CIS 475 – Introduction to Cryptography
Spring 2023

Recommended Textbooks: All materials for this class will be provided in class. Here are some free textbooks for reference.

A Course in Cryptography by Rafael Pass and Abhi Shelat
The Joy of Cryptography by Mike Rosulek.
Cryptoraphy, an Introduction by Nigel Smart.
A Graduate Course in Applied Cryptography by Dan Boneh and Victor Shoup.
An Intensive Introduction to Cryptography by Boaz Barak.

Instructor: Supraja Gurajala,
Phone: 315-267-2091
Email : gurajas@potsdam.edu

Office Hours: MW - 10:00am - 12:00 noon
Tu Th - 11:00am to 12:00 noon

Discord Link: https://discord.gg/GVd3V5KTEm
Class Time/Place: Tu, Th – 9:30am to 10:45am, Dunn Hall 208
Final Exam: Tuesday, May 16, 10:15 a.m. – 12:15 p.m.

Learning Objectives:

This course focuses on cryptographic algorithms and their mathematical background. We will learn basic concepts of cryptography and their applications. This course covers stream ciphers, block ciphers, Data encryption standard (DES), Advance encryption standard (AES) and public-key cryptography. Since most of these topics require background in number theory and probability theory, many lectures will focus on developing the necessary background in these areas.

Students who have taken this course should be able to:

- Understand cryptography and data security.
- Define block and stream ciphers.
- Define Symmetric and Asymmetric cryptographic algorithms
- Understand how Data encryption standard (DES), Advance encryption standard (AES) work and also will be able to implement them using modern programming language.
- Gain knowledge of important concepts in public-key cryptographic systems and be able to program many public-key cryptographic algorithms from scratch.
- Understand basic concepts in number theory that are relevant to cryptography.
- Use modern programming language to implement cryptographic algorithms.

Tentative schedule:

Week 1	The general rules of cryptography Key lengths for short-, medium- and long-term security
Week 2	Attacks against ciphers historical ciphers modular arithmetic,
Week 3	stream ciphers Random and pseudorandom number generators
Week 4	The One-Time Pad (OTP) Linear feedback shift registers and Trivium, a modern stream cipher
Week 5	Symmetric and Asymmetric cryptographic algorithms
Week 6	Modular Arithmetic
Week 7	Number theory introduction
Week 8	Public key Cryptography
Week 9	Factoring Problem RSA Chinese Reminder Theorem
Week 10	Discrete logarithm problem Diffie Hellman Key exchange
Week 11	Elliptical curves Finding points on Elliptical curves
Week 12	Quadratic Residuosity problem Legendre Symbol Jacobi Symbol
Week 13	Blum integer Blum-Blum-Shub-Pseudorandom bit generator Blum Goldwasser probabilistic encryption
Week 14	Symmectric Ciphers DES
Week 15	AES
Week 16	Review and Final exam

Grading for the Course:

1. ***Weekly Quizzes:*** 10 %

   A ten-minute weekly quiz will be given once a week. It can be on any class day. It will be based on lectures and Homework problems assigned to you. There is no make-up quiz.

2. ***Homeworks:*** 10 %

   Several homeworks will be given based on the concepts discussed in lectures. These homeworks will be the essential part of the course. HWs will be posted on brightspace along with the due date. Late work is penalized at 20% per calendar day that they are late.

No late work is accepted beyond the cutoff date. Your final submitted HW should represent your individual work; it is, however, acceptable to discuss the solution approach with other students. You will be responsible for keeping track of due dates posted on brightspace.

3. ***Exams:*** 45%

   a. Midterm 1 – 14 % Date: TBA
   b. Midterm 2 – 14 % Date: TBA
   c. Final Exam – 17 % Date: Tuesday, May 16, 10:15 a.m. – 12:15 p.m.

   Exams will be closed book and closed notes unless specified otherwise. Any request for re-grading must be received in writing and within 3 days of receiving your graded exam back. Prior notice must be given to your instructor. No make-ups will be granted unless satisfactory documentation is produced to show an extenuating circumstance.

4. ***programming Assignments:*** 30%

   There will be four or five programming assignments in this course. Assignments will be posted on brightspace. Late work is penalized at 20% per calendar day that they are late. No late work is accepted beyond the cutoff date. Your final submitted assignment should represent your individual work; it is, however, acceptable to discuss the solution approach with other students. You will be responsible for keeping track of due dates posted on brightspace.

5. ***Research Papers: 5%***

   Students as groups will present latest research papers in Cryptography filed to understand the practical aspects of these algorithms in real world applications.

Course Policies

1. ***Late work***

   All due dates for the course will be strictly enforced. Prior approval will be required from the instructor for any late submission, including making up missed exams.

2. ***Attendance***

   Attending all lectures and labs and completing required work is crucial to your success in this course. While attendance is not graded per se, in-class graded work cannot be made up without prior arrangement with the instructor. In the event of absences from weekly labs, you are required to complete the missed lab work before the beginning of the next lab session. The instructor and CS tutors will be available to help you with completing labs during posted office and tutoring hours.

3. ***Absences***

   As noted above, in-class graded work cannot be made up without prior arrangement with the instructor.

Accommodation of Religious Observances: I will make reasonable accommodation for a student's religious beliefs. Please notify me within the first week of classes about any scheduled class date that conflicts with a religious observance.

4. ***Academic Integrity***

You are expected follow the "SUNY Potsdam Academic Honor Code" (SUNY Potsdam Undergraduate Catalog, https://catalog.potsdam.edu/content.php?catoid=7&navoid=566) by doing your own work on all required work for the course unless specifically directed otherwise by the professor. Copying is strictly forbidden, regardless of the source (online, other students). Students caught cheating will receive a grade of 0 for that evaluation. More than one offense will result in dismissal from the course and possible disciplinary sanctions by the university. Academic Misconduct definitions, procedures, due process, and student rights are described on page in the SUNY Potsdam Undergraduate Catalog, as cited above.

5. ***Grade Distribution***

At the end of the semester, I will calculate what fraction of the possible points you have earned, and your grade will be based on this distribution:

4.0: 95 – 100%
3.7: 90 – 94%
3.3: 85 – 89%
3.0: 80 – 84%
2.7: 77 – 79%
2.3: 73 – 76%
2.0: 70 – 72%
1.7: 67 – 69%
1.3: 63 – 66%
1.0: 60 – 62%
0.0: <60%

Note that final grades may be determined using a class curve of the course-grade averages.