Syllabus

Instructor: Christina Garman (clg@purdue.edu)

Course Webpage: Brightspace

1 Overview

Cryptography has shown itself to be invaluable in our everyday lives, especially as more and more of our devices and interactions are moving to the online world. Whether it is browsing the web, making a purchase, or sending a message to a friend, cryptography is everywhere. Despite the fact that we (often unknowingly) rely on the security of systems that use cryptography in much of our daily lives, in recent years we have seen a number of serious vulnerabilities in the cryptographic pieces of systems, some with large consequences. These have been caused by various problems, including poor designs, difficulty of implementation, and use (or misuse) of (in)secure primitives.

This course will teach cryptography and cryptographic design principles as they are applied to real world systems, both in how to correctly use cryptography to build secure systems as well as examining flaws and "breaks" in already deployed systems. We will discuss the mistakes that led to these flaws, how these flaws could have been prevented, and various tools and techniques that exist for building cryptographic systems in practice. We will also examine modern cryptographic techniques and how they are being used to build more secure and/or more private systems. Students will have the opportunity to implement cryptographic schemes and explore cryptographic failures in practice, as well as engage in a semester-long research project related to applied cryptography.

Time: M/W 4:30pm - 5:45pm
Location: GRIS 133

Prerequisites:

- CS 526 (Information Security) or CS 426 (Computer Security) or permission of the instructor
- Programming experience: Some of the assignments will require programming knowledge and we will be implementing cryptographic schemes, so you should be comfortable programming.
- Strongly recommend either: CS 355 (Introduction to Cryptography) or CS 555 (Cryptography and Data Security) but not required.

2 Office Hours

TBA

I will be available by appointment as well.

3 Grading

The course will be largely lecture based, though we will occasionally be reading and presenting/discussing papers. We will also have a few projects/assignments, both in implementing cryptographic schemes as well as exploring cryptographic failures in practice. Finally, there will be a semester-long research project related to applied cryptography.

While this is a lecture-based course, discussion will still be very important, so part of your grade will include a participation component. So please attend class! If you cannot make class for any reason (such as job interviews, etc.), please let me know as you will not be penalized for this.

- Assignments: 45%
- Midterm: 20%
- Course Project: 25%
- Class participation: 10%

Assignments are due at the beginning of class at 4:30pm on the stated due date. Late assignments will be penalized 5 percentage points per day. There is no collaboration allowed on exams. You must do only your own work. There are no textbooks, notes, or computers allowed during exams.

Final grades will be assigned on a curve at the end of the course.

4 Schedule

Please refer to the course webpage for the most up-to-date schedule as it is subject to change.

Tentative schedule:

Week	**Topic**
Week 1	Introduction
Week 2	Basics of Cryptography
Week 3	Introduction to Symmetric Cryptography
Week 4	Introduction to Public Key Cryptography
Week 5	TLS
Week 6	TLS Attacks
Week 7	Protocols (Authentication, SSH, Secure Messaging, Signal, etc.)
Week 8	Cryptographic Hardware
Week 9	Cryptographic Side-channels
Week 10	Provable Security
Week 11	Provable Security
Week 12	Multi-party computation (MPC)
Week 13	Zero-knowledge proofs
Week 14	Ethics, Law, and Policy
Week 15	Make-up/Catch-up/Relevant current topics

5 Additional Resources

We will be using Brightspace to submit assignments.

Students are expected to have read the associated paper(s) BEFORE each class.

If you have any suggestions for papers that you would like to present, please let me know!

No textbook is required, but if you would like additional resources the following may be useful:
Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (`http://cacr.uwaterloo.ca/hac/`)
Modern Cryptography: Theory and Practice by Wenbo Mao
Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell (`http://www.cs.umd.edu/~jkatz/imc.html`)

6 Disclaimer

I will adhere to this syllabus as much as is reasonable, but there is always the possibility that outside circumstances will require changes and adjustments. I retain the ability to amend or alter the syllabus without notice, though I will strive to provide as much notice as possible.

7 Netiquette

When interacting online via email or the discussion boards, you are encouraged to comment, question, or critique ideas but you should not attack other individuals. Consider that sarcasm and humor can be misconstrued in online interactions and generate unintended disruptions. Please read the Netiquette rules for this course:

- Do not dominate any discussion. Give other students the opportunity to join in the discussion.
- Do not use offensive language. Present ideas appropriately.
- Be cautious in using Internet language. For example, do not capitalize all letters since this suggests shouting.
- Avoid using vernacular and/or slang language. This could possibly lead to misinterpretation.
- Keep an "open-mind" and be willing to express even your minority opinion.
- Think and edit before you push the "Send" button.
- Do not hesitate to ask for feedback.

8 Academic Dishonesty

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 72-18, December 15, 1972] Please review the following resource page on plagiarism: `http://www.education.purdue.edu/discovery/research_integrity.html`.

9 Computer Science Department Academic Integrity Policy

The Department of Computer Science expects and enforces the highest standards of academic integrity and ethics. The Department takes severe action against academic dishonesty, which may include failing grades on an assignment or in a course, up to a recommendation for dismissal from the University.

Academic dishonesty is defined as any action or practice that provides the potential for an unfair advantage to one individual or one group. Academic dishonesty includes misrepresenting facts, fabricating or doctoring data or results, representing another's work or knowledge as one's own, disrupting or destroying the work of others, or abetting anyone who engages in such practices.

Academic dishonesty is not absolute because the expectations for collaboration vary. In some courses, for example, students are assigned to work on team projects. In others, students are given permission to collaborate on homework projects or to have written materials present during an examination. Unless otherwise specified, however, the CS Department requires all work to be the result of individual effort, performed without the help of other individuals or outside sources. If a question arises about the type of external materials that may be used or the amount of collaboration that is permitted for a given task, each individual involved is responsible for verifying the rules with the appropriate authority before engaging in collaborative activities, using external materials, or accepting help from others.

A student accused of academic dishonesty must be afforded due process as defined by Purdue University procedures. The Dean of Students Office may be notified concerning an academic dishonesty incident as provided by Purdue University procedures.

10 Incompletes

A grade of Incomplete (I) will be given only in unusual circumstances. To receive an "I" grade, a written request must be submitted and approved by the instructor. Requests are accepted for consideration but in no way ensure that an incomplete grade will be granted. The request must describe the circumstances, along with a proposed timeline for completing the course work. You will be required to fill out and sign an "Incomplete Contract" form that will be turned in with the course grades. Any requests made after the course is completed will not be considered for an incomplete grade.

11 Attendance Policy

This course follows Purdue's academic regulations regarding attendance, which states that students are expected to be present for every meeting of the classes in which they are enrolled. When conflicts or absences can be anticipated, such as for many University-sponsored activities and religious observations, the student should inform the instructor of the situation as far in advance as possible. For unanticipated or emergency absences when advance notification to the instructor is not possible, the student should contact the instructor as soon as possible by email or on Piazza. When the student is unable to make direct contact with the instructor and is unable to leave word with the instructor's department because of circumstances beyond the student's control, and in cases falling under excused absence regulations, the student or the student's representative should contact or go to the Office of the Dean of Students (ODOS) website to complete appropriate forms for instructor notification. Under academic regulations, excused absences may be granted by ODOS for cases of grief/bereavement, military service, jury duty, parenting leave, or emergent or urgent care medical care. For details, see the Academic Regulations & Student Conduct section of the University Catalog website.

Guidance on class attendance related to COVID-19 are outlined in the Protect Purdue Pledge for Fall 2022 on the Protect Purdue website.

12 Academic Guidance in the Event a Student is Quarantined/Isolated

If you must miss class at any point in time during the semester, please reach out to me via email or CampusWire so that we can communicate about how you can maintain your academic progress. If you find yourself too sick to progress in the course, notify your adviser and notify me via email or Piazza. We will make arrangements based on your particular situation. Please note that, according to Details for Students on Normal Operations for Fall 2021 announced on the Protect Purdue website, "individuals who test positive for COVID-19 are not guaranteed remote access to all course activities, materials, and assignments."

13 Classroom Guidance Regarding Protect Purdue

Any student who has substantial reason to believe that another person is threatening the safety of others by not complying with Protect Purdue protocols is encouraged to report the behavior to and discuss the next steps with their instructor. Students also have the option of reporting the behavior to the Office of the Student Rights and Responsibilities. See also Purdue University Bill of Student Rights and the Violent Behavior Policy under University Resources in Brightspace.

14 Emergency Statement

In the event of a major campus emergency, course requirements, deadlines and grading percentages are subject to changes that may be necessitated by a revised semester calendar or other circumstances.

15 Accessibility

Purdue University is committed to making learning experiences accessible. If you anticipate or experience physical or academic barriers based on disability, you are welcome to let me know so that we can discuss options. You are also encouraged to contact the Disability Resource Center at: drc@purdue.edu or by phone: 765-494-1247.

16 Disability Statement

Students with disabilities must be registered with Disability Resource Center in the Office of the Dean of Students before classroom accommodations can be provided. If you are eligible for academic accommodations because you have a documented disability that will impact your work in this class, please schedule an appointment with me as soon as possible to discuss your needs.

17 Nondiscrimination Statement

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 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. A hyperlink to Purdue's full Nondiscrimination Policy Statement is included in our course Brightspace under University Policies.

18 Mental Health/Wellness Statement

If you find yourself beginning to feel some stress, anxiety and/or feeling slightly overwhelmed, try Well-Track. Sign in and find information and tools at your fingertips, available to you at any time.

If you need support and information about options and resources, please contact or see the Office of the Dean of Students. Call 765-494-1747. Hours of operation are M-F, 8 am-5 pm.

If you find yourself struggling to find a healthy balance between academics, social life, stress, etc. sign up for free one-on-one virtual or in-person sessions with a Purdue Wellness Coach at RecWell. Student coaches can help you navigate through barriers and challenges toward your goals throughout the semester. Sign up is completely free and can be done on BoilerConnect. If you have any questions, please contact Purdue Wellness at evans240@purdue.edu.

If you're struggling and need mental health services: 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 mental health support, services are available. For help, such individuals should contact Counseling and Psychological Services (CAPS) at 765-494-6995 during and after hours, on weekends and holidays, or by going to the CAPS office on the second floor of the Purdue University Student Health Center (PUSH) during business hours.

19 Basic Needs Security

Any student who faces challenges securing their food or housing and believes this may affect their performance in the course is urged to contact the Dean of Students for support. There is no appointment needed and Student Support Services is available to serve students 8 a.m.-5 p.m. Monday through Friday. Considering the significant disruptions caused by the current global crisis as it related to COVID-19, students may submit requests for emergency assistance from the Critical Needs Fund.