CS*4520 (Winter 2023)
Introduction to Cryptography:

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

Disclaimer
Please note that the ongoing COVID-19 pandemic may necessitate a revision of the format of course offerings, changes in classroom protocols, and academic schedules. Any such changes will be announced via Courselink and/or class email.

This includes on-campus scheduling during the semester, mid-terms and final examination schedules. All University-wide decisions will be posted on the COVID-19 website:
[**https://news.uoguelph.ca/2019-novel-coronavirus-information/**] and circulated by email.

Instructor:	**Dr. Charlie Obimbo**
Office:	Reynolds 3310 519 824-4120 x 52634
E-mail:	cobimbo@uoguelph.ca
Office Hours:	**Tue 11:00 a.m. – 12:45 p.m.**
GTA:	
E-mail:	
GTA Hours:	___TBD___
Lectures:	**MWF 9:30 - 10:20 a.m.**
Room:	**Mondays CRSC, Rm 116 ; WF Virtual / Asynchronous**
Labs:	**Wed 11:30AM - 01:20PM & Mon 12:30PM - 02:20PM.**
Room:	THRN, Room 2418
Final Exam:	**Sat 08:30AM - 10:30AM (2023/04/15)**

Text: Cryptography and Network Security: Principles and Practice. 2017. (7th Ed.) William Stallings. Pearson Education. (ISBN 10:1-292-15858-1.)

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. The last lab-report is due on March 18th.

6 Class Policy

- Mobile phones should be switched OFF during class session.

7 Course Evaluation

Assessment	Marks	
Class Exercises	5 %	[In Class Questions] Jan 23 (1 mk), Feb 6 (2 mks), Mar 7 (2 mks)
Labs	12 %	[Lab assessments due qFeb 3, qMar 3, Mar 24 (4 mks each)]
Assignments	15 %	[A1q (see below) - Jan 27 (Class time - Online); A2 due Feb 11; A3 due Mar 8 5 marks each.]
Quizzes	30 %	[Q1 is on Feb 13 ; Q2 is on Mar 15; **(1 hour each)**]
Presentation	10 %	[Period of Mar 21 - 28; **(12 mins Pres 3 mins Qtns)** 7% pres 3% Eval]
Final Exam	28 %	[The Final Exam is on **Sat 08:30AM - 10:30AM (2023/04/15).**]

Please note that the first three Lab assessments, and Assignment 1 will be done through CourseLink Quizzes. In order to do this, you need to do the given labs and assignments in preparation to do the Quizzes - as the questions will be similar in the most part.

The first Lab assessment will be on Labs 1, 2 & 3, the second on Labs 4,5 & 6 and the third will be a report on Labs 7 & 8.

To Pass the course, the student has
1. to do 67% of the lab assessments/reports,
2. to do at least 2 out of 3 assignments,
3. get at least 50% in the Course work (Class Exercises, assignments and labs), &
4. get at at least 50% on the Tests + Final Exam.

Failure to do so will end in the student achieving a Maximum grade of 45% for the whole course.

In the event that the above criteria for PASS is not attained, the student marks will be calculated as:

30% of (Assigns + Labs + Pres) + 50% of (Midterms)+ Final

Important Dates

Dates	
Mon Jan 9th	Classes Commence
Feb 19th - 26th	Winter Break
March 10th	40th day of class
April 6th	Last day of class
April 7th	Good Friday

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

8 Topics Covered

1.	**Introduction to Information Security**
2.	**Cryptography: Mathematical Preliminaries:**
3.	Number theory, Algorithm issues, Symmetric Key Cryptography,
4.	Public Key Cryptography, Key Exchange, Authentication,
5.	Digital Signatures, Digests;
6.	Public Key Infrastructure (PKi);
7.	Presentations of various interesting Crypto topics

9 ILLNESS

This course will not require verification of illness (doctor's notes) for the Winter 2023 semester.

Presentations that are made in relation to course work - including lectures - cannot be recorded or copied without the permission of the presenter, whether the instructor, a student, or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

Do not redistribute recorded interactive discussions that involve your classmates. This includes advising times and question and answer sessions with the instructor.

Online activities such as advising times, question and answer sessions, and interactive lectures may be recorded by the instructor or TAs and posted to CourseLink. By taking this course you are agreeing that your participation in these activities can be used in this manner. If you do not wish to have your image or voice recorded as part of these activities then either do not take this course or do not ask verbal questions during these activities.
A reliable internet connection that is sufficient for online learning is necessary for this course. If you do not have a sufficiently fast and reliable internet connection then you may not be able to view or download lectures or other course material. It may also not be possible to attend online advising with teaching assistants or the instructor.

This course is offered in the eastern standard time zone (EST). While taking this course then you may be required to attend online activities such as advising times or labs between 9:00 and 4:30 EST.

Keep copies of assignments which you have submitted. You may be asked to resubmit assignments at a later time.

10 ACADEMIC INTEGRITY

The University of Guelph is committed to the highest standards of academic integrity and honesty. Students are expected to be familiar with these standards, and must abide by the applicable policies (see Section VIII of the Undergraduate Calendar on "Academic Misconduct").

Respondus Monitor and Lockdown will be used for the Tests and Final Exam in this course.

For educational purposes, instructors impose conditions on assignments that may limit students' permission to collaborate with others or to utilize external sources (including, but not limited to, software, data, images, text, etc.). The use of **Chegg and such like websites is not allowed**. Any permitted utilization must be done with proper references. **Instructors may use automated tools: such as TurnItIn to detect possible cases of plagiarism.** Work that shows significant unnatural similarity, or that appears to be copied from unacknowledged sources, will be investigated as potential academic misconduct.

"**Aiding and abetting**" is also a punishable offence, and students must be careful not to help others commit offences by giving out their files or allowing others to access their computer accounts. Consider yourself warned.

10.1 ACCEPTABLE USE POLICY

Please read the complete University of Guelph policy found on http://www.uoguelph.ca/web/aupg.shtml.

10.2 CHANGES IN DATES ON COURSE OUTLINES

See: Undergraduate Calendar: VIII. Undergraduate Degree Regulations and Procedures: Grading Procedures (Resolution 5)

10.3 E-MAIL POLICY

Students should include their name and course number in every email, e.g.

Joe Smith: CIS*4520,

since instructors are often involved in teaching more than one course per term. To comply with university privacy policy, all emails should be sent from your uoguelph account (not from hotmail.com, gmail.com, or any other non-UoG host). All students are responsible for reading their uoguelph email and therefore should maintain their accounts, i.e. disk quotas should be monitored so that email is not rejected due to lack of space.