Each 6.1800 lecture will come with an outline. You can fill this in during lecture, after lecture, or not at all — it's entirely up to you how you use it. The goal of these outlines is to help you understand the main points that you should be taking away from each lecture. In some cases we will also include examples of things you should be able to do after each lecture.

In the past, these outlines have proved to be an effective tool for studying for the exams. Note that the outlines are ***not exhaustive****; there will be topics and nuances in lecture that aren't captured by the outline.*

Lecture 24: Tor

- Why don't secure channels encrypt packet headers? What can an adversary learn from observing packet headers?
- How is using public-key cryptography for encryption different from using it for signatures?
    - *A good test: what operations are present in each scheme? What are the public keys used for? The secret keys? Who performs what action?*

We're going to build up to a working version of onion routing. Along the way you should understand:

- What is the problem with using a single proxy between A and S?
- What is the problem with using multiple proxies between A and S (without onion routing)?
- In onion routing, suppose A wants to send a packet to S through P1, P2, and P3.
    - What layers of encryption — and in what order — should A apply?
    - What action does each proxy in the circuit take as it forwards A's packet along?
    - How does A set up the circuit?
- The scheme shown in lecture doesn't allow S to send packets back to A in the same way. Why not?
    - *Bonus question: how would using symmetric keys on each link address this issue?*

- What attacks is Tor still open to?
- What can a single proxy (without onion routing) be useful for?