`CIS*6570
Advanced Cryptography and Cryptanalysis
Winter Semester

UNIVERSITY of GUELPH

---

1 INSTRUCTOR

Instructor: Dr. Charlie Obimbo

Office: Reynolds 3310

Phone extension: 52634

E-mail: cobimbo@uoguelph.ca

2 AIMS & OBJECTIVES

The abilities 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 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. This course will:

- Introduce the main types of cryptographic techniques;
- Explain how different cryptographic techniques provide different security services; and
- Identify some key issues relating to the management of these services.

2.1 Calendar Description

This course provides an in-depth understanding of modern cryptography, with emphasis on practical applications. Topics covered include classical systems, information theory, symmetrical cryptosystems, block ciphers, stream ciphers, DES, AES, asymmetric cryptosystems, ECC, provable security, key-exchange and management, and authentication and digital signatures, among others.

2.2 Course Description

This course provides an in-depth understanding of modern cryptography, with emphasis on practical applications. Topics covered include classical systems, information theory, symmetrical cryptosystems,

block ciphers, stream ciphers, DES, AES, hash functions and message authentication and their cryptanalysis; asymmetric cryptosystems, RSA and El-Gamal, ECC, provable security, key-exchange and management, and authentication and digital signatures.

2.3 Learning Outcomes

Upon successful completion of this course, students will have demonstrated the ability to:

1. Apply the concepts of number theory (modular arithmetic and congruencies) necessary for cryptography and cryptanalysis as well as distinguish between symmetric and asymmetric cryptography;
2. Encrypt and decrypt messages using block ciphers;
3. Sign and verify messages using well known signature generation and verification algorithms;
4. Describe the use of end-to-end encryption and how cryptographic techniques are used to establish security in modern information communication systems;
5. Analyze existing authentication and key agreement protocols, identify the weaknesses of these protocols, and describe the different key management requirements and methodologies;
6. Integrate ethics, regulations, and best practices in cybersecurity; and
7. Apply steganography and watermarking in digital rights management.

2.4 Instructor's Role and Responsibility to Students

The role of the instructor is to give lectures and organize and moderate class discussions, give illustrations using computers, and practical create lab exercises for students to practice on.

3 TEACHING AND LEARNING ACTIVITIES

3.1 Timetable

Lectures: 3 hours per week

3.2 Course Topics and Schedule

Week	Topic
Week 1	Introduction to Cryptography, & Mathematical Background
Weeks 2-4	Classical Private Key Encryption: - Caesar-Shift, Monoalphabetic ciphers, - Transposition ciphers, - Columnar; and Hill-ciphers
Weeks 5-6	- Vigenere - One-time pads - Weakness in cryptosystems & attacks (statistical attacks) **- Midterm**
Weeks 7-8	Number Theoretic Algorithms: - Public Key Encryption

	- RSA
Weeks 9-10	DES, AES Steganography Encrypting medical images Public-key Infrastructure
Weeks 11-12	RC5 Elliptic-Curve Cryptography

4 LEARNING RESOURCES

4.1 Course Website

Course material, news, announcements, and grades will be regularly posted to the CIS*6550 CourseLink site. Students are responsible for checking the site regularly.

4.2 Required Resources

Textbook:

1. William Stallings. Cryptography and Network Security: Principles and Practice, Sixth Edition. Pearson Education, 2014. 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.

5 ASSESSMENT

5.1 Dates and Distribution

Assignment	Due Date	Weighting	Learning Outcome(s) Assessed
Labs	TBD	20%	L02, L03, L05, L07
Assignments	TBD	20%	L01, L02, L04, L06
Midterms	TBD	30%	L01, L02, L04, L06, L07
Project	TBD	30%	L03, L04, L06, L07

There will be four lab tasks and three assignments done individually. Two midterms also done individually, and the Final project will be done in groups of 2.

5.2 Assessment Descriptions

Labs: The labs will be half of the form of authentic assessment, where employment-like conditions will be created, with tools like CrypTool, to help students learn to encrypt, decrypt, and cryptanalyze given texts.

Assignments: The assignments will have the form of diagnostic assessment and synoptic assessments. There will be in-class formative assessments in terms of small exercises on concepts learnt. These will be marked but not account for grades awarded for the course.

Midterm: The midterm will have the form of diagnostic assessment and synoptic assessments.

Project:

5.3 Course Grading Policies

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the course instructor within two weeks of the start of the semester to make alternate arrangements. See the graduate calendar for information on regulations and procedures for Academic Accommodation of Religious Obligations: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2228.shtml

Passing grade: In order to pass the course, students must obtain a grade of 65% or higher on the total mark of all assessments.

---

6 University Statements

6.1 Email Communication

As per university regulations, all students are required to check their e-mail account regularly; e-mail is the official route of communication between the University and its students.

6.2 When You Cannot Meet a Course Requirement

When you find yourself unable to meet an in-course requirement because of illness or compassionate reasons please advise the course instructor (or designated person, such as a teaching assistant) in writing, with your name, id#, and e-mail contact. The grounds for Academic Consideration are detailed in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/index.shtml

6.3 Drop Date

Courses that are one semester long must be dropped by the end of the fortieth class day; two-semester courses must be dropped by the last day of the add period in the second semester. The regulations and procedures for changing graduate course registration are available in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-reg-regchg.shtml

6.4 Copies of Out-of-class Assignments

Keep paper and/or other reliable back-up copies of all out-of-class assignments; you may be asked to resubmit work at any time.

6.5 Accessibility

The University promotes the full participation of students who experience disabilities in their academic programs. To that end, the provision of academic accommodation is a shared responsibility between the University and the student.

When accommodations are needed, the student is required to first register with Student Accessibility Services (SAS). Documentation to substantiate the existence of a disability is required; however, interim accommodations may be possible while that process is underway.

Accommodations are available for both permanent and temporary disabilities. It should be noted that common illnesses such as a cold or the flu do not constitute a disability.

Use of the SAS Exam Centre requires students to book their exams at least seven days in advance and not later than the fortieth class day.

More information can be found on the SAS website: https://www.uoguelph.ca/sas

6.6 Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity, and it is the responsibility of all members of the University community—faculty, staff, and students—to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's policy on academic misconduct regardless of their location of study; faculty, staff, and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

Please note: Whether or not a student intended to commit academic misconduct is not relevant for a finding of guilt. Hurried or careless submission of assignments does not excuse students from responsibility for verifying the academic integrity of their work before submitting it. Students who are in any doubt as to whether an action on their part could be construed as an academic offence should consult with a faculty member or faculty advisor.

The Academic Misconduct Policy is detailed in the Graduate Calendar:
https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2642.shtml

6.7 Recording of Materials

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.

6.8 Resources

The Academic Calendars are the source of information about the University of Guelph's procedures, policies, and regulations that apply to undergraduate, graduate, and diploma programs: https://www.uoguelph.ca/academics/calendars