

6.857 Administrivia

Ron Rivest and Yael Kalai

February 22, 2021

- **Outline for today:**
 - **Welcome!**
 - Rivest's "**Killian Lecture**" (see slides)
 - Suggested reading: Diffie & Hellman "New Directions in Cryptography"
 - The "**One-Time Pad**" (see slides) [Maybe]
 - Suggested reading: Katz and Lindell, Modern Cryptography, Chapter 2.
- **Problem Set 1:** Will be posted this evening, and due **Tuesday, March 9, 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.
- **Reminder:** Class website is here:

<https://courses.csail.mit.edu/6.857/2021/>

See Piazza for forum, zoom links, etc.