is a core principle in university study. Students should view the Student Code of Conduct - Academic Integrity for a full description of academic offences, procedures when Academic Integrity breaches are suspected and sanctions for breaches of Academic Integrity.