Problem Set 1

This problem set is due *online,* at `https://courses.csail.mit.edu/6.857/` on *Friday, February 24* by **11:59 PM**. Please note that no late submissions will be accepted.

You are to work on this problem set with your assigned group of three or four people. You should have received an email with your group assignment for this problem set. If not, please email `6.857-tas@mit.edu`. Be sure that all group members can explain the solutions. See Handout 1 (*Course Information*) for our policy on collaboration.

Homework must be submitted electronically! Each problem answer must appear on a separate page. Mark the top of each page with your group member names, the course number (6.857), the problem set number and question, and the date. We have provided templates for LaTeX and Microsoft Word on the course website (see the *Resources* page).

Grading: All problems are worth 10 points.

With the authors' permission, we will distribute our favorite solution to each problem as the "official" solution—this is your chance to become famous! If you do not wish for your homework to be used as an official solution, or if you wish that it only be used anonymously, please note this in your profile on the homework submission website.

Problem 1-1. Security Policy for Cars

Cars are becoming rapidly computerized—a modern car may contain as many as 20 CPU's in it, and manufacturers are networking them together. In addition, cars are gaining access to wireless or cellphone networks, and providing access to internet-based services (and even basic internet access for the cars occupants or their devices).

Imagine you are buying a very nice car fifteen years from now.

(a) What information-processing and communication services do imagine your car might contain, or provide?

(b) Write a security policy governing these information processing and communication services. Be as explicit as you can.

(This problem is a bit open-ended, but should give you excellent practice in writing a security policy. Also, you may actually care about such security policies when you buy a car in the future!)

Problem 1-2. Cryptosystem proposal by Nash

In the 1950's the mathematician John Nash (now famous for his work on game theory, and also the subject the movie *A Beautiful Mind*), privately proposed to the National Security Agency (NSA) an idea for a cryptosystem.

This proposal was just declassified (*two weeks ago*!); a copy of it is available on the class website as Handout # 3, together with some relevant correspondence with the NSA.

Note that this proposal was not accepted by the NSA, who said that it didn't meet their security requirements.

What reasons, if any, can you figure out for this rejection?

(Note that this assignment is a bit of an open problem! Do the best you can, and write up what you can figure out. We don't know the answer to this question ourselves...)