Problem Set 7

This meta-problem-set is due on *Thursday, November 12, 1998* at the end of class. Late homeworks will *not* be accepted. You are to work on this problem set in groups of three to four people. Mark the top of each sheet with your names, 6.857, the problem set number and question, and the date. **Type up your solutions**, and be clear. Points may be deducted if your TA has problems understanding your solution. We strongly recommend you get started on this problem set early.

Problem 7-1. Project Proposal

Please submit an initial proposal for your term project. It should be less than a page and describe the topic you plan to research, and the names of the people who will be on the team.

Several past projects are available on the web, and the following are titles of some other past ones:

- *Implementation Notes for a Platform for Internet Content Selection System*
- *SHTTP and SSL*
- *ElGamal Based Threshold Signature*
- *A Study of Secure Sockets Layer*
- *Steganography*
- *Providing Software Services on the WWW Securely*
- *Java Security*
- *Poking Holes in Athena*
- *Security Requirements for Uniform Resource Identifiers*
- *Alladin: An Authentication System Based on MD5*
- *Verification of the iKP Family of Protocols*
- *Internet Security Protocols*
- *Copyright in the Information Age: A survey of the legal and technical aspects*
- *DCE and Security*
- *PayMe! : A customer-oriented efficient micropayment scheme*
- *Designing Secure Programs in Java*

The topic can be either implementation oriented or research/design oriented, but must be appropriate for a group of your size.