Problem Set 1: Will be posted this evening, and due Tuesday, February 18, at 11:59pm. Note that this problem set is to be done in groups, and that groups will be assigned for the first three problem sets.

Outline for today:

- Rivest’s “Killian Lecture” (see slides)
- The “One-Time Pad” (see slides)
  - Suggested reading: Katz and Lindell, Modern Cryptography, Chapter 2.

Reminder: Class website is here: https://courses.csail.mit.edu/6.857/2020/

News: What went wrong with the Democratic caucus in Iowa yesterday?