CIS 475 – Introduction to Cryptography
Spring 2021

Recommended Textbooks:
Cryptography Made Simple (Information Security and Cryptography) 1st ed. 2016 Edition by Nigel Smart
Understanding Cryptography: A Textbook for Students and Practitioners 2010th Edition by Christof Paar , Jan Pelzl
A Graduate Course in Applied Cryptography (online free) by D. Boneh and V. Shoup

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

Office Hours:
Tuesday - 2:00pm - 3:00pm
Wednesday - 10:00am to 12:00 noon
Thursday - 9:00am to 11:30am
Friday - 10:00am to 12:00 noon

Discord Text Channel : dr_gurajala_office
Discord Voice Channel : Dr. Gurajala_office

Discord Link: https://discord.gg/GVd3V5KTEm
Class Time/Place: T,TH – 11:30am to 12:45pm, Zoom link provided on moodle course page
Final Exam: Wednesday, May 19, 8:00- 10:00 am

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.

Lectures:

This is a virtual course taught synchronously. This class meets three times a week MWF at 9:10am on Zoom (link provided on moodle course page). As professionals, we are expected to:

- show up on time;
- be prepared for our collective work;
- be appropriately attired; and
- try to limit distractions in our individual workplaces.

As members of a community, please consider the effects of your actions on your colleagues, just as you would in a physical classroom:

- keep your video on (when possible and as appropriate to the course session); if a video isn't feasible, you are encouraged to attach a picture to your profile in Zoom so that your classmates can get to know you (https://support.zoom.us/hc/en-us/articles/201363203-Customizing-your-profile);
- mute yourself when not speaking; and
- focus your attention on the speaker.

Please let me know if you are having difficulties interacting in class via Zoom, and if there are reasons you cannot follow the above guidelines.

Caring Community:

I recognize that this is an incredibly stressful time for you, your peers, and our community. Please know that there are resources available to you, both on and off campus, to support you during these very uncertain times. Our excellent Counseling Center staff are available to meet with you; more information can be found on their FAQ page accessed at: https://www.potsdam.edu/studentlife/wellness/counseling-center/coping-covid-19-pandemic/counseling-center-faqs. In addition, information on a variety of on- and off-campus resources can be found our Bear Care site: https://www.potsdam.edu/studentlife/wellness/bear-care. You are an incredibly important member of our Potsdam community; please take care of yourself, and each other.

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	Final exams

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:*** 15 %

   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 moodle page 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 moodle.

3. ***Exams:*** 40%

   a. Midterm 1 – 15 % Date: TBA
   b. Midterm 2 – 15 % Date: TBA
   c. Final Exam – 15 % Date: Wednesday, May 19, 8:00- 10:00 am

   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.

   Final grades are determined using a class curve of the course-grade averages.

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

90% >=	A
80% - 90	B
70% - 80	C
60% - 70	D
< 60%	F

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

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

   There will be four or five programming assignments in this course. Assignments will be posted on moodle. 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 moodle.

Final grades are determined using a class curve of the course-grade averages.

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.

Due Dates

All due dates for the course will be strictly enforced. Prior approval will be required from the instructor for any late submission.

Hardware*:* The course is being taught virtually, with all participants working remotely. That means that you will need to have the following computer hardware:

- Laptop or desktop computer – This is a programming-intensive course. You will need a computer to be able to do the programming. If you have only a tablet or a smartphone, please contact me so we can talk about alternatives for you to do the work.
- Camera and microphone – You need these to support video/audio for synchronous class meetings and for using the CS Department Discord server (more information below). Your laptop or desktop system may have built-in camera and microphone, or you could use eternal camera and microphone. You can also use a tablet or smartphone for video/audio communication.

Software*:* Here is a summary of the various software you will need for the course, in addition to the basics of a computer, browser, and typical software.

- **VPN (virtual private network) software** – You may want to connect to the university's VPN so that you can connect remotely to the CS lab in Dunn 302. If you are using Windows or Mac OS, you can find instructions for the software download and setup here: https://www.potsdam.edu/about/administrative-offices/computing-technology-services/services/vpn. If you use Linux, Dr. Ladd has made a video to help you set up to use the VPN. The video is available near the top of the Moodle course page.
- **Command line interface (cli) tool** – If you access the CS lab remotely, you will need a command line tool to work on the lab machines. You will not have access to any graphical user interfaces when working remotely. Windows, Mac, and Linux operating systems have a version of the command line interface available to users.
- **VSCode** – We recommend that you install this free programming environment. It is free (as just noted), available for any OS, easy to use, and allows for users to share code. You can download VSCode from https://code.visualstudio.com/download.
- **Java 11** – This is the version of Java that is installed in the lab, and VSCode will want you to use this version as well.
- **Discord** – The CS Department has Discord server (more information below) that is our "virtual department". My office hours will take place in Discord, our CS tutors will work on Discord, and our ACM chapter has its meetings on their Discord server. You can join our server at https://discord.gg/GVd3V5KTEm and find information about getting started with Discord at https://discord.com/new
- **Zoom** – Our synchronous (real-time) class meetings will take place through Zoom. You can get a free Zoom account here https://zoom.us/.

Impact of extracurricular activities on class work

You make the choices about how you will spend your time, including investing your time in non-academic activities. As a student, you need to give priority to your academic work, and prevent extracurricular commitments from negatively impacting your work for classes. You are, of course, free to participate in activities that are meaningful to you; however, do not expect me to give special consideration because of time management issues that arise from those activities. You should not be missing class because of extracurricular activities, nor should you allow yourself to fall behind on assignments. **NOTE: I will not give extensions that relate to participation in extracurricular activities, even if the activity is related to Computer Science.**

Expectations for the Course

- You will be expected to come prepared to class and be an active participant in class discussions. You should plan on spending a significant time outside class in reviewing course material covered in class. It is critical that you keep up with the course material on a timely basis.
- Academic dishonesty: Students are expected follow the "SUNY Potsdam Academic Honor Code" (SUNY Potsdam 2014-2016 Undergraduate Catalog, p. 42) by doing their own work on quizzes, exams and programming assignments unless specifically directed otherwise by the instructor. Copying is strictly forbidden. Students caught cheating will receive a grade of 0 for that evaluation. Repeated offenses 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 43 of the SUNY Potsdam 2014-2016 Undergraduate Catalog.
- Disability Assistance: Anyone who has special needs that must be accommodated to fulfill the course requirements should notify the instructor and the Director of Accommodative Services, 111 Sisson Hall, 267-3267. The college has resources available to assist qualified students with their academic studies.
- Food and Drink in Class and Lab**:** Beverages are allowed in the classroom as long you clean up after yourself and do not disturb others. In the Unix lab, food and drink are restricted to the coffee table. UNDER -NO- CIRCUMSTANCES ARE FOOD AND BEVERAGES (EVEN GUM) ALLOWED NEAR THE COMPUTERS.
- No devices are allowed during class. Notes must be hand-written
- Accommodation of Religious Observances: We will make reasonable accommodation for a student's religious beliefs. Please notify us within the first week of classes about any scheduled class date that conflicts with a religious observance.

Attendance

Regular attendance is critical for your success in this course. You are responsible for updating yourself with announcements made in class concerning material covered, home works, and any changes in course syllabus, due dates, or other course-related issues.

SUNY Potsdam Department of Computer Science Code of Professional Conduct

1. ***Preamble***
   All members of the ACM, including the Computer Science faculty of SUNY Potsdam, are committed to ethical professional conduct as specified in the ACM Code of Ethics and Professional Conduct. Students, taking courses from the faculty, are bound by our commitment.

   All members of the Department are obliged to remind one another to behave professionally. Violations should be reported promptly; however, capricious or malicious reporting of violations is, itself, a violation. When reporting, bring all relevant aspects of the incident to the faculty's attention.

2. ***Moral Imperatives***
   As a Computer Science student I will...

   2.1. Respect all members of the Department.

      2.1.1. Be professional in face-to-face and electronic interactions.

      2.1.2. Be fair so everyone is free to work and learn.

      2.1.3. Be active in preventing discrimination in physical and electronic spaces frequented by Department members.

   2.2. Accept and provide appropriate feedback.

      2.2.1. Avoid starting or spreading rumors.

      2.2.2. Respect confidentiality.

   2.3. Be honest, trustworthy, and respect intellectual property.

      2.3.1. Only take credit for my own work.

      2.3.2. Respect the privacy of others.

      2.3.3. Access computing resources only when authorized and report any access risks discovered.

   2.4. Contribute to society and human well-being.

      2.4.1. Improve public understanding of computing and its consequences.

      2.4.2. Consider both the direct and indirect impacts of my actions.

Based on the ACM Code of Ethics and Professional Conduct, retrieved from https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct 11 August 2017

Student Support

Every student in this class is a valued individual. If you are struggling with issues outside of the classroom, please know that there are professionals both on and off campus who can assist you.

If you need immediate assistance, please contact our campus Counseling Center (with free counseling) at (315) 267-2330 or visit their website. Links to other resources are provided below:

Rachel Bayliss- Title IX Support Staff & Title IX Core Team
Draime Extension S184, (315) 267-2350
VanHousen Extension, Rm. 392, (315) 267-2516
http://www.potsdam.edu/offices/hr/titleix

Bias Incident Reporting-
http://www.potsdam.edu/about/diversity/biasincident

Center for Diversity
223 Sisson Hall
(315) 267-2184
http://www.potsdam.edu/studentlife/diversity

University Police
Van Housen Extension
(315) 267-2222 (number for non-emergencies; for an emergency please dial 911)

Student Conduct and Community Standards
208 Barrington Student Union
http://www.potsdam.edu/studentlife/studentconduct/codeofconduct

Reachout (24-hour crisis hotline) ▪□(315) 265-2422

Renewal House (for victims of domestic violence)
SUNY Potsdam Campus Office: Van Housen Extension 390 (open Wednesdays, 9-5:00)
(315) 379-9845 (24-hour crisis hotline)
Renewalhouse_campus@Verizon.net

And please: if you see something, say something. If you see that someone that you care about is struggling, please encourage them to seek help. If they are unwilling to do so, Care Enough to Call has guidelines on whom to contact. Everyone has the responsibility of creating a college climate of compassion.