The most important part of this class is a semester-long course project. The project will require significant self-directed effort and learning outside of class. It is the biggest part of your grade and the main source of outside-of-classroom work. You may work on the project in groups of up to 4 students. Every member of the group will be expected to contribute.

The project requires the following deliverables. The exact contents of the updates/report may differ from what is listed here based on the nature of your particular project.

1. **Pre-proposal meeting:** Form your group, start thinking about project ideas, and meet with the instructor to decide on your project plan and scope. You can either pick a project of your design or choose a project suggested later in this document. Multiple groups cannot do the same project. If you try to schedule this meeting at the last minute and there is not enough time to meet, you will not receive credit.

2. **Project proposal:** In 1 page (in any format), describe what the project will be, what work you intend to complete by each project update, and roughly what each group member will do.

3. **Project update 1:** 2-3 page document typeset in Latex using IEEE document style. This update should consist of 1) an introduction motivating and describing your project goals, 2) a related work section summarizing existing tools or approaches to solving your problem or related problems, 3) a brief sketch of how your solution/tool will work, and 4) a summary of what has been done so far and what each group member has done.

4. **Project update 2:** 4-6 page document with same formatting requirement as above that has an introduction and related work section from the first update, followed by a section describing your solution to the problem in some detail, and a discussion section explaining some of the design decisions you faced in making your solution and any implications of choices you made. Also include a summary of what has been done/what remains to be done and what each group member has done since the last update.

5. **Final presentation:** present your project in front of the class. Motivate the problem, explain your solution, and present any evaluation or implementation you did. This should be a presentation that will be accessible to a broad CS audience, not one tailored to security or privacy experts.

6. **Final report:** 5-10 page document that has introduction, related work, overview of your solution, discussion of the design (potentially revised from previous updates), any necessary technical details needed to understand your solution, a brief evaluation of your resulting tool/scheme, and a brief description of what could be completed in future work. Please also state what each group member has done since the last update. If you can keep this one to 7 pages that would be great, but up to 10 pages are allowed.
Some Potential Project Ideas

- Build an end-to-end encrypted private messaging application (desktop, web-based, or mobile – your choice). In addition to having end-to-end encryption, the system should allow users to authenticate their sessions with each other out of band and make an effort to reduce the amount of user metadata it requires to deliver messages.

- Build a tool for end-to-end encrypted private file storage on top of a public cloud storage system, e.g., Google drive or dropbox. In addition to encrypting files, the tool should try to hide metadata like file names and which files you are accessing/modifying. If time permits, a cryptographic tool like ORAM may be a good thing to study and discuss.

- Build a tool for a group of users, each of which holds sensitive private data, to compute joint statistics on their data, without sharing it. This will require learning about and implementing cryptographic multiparty computation (MPC) techniques.

- Build a tool that allows users to stay logged in to a few selected sites, e.g., news websites, while browsing the web on private browsing mode, while maintaining the benefits of this mode for other sites. Use hardware enclaves to protect and hide information needed across multiple sessions. This will require building a browser extension that manipulates session cookies and connects the browser to the hardware enclave.

- Suggest a project of your own design. The project should be large enough to involve a semester’s worth of work. A good starting point for this is to think of some technology with which you regularly interact that would benefit from additional privacy features.

- Talk to instructor about undertaking a small research project

- Use your own pre-existing security or privacy-related research as the course project