CS 50010 : Foundational Principles of Information Security

Summer 2023

Instructor: Mohammad Hassan Ameri
Email: mameriek@purdue.edu

Professor in Charge: Dr. Jeffrey A. Turkstra
Email: jeff@purdue.edu

Module 1 Lecturer and Content Expert: Dr. Ananth Grama
Module 2 Lecturer and Content Expert: Dr. Jeremiah Blocki

Module 1: Data structures and Algorithms

This course module considers foundational topics in data structures and algorithms. CS 50010 Module 1 covers these topics:

- Basic logic
- Proofs
- Recursion and recursive algorithms
- Sets & functions
- Sequences and summations
- Matrices
- Algorithm analysis
- Growth of Functions
- Stacks and Queues
- Graphs and Trees
- Searching and Priority Queues
- Tries
- Sorting algorithms
- Algorithm strategies
- The Halting problem

Prerequisites

The student should have some basic knowledge of computer science, calculus and linear algebra, as taught in CS 25100 and MA 35100.

Module Goals

The course goals are to learn common analysis techniques, including how to reason about logical statements, how to analyze algorithms, and how to use several common data structures.

Module Objectives

Student should learn to:

- Understand how to properly design and analyze an algorithm
- How to use and apply the data structures and algorithms we cover in this module

Module 2: Foundational Principles of Information Security

This course module considers foundational topics in cryptography and information security. CS 50010 Module 2 covers these topics:

- Elements of probability
- Bayes' Theorem
- Random variables
- Birthday problem and hash functions
- Elements of number theory used in cryptography
- Arithmetic with very large integers
- Euclidean algorithm for GCD
- Prime numbers
- Congruences
- Public and private key ciphers

Prerequisites

The student should have some basic knowledge of computer science, calculus and linear algebra, as taught in CS 25100 and MA 35100.

Module Goals

The course goals are to learn basic topics in cryptography.

Module Objectives

Student should learn to:

- Apply basic principles of probability and statistics to problems in information security.
- Apply fundamental principles of discrete mathematics and number theory to problems in cryptography.

Course Requirements

The lectures for this course have been recorded and are available on Brightspace. You are responsible for watching the lectures each week and for making sure that you understand the covered.

There will be two final exams - one for each module. There will be eight homework assignments - four for each module. One per week. The grading weights for each module will be 48 points for homework, 45 points for the final exam and 7 points course participation. Course Participation will primarily be based on your participation on the Ed Discussion discussion board i.e., asking good questions, providing good answers to student questions (see table 1).

Please format your written homework using a word processor (or else print it very neatly). If we can't read it, then we can't give you credit for it.

Office Hours

The instructor and TA office hours will be posted to Ed Discussion. During some weeks it may be necessary for the instructor or TA to move office hours due to unexpected travel. In such cases updates will be posted to Ed Discussion.

Course Policy

We will be using Ed Discussion for the course discussion board. You can find it at https://edstem.org/us/join/gK7Wut.

Ed Discussion is the preferred method of communication for the course. We will make every effort to answer your questions as quickly as possible. When you have a general questions about a lecture or homework set we would ask that you post these questions publicly.

Homework

We will have weekly homework sets (four total for each module). Each homework set will be worth 12 points. The assignments will be posted on Brightspace. You are responsible to complete the entire homework assignment by the posted deadline. Your solutions should be typed in any text editor you prefer (LaTeX, Word, etc) and you should turn in an electronic copy of the assignment on Gradescope by the posted deadline. Write your solutions as succinctly as possible while including all the necessary details. Please ask your questions on Ed Discussion and answer your colleague's questions to receive participation points. Some assignments might have an optional problem. The optional problem does not count towards your score, unless your grade will be a borderline case.

Collaboration Policy

You may ask questions about the homework on Ed Discussion to seek clarification from your classmates or from the professor. However you must write down the solutions yourself, and you must completely understand any solutions you submit. No other sources are allowed and violations will be penalized according to Purdue's integrity policies. Do not copy another students homework and do not allow another student copy your homework. Discussions with other students should be appropriately acknowledged. Turning in a solution that you could not explain to the instructor is considered cheating.

Final Exam

The final exam for each module will be worth 45 percent of your final module grade. The exam will be closed book. However, for each exam you will be allowed to prepare a 3x5 index card with your own notes (3x5 inches, double sided). You may not use calculators, cell phones, smart watches, computers, cameras, radios, televisions, books, Morse code, signals or sign language during exams. Communication with anyone besides the instructor (or TA) during an exam is considered cheating.

Grading

It often happens that students receive higher numerical scores on homework than on exams. Scores will be entered on Gradescope. All requests for a regrade of a homework must be submitted to the instructors within one week of the day the work was returned to the class.

Academic Integrity

Behavior consistent with cheating, copying, and academic dishonesty is not tolerated. Depending on the severity, this may result in a zero score on the assignment or exam, and could result in a failing grade for the class or even expulsion. Purdue prohibits dishonesty in connection with any University activity. Cheating, plagiarism, or knowingly furnishing false information to the University are examples of dishonesty. (Part 5, Section III-B-2-a, University Regulations) Furthermore, the University Senate has stipulated that the commitment of acts of cheating, lying, and deceit in any of their diverse forms (such as the use of substitutes for taking examinations, the use of illegal cribs, plagiarism, and copying during examinations) is dishonest and must not be tolerated. Moreover, knowingly to aid and abet, directly or indirectly, other parties in committing dishonest acts is in itself dishonest. (University Senate Document 7218, December 15, 1972). You are expected to read both Purdue's guide to academic integrity (https://www.purdue.edu/purdue/about/integrity_statement.php) and Prof. Genes Spaffords guide (https://spaf.cerias.purdue.edu/integrity.html) as well. You are responsible for understanding their contents and how it applies to this class.

Posting Class Material: Posting material associated with this class (e.g., solutions to homework sets or exams) without the written permission of the instructor is forbidden and may be a violation of copyright.

Purdue's Honor Pledge: As a boilermaker pursuing academic excellence, I pledge to be honest and true in all that I do. Accountable together - we are Purdue.(https://www.purdue.edu/provost/teachinglearning/honor-pledge.html)

Grief Absence Policy

Purdue University recognizes that a time of bereavement is very difficult for a student. The University therefore provides the following rights to students facing the loss of a family member through the Grief Absence Policy for Students (GAPS). GAPS policy: Student will be excused for funeral leave and given the opportunity to earn equivalent credit and to demonstrate evidence of meeting the learning outcomes for missed assignments or assessments in the event of the death of a member of the student's family.

CAPS Information

Purdue University is committed to advancing the mental health and well-being of its students. If you or someone you know is feeling overwhelmed, depressed, and/or in need of support, services are available. For help, such individuals should contact Counseling and Psychological Services (CAPS) at (765)494-6995 and https://www.purdue.edu/caps/ during and after hours, on weekends and holidays, or by going to the CAPS office of the second floor of the Purdue University Student Health Center (PUSH) during business hours.

Missed or Late Class Work

If a student misses a homework because he or she didn't get around to doing it, then the grade will be 0 for that homework. If a student has a planned absence for a class when homework is due, the student should turn in the homework before it is due or email it to both the instructor and the teaching assistant by the time it is due. There is a penalty for late homework in this case. Homework will be accepted late without penalty in case of serious illness or bereavement.

If a student misses an exam, then the grade will be 0 for that exam, except in case of serious illness or bereavement, in which case the student will be given an opportunity to make up the exam. If a student has a planned absence for a class when an exam will be given, the student should make arrangement before the planned absence to take the exam early or to take a makeup exam after returning to campus.

Violent Behavior Policy

Purdue University is committed to providing a safe and secure campus environment for members of the university community. Purdue strives to create an educational environment for students and a work environment for employees that promote educational and career goals. Violent behavior impedes such goals. Therefore, violent behavior is prohibited in or on any University facility or while participating in any university activity.

Students with Disabilities

Purdue University is required to respond to the needs of the students with disabilities as outlined in both the Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990 through the provision of auxiliary aids and services that allow a student with a disability to fully access and participate in the programs, services, and activities at Purdue University.

Please tell the instructor at least one week in advance if you wish to take an exam there. If you have a disability that requires other special accommodation, please tell the instructor early in the semester. It is the student's responsibility to notify the Disability Resource Center of an impairment/condition that may require accommodations and/or classroom modifications. We cannot arrange special accommodations without confirmation from the Disability Resource Center.

Emergencies

In the event of a major campus emergency (such as a tornado, earthquake, flu epidemic or terrorist attack), course requirements, deadlines and grading percentages are subject to changes that may be necessitated by a revised semester

calendar or other circumstances beyond the instructor's control. Relevant changes to this course will be posted on Brightspace or can be obtained by contacting the instructor or TA via email or phone. You should read your Purdue email frequently.

Nondiscrimination

Purdue University is committed to maintaining a community which recognizes and values the inherent worth and dignity of every person; fosters tolerance, sensitivity, understanding, and mutual respect among its members; and encourages each individual to strive to reach his or her own potential. In pursuit of its goal of academic excellence, the University seeks to develop and nurture diversity. The University believes that diversity among its many members strengthens the institution, stimulates creativity, promotes the exchange of ideas, and enriches campus life.

Purdue University prohibits discrimination against any member of the University community on the basis of race, religion, color, sex, age, national origin or ancestry, marital status, parental status, sexual orientation, disability or status as a veteran. The University will conduct its programs, services and activities consistent with applicable federal, state and local laws, regulations and orders and in conformance with the procedures and limitations as set forth in Executive Memorandum No. D-1, which provides specific contractual rights and remedies.

Privacy

The Federal Educational Records Privacy Act (FERPA) protects information about students, such as grades. If you apply for a job or graduate school and wish to use the instructor as a reference, you should tell the instructor beforehand. Otherwise, the instructor cannot say anything about you to a prospective employer who might call. The instructor is happy to provide references and to write letters of recommendation for his students as needed.

Class Schedule

The class schedule can be found on Brightspace. Updates will be posted to Ed Discussion and/or Brightspace.

This syllabus is subject to change.

Criteria	0 points	1 points	2 points	3.5 points
Frequency and Quality of Questions	Asks fewer than 2 questions or makes fewer than 2 comments OR Has 2 questions or comments but makes them all during the last week of the module.	Asks a minimum of 2 questions or makes a minimum of 2 comments (or any combination) using Ed Discussion. Questions or comments are not all made during the last week of the module but are spread out throughout the course.	Asks a minimum of 3 questions using Ed Discussion or makes a minimum of 3 comments (or any combination) using Ed Discussion throughout module. Questions/comments are not all made during the last week of the module but are spread out throughout the course.	Asks a minimum of 4 questions using Ed Discussion or makes a minimum of 4 comments (or any combination) using Ed Discussion throughout module 1. Questions/comments are not all made during the last week of the module but are spread out throughout the course.
Frequency and Quality of Responses	Provides no accurate and thorough answer to classmates' questions using Ed Discussion throughout the module.	Provides minimum of one accurate and thorough answers to classmates questions	Provides a minimum of 2 accurate and thorough answers to classmates questions using Ed Discussion throughout the module.	Provides a minimum of 3 accurate and thorough answers to classmates questions using Ed Discussion throughout the module.

Table 1: Ed Discussion Course Participation Rubric