Course Code Course Title
COMP 4631 **Computer and Communication Security**

Course Description

This course has two parts. The first part is called cryptography, which deals with basic security tools for building up secure computer and communication systems. The second part is about real-world security systems such as PGP (Email security), IP Security (networking security), Secure Sockets Layer (Web security), Firewalls (distributed system security), access control and Unix security (operating systems security), Secure Shell and virtual private networks.
Prerequisite(s): COMP 2711 or COMP 2711H
Exclusion(s): COMP5631

List of Topics

1. Conventional and public-key cryptosystems
2. Hash algorithms, digital signature, authentication, identification
3. Access control, Unix security
4. Distributed system security, network security
5. Firewalls, Email security, WWW Security, Secure Shell, virtual private networks

Textbook
Cryptography and Network Security, Behrouz A. Forouzan (McGraw Hill, 2008).

Reference books
Computer Security, D. Gollmann (Wiley, 1996).

Grading Scheme

Four assignments	24% (6% each assigment)
Class attendance	6%
Midterm quiz	30%
Exam	40%
Total	100%

Course Intended Learning Outcomes

On completion of this course, you will be able to:
1. evaluate potential vulnerabilities and attacks on computer and communication systems,
2. learn the basic security tools,
3. select and apply basic tools to build security systems, and
4. get familiar with real-world security systems.

Assessment Rubric: N/A