UNIVERSITY of GUELPH
SCHOOL OF COMPUTER SCIENCE

CIS*4520 Introduction to Cryptography, Winter 2024

Course Information

Instructor:	Dr. Wenjing Zhang
Email:	wzhang25@uoguelph.ca
Lecture Time:	Tues/Thurs 5:30 PM – 6:50 PM
Lecture Type:	In-Person
Lecture Location:	Guelph, Rozanski Hall 105
Office Hours:	Thursdays 10:30 AM – 11:30 AM
Office Hours Location:	Guelph, J.D. MacLachlan Room 211

Teaching Assistant:	Vaideeshwaran Saravanan
Email:	saravanv@uoguelph.ca
Office Hours:	Tuesdays 3:00 PM – 4:00 PM
Office Hours Location:	Guelph, Reynolds Building Room 0003

Course Pages

1. CourseLink – www.courselink.uoguelph.ca (Primary).
2. Tophat – Join Code: TBD; Password: TBD (In Class Questions).

Course 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, symmetric and asymmetric crypto-systems and their cryptanalysis, hash functions and message authentication, provable security, key-exchange and management, authentication, digital signatures, and network security. The course will cover the recent developments in cryptography and security and include a group project that will also provide hands-on interaction with implementation of cryptography and security. The students will have the chance to apply what they have learned in the course during the project.

Prerequisites (By Topics)

Probability Theory, Algorithms, Linear Algebra, Programming.

Textbooks

Required Textbook:

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

Additional References:

– Introduction to Modern Cryptography (2nd Edition), Jonathan Katz and Yehuda Lindell, Chapman & Hall/CRC, 2014.

- Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, CRC Press, 1996, Available Online.
- Cryptography: Theory and Practice, Douglas Stinson, 3rd Edition, Prentice Hall, 2005.
- The Joy of Cryptography, Mike Rosulek, Oregon State University, 2017, Available Online.

Course Objectives

Upon the completion of this course, students should have achieved the following objectives:

- Become familiar with the cryptographic techniques that provide information and network security.
- Be able to apply suitable cryptographic primitives to achieve specific security goals for communication systems and networks.
- Be able to evaluate the security of communication systems, networks and protocols based on a multitude of security metrics.

Expected Learning Outcomes

By the end of this course, students will be able to:

- Identify the basic notions of information security.
- Describe and apply cryptographic primitives for achieving confidentiality in both private key and public key settings.
- Describe and apply cryptographic mechanisms for achieving information integrity.
- Evaluate the security/computation/communication tradeoffs between public key and private key cryptography.
- Apply private key or public key cryptographic primitives for building mutual authentication protocols.
- Outline key agreement and key distribution protocols and analyze their overhead.
- Explain the application of cryptographic primitives and protocols in the context of network security.

Course Topics

Introduction to Information Security (∼1 week)

- Information security objectives
- Schematic of a secure communication system
- Formal definition of a cryptosystem, and adversary models

Classical Encryption Techniques (∼1.5 weeks)

- Number theory basics
- Early cryptosystems: substitution and transposition
- Cryptanalysis of early cryptosystems

Measures of Security and Ideal Cryptosystems (∼1 week)

- Measures of security

– Perfect secrecy
– Definition of entropy
– Ideal cryptosystems, and one-time pad

Symmetric Key Cryptography (∼2 weeks)

– The notion of symmetric key cryptography, and computational security
– Block cipher, product cipher, and substitution-permutation networks
– The Data Encryption Standard (DES)
– The Advanced Encryption Standard (AES)
– Modes of operation
– Pseudorandom numbers and stream ciphers

Public Key Cryptosystems (∼2 weeks)

– Principles of Public Key Cryptography (PKC)
– More number theory basics
– Common public key cryptosystems: RSA
– Diffie-Hellman key exchange and ElGamal

Message Integrity and Authentication (∼1.5 weeks)

– Definition of hash functions and security properties
– Examples of hash functions: MD series, and Secure Hash Algorithm (SHA)
– Message Authentication Codes (MAC), HMAC
– More hash applications, including commitment protocols
– Common digital signatures schemes: RSA, ElGamal, Schnorr, and DSA

Key Management and Distribution (∼1 week)

– Symmetric key distribution schemes, Key Distribution Centers (KDC), session keys
– Public key distribution and Certificate Authorities (CA)
– Public Key Infrastructure (PKI)

User Authentication (∼1 week)

– User authentication principles
– Password authentication protocols
– Challenge-response protocols and common pitfalls
– Kerberos

Network Security (∼1 week)

– TCP/IP Threats
– IP security: the IPSec protocol
– Transport-level security: SSL and TLS protocols
– Web security

Grading Policy

Grades will be assigned based on the performance on *class participations*, *homework assignments*, *projects*, and *final examination*. The weights assigned to each component are listed as below.

Component	**Percentage**
Class Participations	5%
Assignments	30%
Project Proposal	10%
Final Project (Report, Code, Demo Video)	30%
Final Examination	25%

Important Dates (Tentative)

Course Deliverable (Sorted by Due Date)	**Due Date (11:59pm EST)**
Project Proposal	Friday, January 26
Assignment 1	Friday, February 2
Assignment 2	Monday, February 26
Midterm Project Discussion	Tuesday, February 27
Assignment 3	Friday, March 29
Final Project - Pre-Recorded Presentation & Demo Video	Friday, April 5
Final Project - Report & Code	Friday, April 12
Final Examination	Thursday, April 18

Course Policies

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. Please note that the distribution of course materials is prohibited without the explicit permission of the instructor.

Assignment Policies

Assignments must be submitted by their respective due dates. Any late submissions will incur a penalty of 10% of the total grade for each day they are delayed. Please note that submissions will not be accepted if they are more than 2 days late, except in cases where prior arrangements have been made with the instructor. Additionally, once the solutions are posted, no further assignments will be accepted under any circumstances.

For any concerns regarding assignment grades, I recommend initially discussing them with the TA. Should your issue remain unresolved, feel free to visit me during office hours or contact me via email. Please note that this should be done within one week of the original assignment grade being posted. Additionally, keep in mind that a single point on an assignment typically represents a minor fraction of your overall grade. Therefore, I kindly ask that you consider the significance of your query to avoid overburdening the TA with minor concerns.

Course Project

You are required to complete an implementation project for this course. You have the option to collaborate in teams of up to two members, which allows for a broader project scope. Alternatively, you may choose to work independently. Regardless of your choice, a final report is mandatory for all projects. To ensure you are on track, you must submit a project proposal and engage in a midterm project discussion. The final phase of your project will require you to submit a final report and code, as well as present your findings in a 10-15 minute pre-recorded video.

Please be aware of the importance of adhering to deadlines. Late submissions will result in a deduction of 10% of the total grade per day delayed. Submissions received more than 2 days late will not be considered unless prior arrangements have been made with the instructor.

Final Examination

There will be one final examination. The examination is open book/notes.

Accessibility

The University of Guelph prioritizes establishing an environment free from barriers. Supporting students is a collective responsibility shared by students, faculty, and administrators. This cooperative effort is grounded in mutual respect for individual rights, the dignity of every individual, and a commitment from the University community to foster an open and supportive learning environment. Students in need of services or accommodations, whether due to a long-term identified disability or a short-term disability, are encouraged to reach out to Student Accessibility Services (SAS) at the earliest opportunity. For additional information, please contact Student Accessibility Services (SAS) at 1.519.824.4120 ext 56208, email accessibility@uoguelph.ca, or visit Wellness.uoguelph.ca/accessibility.

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 The Academic Misconduct Policy in the Undergraduate Calendar).

The Academic Misconduct Policy is detailed in the Undergraduate Calendar:
http://www.uoguelph.ca/registrar/calendars/undergraduate/current/c08/c08-amisconduct.shtml

Health & Wellness

Should you encounter any personal challenges, please feel free to reach out to the instructor. Remember, the University of Guelph offers various resources to support you.

For medical concerns, contact Student Health Services at 1.519.824.4120 ext 52131.

For threats of violence or personal safety issues, contact Campus Police at 1.519.824.4120 ext 2000.

For psychological or emotional concerns, get in touch with Counselling Services at 1.519.824.4120 ext 53244.

For accessibility concerns, reach out to SAS at 1.519.824.4120 ext 56208.

In case of sexual assault, contact Campus Police at ext 2000, or Counselling Services at 1.519.824.4120 ext 53244.

For mental health concerns, visit https://wellness.uoguelph.ca/mental-health-support-services.