Problem Set 6

This problem set is due on *Thursday, October 29, 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 6-1. Protocol Design

Design and analyze a protocol for the following situation.

Alice is an employee of ABC Corp. She has a public RSA key P_A and a secret RSA key S_A. ABC has many PC's, any one of which Alice may wish to sit down at and log in to. All the PC's run the same software, and all are connected to a central ABC server via a network. The server is capable of storing user files remotely and securely, and capable of performing secure cryptographic operations securely. Assume that the PC and server software is secure, but that the network connection is not secure.

Alice wishes to use her secret key S_A to sign documents, etc. However, she does not have a smart card or any secure way of carrying her secret key with her from PC to PC. Alice is, however, capable of remembering a password.

Your answer should show:

- How the server can store an encrypted form of Alice's secret key.
- How Alice can securely download the secret key from the server.
- How well your protocol protects Alice's secret key from various attacks, including at least:
  - An off-line dictionary search for Alice's password by a passive eavesdropper who overhears Alice download her secret key (your solution should definitely protect Alice against this threat).
  - An attack on Alice's secret key by a corrupted server.
  - An on-line attack by someone attempting to impersonate Alice to the server.
  - An on-line attack by someone attempting to impersonate the server to Alice.

You should also try to be efficient, and minimize the number of messages required by the protocol.

Problem 6-2. Generalized Secret-Sharing

Suppose you are given a formula involving people's names as atomic formula, and the operators AND and OR, such as

$$\mathit{Alice} \text{ OR } ((\mathit{Bob} \text{ AND } (\mathit{Charles} \text{ OR } \mathit{David})) \text{ OR } (\mathit{David} \text{ AND } \mathit{Ethan}))\ .$$

How can you do generalized secret-sharing so that any combination of the people named that satisfy the formula will be able to obtain the secret?

Does your solution generalize to handle the operator $Threshold_k(F_1, \ldots, F_n)$ where the F_i are formulas (possibly involving the threshold operator), and k is an arbitrary integer, $0 < k < n$?