CS*4520 (Winter 2020)
Introduction to Cryptography

School of Computer Science
University of Guelph, Guelph, Ontario, Canada.

Instructor:	**Dr. Charlie Obimbo**
Office:	Reynolds 3310 519 824-4120 x 52634
E-mail:	cobimbo@uoguelph.ca
Office Hours:	TUES 11:00 - 1 p.m.
GTA:	**Harsh Mandali**
Lectures:	MWF 3:30 - 4:20 p.m.

Text: Cryptography and Network Security: Principles and Practice. 2014. (6th Ed.) William Stallings. Pearson Education. (ISBN 0-13141098-9.)

Recommended Reference Material:

1. Konheim, A.G. (2007). Computer security and Cryptography. Wiley. ISBN: 978-0-471-94783-7.
2. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein (CLRS). Introduction to Algorithms. MIT Press, 2009, ISBN:?9780262033848.
3. JOC - Journal of Cryptology.

1 Course Rational

The ability to protect the confidentiality of information, to prevent unauthorized access to data or services and to prevent the unauthorized modification of data is fundamental elements of security. Similarly, the ability to know who you are talking to and where something has come from, and to be able to bind parties to previous commitments or actions, is essential for trust. In the electronic world, these services typically rely on the use of cryptographic techniques. However, it is imperative that these techniques are used in the correct fashion if they are to satisfy their objectives. In particular, it is crucial that cryptographic keys are managed in an appropriate way.

2 Prerequisites

Discrete Mathematics;
Algorithms

3 Course Learning Outcomes

Upon successful completion of this course, students will be able to:

1. Understand central aspects of symmetric and asymmetric cryptography.
2. Understand how cryptographic techniques are used to establish security in modern information and communication systems.
3. Appreciate the different key management requirements and methodologies

4 Calendar Description

This course is and introduction to the foundations of modern cryptography, with an eye toward practical applications. Topics covered include classical systems, information theory, mathematical background material, symmetrical crypto-systems, block ciphers, stream ciphers, DES, Advanced Encryption Algorithm (AES), hash functions and message authentication (MAC), RC4, and their cryptanalysis; asymmetric crypto-systems, RSA and El Gamal, digital signatures, elliptic curves, provable security, key-exchange and management, authentication & Digital signatures. Importance of learning Cryptography in Digital Forensics will also be discussed.

5 Teaching methodology

The course will be conducted through lectures and class discussions, illustrations using computers, and practical lab exercises.

6 Class Policy

- Mobile phones should be switched OFF during class session.

7 Course Evaluation

Assessment	Marks	
Class Participation	10 %	[In Class Questions]
Labs	20 %	Lab Assessments
Assignments	20 %	[A1 due Jan 24; A2 due Feb 5; A3 due Mar 2]
Quizzes	50 %	[Q1 is on Feb 7; Q2 is on Mar 23; 25 marks each]

To Pass the course, the student has to get at least 50% in the Course work (Participation, assignments and labs), at least 50% on the Tests Failure to do so will end in the student achieving a Maximum grade of 45% for the whole course.

Your final grade is the weighted sum of all assessments shown above unless you fail the final exam, in which case your final grade is calculated by

0.4(Labs+ Assignments) + Participation + Midterm

Courselink

Check for announcements frequently. Also, read your general e-mail.

Academic Misconduct

The University of Guelph takes a very serious view of Academic Misconduct. Included in this category are such activities as cheating on examinations, plagiarism, misrepresentation, and submitting the same material in two different courses without written permission. Students are expected to be familiar with the section on Academic Misconduct in the Undergraduate Calendar, and should be aware that expulsion from the University is a possible penalty. If an instructor suspects that academic misconduct has occurred, that instructor has the right to **examine students orally** on the content or any other facet of submitted work. Moreover, it is expected that unless a student is explicitly given a collaborative project, all submitted work will have been done independently.

When You Cannot Meet a Course Requirement

When you find yourself unable to meet an in-course requirement due to illness or compassionate reasons, please advise the course instructor (or other designated person) in writing, with name, address and e-mail contact. Where possible, this should be done in advance of the missed work or event, but otherwise, just as soon as possible after the due date, and certainly no longer than one week later.
Note: if appropriate documentation of your inability to meet that in-course requirement is necessary, the course instructor, or delegate, **will request it of you**. Such documentation will rarely be required for course components representing less than 10% of the course grade.

Turnitin:
In this course, your instructor will be using Turnitin, integrated with the CourseLink Dropbox tool, to detect possible plagiarism, unauthorized collaboration or copying as part of the ongoing efforts to maintain academic integrity at the University of Guelph.

All submitted assignments will be included as source documents in the Turnitin.com reference database solely for the purpose of detecting plagiarism of such papers. Use of the Turnitin.com service is subject to the Usage Policy posted on the Turnitin.com site.

A major benefit of using Turnitin is that students will be able to educate and empower themselves in preventing academic misconduct. In this course, you may screen your own assignments through Turnitin as many times as you wish before the due date. You will be able to see and print reports that show you exactly where you have properly and improperly referenced the outside sources and materials in your assignment.