ECE 59500 - Introduction to Applied Cryptography

Fall 2024

Lecture Time: TR 4:30pm – 5:45pm, **Place:** Hampton Hall of Civil Eng 2107

Instructor:
Prof. Zahra Ghodsi, Office: BHEE 331A
Office Hours: Mon 3pm–4pm, Wed 11am–12pm
Email: zahra@purdue.edu

Course Page: Content delivery on Brightspace.

Prerequisites: An undergraduate-level understanding of probability and algorithms is assumed.

Course References:

- Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography*, 3rd Edition, Chapman & Hall/CRC, 2020.
- Supplemental material handed out in class.

For reference only
Subject to change

Course Description: Cryptography is an essential component of securing communication and data in a wide range of applications. This course explores fundamental building blocks in cryptography such as ciphers, hash functions, and digital signatures. We will then demonstrate how these building blocks are used practically to secure communications and systems. We will also learn about the power of advanced cryptography to enable complex functionalities with rigorous security guarantees. We will cover fundamental secure multiparty computation protocols and review their application in building secure and privacy-preserving systems. We will also explore social and ethical issues in developing and deploying cryptographic systems.

Tentative Grading Policy:

20% Labs
20% Homeworks
10% Weekly reading
50% Final Project
- 5% Project proposal
- 10% Project update
- 15% Project presentations
- 20% Project final report

Labs and Homeworks: Homeworks and labs (roughly posted every 1 or 2 weeks) should be submitted individually by each student. Homeworks cover concept and analytical questions, whereas labs require programming (in `Python` or `C/C++`).

Weekly Reading: Each week there will be a reading assignment for which you have to submit a short summary paragraph. Additionally, a few students will sign up to lead the discussion of the reading assignment in class. You have to sign up as discussion lead at least once over the semester, and your participation in weekly discussions contribute towards your grade.

Final Project: The final project is an important part of this class. Students will work on a semester long project in groups of two. Individual projects are also acceptable as long as it's an ongoing research project that is related to the course. There will be four deliverables for projects. Please use LaTeX for all write-ups, and follow the USENIX format. Each deliverable should include specific details which will be announced in class ahead of time.

Tentative Course Outline (subject to change):

Week	Lecture	Project checkpoints
1	Introduction and historical ciphers	
2	Private key cryptography	
3	Message authentication and hash functions	
4	Symmetric key constructions	
5	Hardness assumptions and key management	
6	Public key cryptography and digital signatures	
7	PKI, PGP, SSL/TLS, multi-factor authentication	
8	Secret sharing	Proposals (due Fri Oct 11th)
9	Threshold cryptosystems	
10	Secure multi-party computation I	
11	Secure multi-party computation II	
12	Partial homomorphic encryption and commitments	Update (due Fri Nov 8th)
13	Cryptography for secure machine learning	
14	Ethics of cryptographic work	
15	(Last week of class)	Presentations (Week of Dec 2nd) Final report (due Fri Dec 6th)

For reference only
Subject to change

ECE 59500 Specific Academic Dishonesty Guidelines

Professionalism and Academic Honesty:

For the purposes of this class, we broadly define academic dishonesty as being any attempt by a student to improve a grade beyond his or her own personal understanding of the material. Evidence of lack of personal understanding often manifests itself in the form of work that is substantially similar to that of other students (i.e., copied). To ascertain levels of similarity, we use computer software to analyze the submitted work of the entire class. When we find inordinate similarity between the work of two or more students, we act on it. All documented cases of academic dishonesty will result in, at minimum, a zero score for all work in question for each student involved and at the instructor's discretion may result in a failing grade for the course. In addition all incidents of academic misconduct will be forwarded to the Office of Student Rights and Responsibilities (OSRR), where university penalties may be considered.

Academic integrity is one of the highest values that Purdue University holds. Individuals are encouraged to alert university officials to potential breaches of this value by either emailing integrity@purdue.edu or by calling 765-494-8778. While information may be submitted anonymously, the more information is submitted the greater the opportunity for the university to investigate the concern. Students are also encouraged to inform the course staff about their own mistakes before they are detected by the course staff. Depending on the severity of the circumstance, a penalty may still be imposed, but we will always make sure it is better than if it is found by the course staff.

Use of artificial intelligence (AI) or Large Language Models (LLM): Unless otherwise announced, students are permitted to use generative AI/LLM tools, but only for the purposes of experimentation, and in order to learn, train and practice material presented in the lectures and labs. However, you must exercise caution while using them. These tools are trained to produce results based on a large amount of public information, all of which may not be accurate, and therefore the tools themselves may produce inaccurate and/or inconsistent results. Your first reference for all concepts covered in this class must always be the course materials, such as lecture notes, hws/labs descriptions, and documents hosted on the course Brightspace page. *Students are explicitly prohibited from presenting the output of such tools, or any portion of the output, (eg. ChatGPT's response to any prompt) as their own work in any type of course assignment.* Such an action will be treated as an academic integrity violation, and will be handled the same way as any other academic integrity violation. When in doubt, always ask the instructor.

Purdue Specific Guidelines

Copyright: See the University Policies and Statements section of Brightspace for guidance on Use of Copyrighted Materials. Effective learning environments provide opportunities for students to reflect, explore new ideas, post opinions openly, and have the freedom to change those opinions over time. Students and instructors are the authors of the works they create in the learning environment. As authors, they own the copyright in their works subject only to the university's right to use those works for educational purposes Students may not copy, reproduce other outlet (e.g., YouTube, Facebook, or other open media sources or websites) any work in which they are not the sole or joint author or have not obtained the permission of the author(s).

Nondiscrimination: Purdue University is committed to maintaining a community that 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 and Statements.

Mental Health and Wellness: If you find yourself beginning to feel some stress, anxiety and/or feeling slightly overwhelmed, try WellTrack. 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 a.m.- 5 p.m. 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 free and can be done on BoilerConnect. 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.

Basic Needs and 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.

Emergency Preparedness: 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 beyond the instructor's control. Relevant changes to this course will be posted onto the course website or can be obtained by contacting the instructors or TAs via email or phone. You are expected to read your @purdue.edu email on a frequent basis. A link to Purdue's Information on Emergency Preparation and Planning is located on our Brightspace under "University Policies and Statements." This website covers topics such as Severe Weather Guidance, Emergency Plans, and a place to sign up for the Emergency Warning Notification System. I encourage you to download and review the Emergency Preparedness for Classrooms document (PDF) or (Word). The first day of class, I will review the Emergency Preparedness plan for our specific classroom, following Purdue's required Emergency Preparedness Briefing. Please make note of items like: · The location to where we will proceed after evacuating the building if we hear a fire alarm. · The location of our Shelter in Place in the event of a tornado warning. · The location of our Shelter in Place in the event of an active threat such as a shooting.

A link to Purdue's Information on Emergency Preparation and Planning is located on our Brightspace under "University Policies and Statements." This website covers topics such as Severe Weather Guidance,

For reference only
Subject to change

Emergency Plans, and a place to sign up for the Emergency Warning Notification System. I encourage you to download and review the Emergency Preparedness for Classrooms document here.

Netiquette: We want to foster a safe online learning environment. All opinions and experiences, no matter how different or controversial they may be perceived, must be respected in the tolerant spirit of academic discourse. You are encouraged to comment, question, or critique an idea, but you may not attack an individual. Our differences, some of which are outlined in the University's nondiscrimination statement below, will add richness to this learning experience. Please consider that sarcasm and humor can be misconstrued in online interactions and generate unintended disruptions. Working as a community of learners, we can build a polite and respectful course ambience. Please read the Netiquette rules for this course:

- Monitor how much space/time you are taking up in 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 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.
- Seek and take in feedback from others; learning from other people is an important life skill.

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. See the University Policies and Statements on our course Brightspace for more information on the Violent Behavior Policy.

Diversity, Inclusion & Belonging:

- In our discussions, structured and unstructured, we will explore a variety of challenging issues, which can help us enhance our understanding of different experiences and perspectives. This can be challenging, but in overcoming these challenges we find the greatest rewards. While we will design guidelines as a group, everyone should remember the following points:
  - We are all in the process of learning about others and their experiences. Please speak with me, anonymously if needed, if you have concerns about aspects of/experiences in the course.
  - Intention and impact are not always aligned, and we should respect the impact something may have on someone even if it was not the speaker's intention.
  - We all come to the class with a variety of experiences and a range of expertise, we should respect these in others while critically examining them in ourselves."
- This course, as with every course offered at Purdue, plays a part in creating and sustaining a welcoming campus where all students can excel. There are many initiatives in the electrical and computer engineering department and supported by the university focused on this goal, and this course is designed to take advantage of those resources. Learning experiences and assignments address diversity and inclusion, not because they are "topics," but because they are necessary to prepare students to be successful in a diverse, global environment.

For reference only
Subject to change

- We strive for equity, providing equal access and opportunity, and working to maximize student potential. This requires both instructor and students to identify and remove barriers that may prevent someone from full access or full participation. You can help by:
  - Contacting me, anonymously if needed, if you see a potential barrier for someone or yourself in participating fully in the class. This might be a physical barrier such as access to technology or a personal situation.
  - Suggesting ways in which members of our class can support each other. Virtual study groups and discussion boards are examples, but I encourage you to be creative in your ideas.
  - Getting to know each other as contributing members of our learning community. Everyone has something to contribute, and while I designed the course to take advantage of the wealth of knowledge, expertise, and experience we bring together, I cannot do it well without your participation. There are many opportunities built into this course for this type of work. It is important we do it together.

Disclaimer: This syllabus is subject to change. You will be notified of any changes as far in advance as possible via an announcement on Brightspace. Monitor your Purdue email daily for updates.

For reference only
Subject to change