Problem Set 7

This problem set is due on *Thursday, November 9* at the end of class.

Each solution is to be handed in *separately*, i.e. on separate sheets of three-hole punched paper. If the solution to a single problem takes more than one page, staple together only the pages relative to the same problem. Mark the top of each sheet with your name, 6.915, the problem number, and the date.

If you collaborate with other students, you MUST write up solutions on your own and acknowledge the people you work with.

Problem 7-1. Fingerprinting vs. Steganography

One of the drawbacks of using cryptography to protect privacy in communications is that although encrypted messages will not be understood they may look suspicious and attrack attention because unintelligible.

Steganography is the technique that allows to send a secret message embedded into a larger message that may look completely normal to an adversary. For example Alice can send a encoded picture of her dog to Bob and change all the low order bits of each pixel in order to encode a message. An evesdropper Eve would just think that Alice is showing her dog to Bob.

Steganography and fingerprinting have thus something in common. Both techniques embed a "message" in a larger object in a way that the larger object functionality is not compromised.

Comment on the similarities and the difference in goals between the two techniques. Also comment how the differences would influence the design of a steganographic scheme versus a fingerprinting scheme.

Problem 7-2. Clark–Wilson Integrity Model

We saw in class that the CW integrity model relies on the existence of so-called **Integrity Validation Procedures** (or IVPs). One of the problems that has been identified in trying to apply the CW model in actual settings is that it is not always clear how such IVPs can be actually constructed or carried out.

Discuss the question of existence of IVPs. Give examples in which the IVP assumption is unreasonable. How well does the CW model works in cases in which IVPs are not available?