Code Review 1: Signal and Auth

For our first code review of the semester, we will evaluate your conceptual understanding of the Signal and Auth projects. To sign up for a code review, please use the link provided here. Please sign up for only one slot using your Brown email address. If you cannot make any of the listed slots, please reach out to the TA staff by email or Edstem by no later than *Monday, March 2nd*. Code review slots will be distributed on a first-come, first-served basis. If you have known conflicts, we suggest signing up as soon as possible. Code reviews will run from *Saturday, February 28th* through *Friday, March 6th*.

1 Format

Code reviews will be conducted in-person, 1-on-1 with a member of the course staff. The location of the code review will be listed here once the room bookings are finalized. The only exception is for students in the online section or given explicit permission from the instructor (with a Dean's note or a doctor's note), who will conduct their code reviews over Zoom.

Code reviews will take no longer than 15 minutes each. In your code review, you will be asked 2 conceptual questions. The first will be about the Signal project, the second will be about the Auth project.

Code reviews will be closed-book, meaning you will have no access to outside resources or your code during the review. We will ask conceptual questions that do not rely upon specifics of the code, but rather the higher-level protocols and principles found in the projects.

2 Preparing for the Code Review

2.1 Reviewing Content

To prepare for your code review, we suggest several key approaches:

1. **Assignment Handouts**: Reviewing the assignment handouts will be extremely relevant to code reviews. In particular, we suggest reviewing the *Background Knowledge* section of both Signal and Auth, which includes information you may be evaluated on.

2. **Lecture Notes/Recordings**: Lecture notes and recordings are an excellent resource to solidify conceptual understanding.

3. **Implementation**: Reviewing your implementation, especially for parts of your code that you find conceptually confusing, would be a strong preparation strategy. We will not ask specifics about the code, but this can help brush up your conceptual understanding.

4. **Edstem**: If you have specific questions or concerns, feel free to reach out to the course staff, and we will do our best to resolve them.

2.2 Relevant Material

Below is an exhaustive list of all broad topics from which questions could be drawn, separated by project.

1. **Signal**: Diffie-Hellman key exchange, Diffie-Hellman ratchet, key derivation, authenticated encryption.

2. **Auth**: One- and two- sided authenticated key exchange, password-based authentication with salt and pepper, two-factor authentication.

Using the strategies described in Section 2.1 for each of the above topics will more than adequately prepare you for the code review. All questions are related to the conceptual things from projects, not homeworks. Topics such as attacks (man-in-the-middle, replay, etc.) and various security types (CCA, CPA, etc.) will not be evaluated.

3 Miscellaneous

3.1 Accommodations

If you have SAS Accommodations that permit additional time for evaluation, the instructor will reach out directly via email with information on how to sign up for an extended code review slot. If you have accommodations but have not received an email by *Monday, March 2nd*, please reach out to the instructor by email.

3.2 Unable to find a Time Slot

If you cannot make any of the listed slots, please reach out to the TA staff by email or Edstem by no later than *Monday, March 2nd*. If you do not reach out by then, we will be unable to accommodate any other slots. You must provide direct information on what your conflicts are that prevent you from making any of the available times.