UNIVERSITY of GUELPH

SCHOOL OF COMPUTER SCIENCE

SEMESTER:	Winter 2020
COURSE:	**CIS*4520 – INTRODUCTION TO CRYPTOGRAPHY**
PRE-REQUISITES :	CIS*3490: Computer Algorithms and Design
PROF:	**Dr. Charlie Obimbo**
LECTURES:	
CLASS VENUE:	*Online – Hybrid – Synchronous / Asynchronous*
GRAD. TAs:	
CREDIT UNIT:	0.5 CREDIT HOURS
OFFICE HOURS:	
CONTACTS:	

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 are fundamental elements of security. Similarly, the ability to know who one is talking to and where something has come from, and 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.

Description:

This course is an 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.

Prerequisites:

Discrete Mathematics;
Algorithms

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

Textbook:

1. William Stallings. Cryptography and Network Security: Principles and Practice, Sixth Edition. Pearson Education, 2014. ISBN 0-13141098-9.

Recommended Reference Material:

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

Teaching methodology:

The course will be conducted through lectures and class discussions, illustrations using computers, and practical lab exercises. Lab reports are due 1 week after the labs.

Tentative Course Evaluation:

Labs	20 %	[First 4 labs are 3 marks each, the rest 4 marks each.]
Assignments	20 %	
Midterms (2)	30 %	
Final Exam	30 %	