# Homework 3

**Due Date**: May 3, 2001
**Points**: 100

1. (*20 points*; text, exercise 5.2) Given the security levels TOPSECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, say what type of access (read, write, or both) is allowed in the following situations. Assume discretionary access controls allow anyone access unless otherwise specified.
   a. Paul, cleared for (TOPSECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).
   b. Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).
   c. Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).
   d. Sammi, cleared for (TOPSECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).
   e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).
2. (*20 points*; text, exercise 6.5) Explain why the system controllers in Lipner's model need clearances of (SL, { D, PC, PD, SD, T }).
3. (*20 points*; text, exercise 7.4) Consider using mandatory access controls and compartments to implement an ORCON control. Assume there are $k$ different organizations. Organization $i$ will produce $n(i,j)$ documents to be shared with organization $j$.
   a. How many compartments are needed to allow any organization to share a document with any other organization?
   b. Now assume that organization $i$ will need to share $n_m(i, i_1, \ldots, i_m)$ documents with organizations $i_1, \ldots, i_m$. How many compartments will be needed?
4. (*20 points*; text, exercise 9.11) Please prove the following:
   a. If $p$ is a prime, $\phi(p) = p-1$.
   b. If $p$ and $q$ are both prime, $\phi(pq) = (p-1)(q-1)$.
5. (*20 points*; text, exercise 11.6) Needham and Schroeder suggest the following variant of their protocol:
   a. Alice $\rightarrow$ Bob : Alice
   b. Bob $\rightarrow$ Alice : { Alice, $rand_3$ } $k_{Bob}$
   c. Alice $\rightarrow$ Cathy : { Alice, Bob, $rand_1$, { Alice, $rand_3$ } $k_{Bob}$ }
   d. Cathy $\rightarrow$ Alice : { Alice, Bob, $rand_1$, $k_{session}$, {Alice, $rand_3$, $k_{session}$} $k_{Bob}$ } $k_{Alice}$
   e. Alice $\rightarrow$ Bob : { Alice, $rand_3$, $k_{session}$ } $k_{Bob}$
   f. Bob $\rightarrow$ Alice : { $rand_2$ } $k_{session}$
   g. Alice $\rightarrow$ Bob : { $rand_2$–1 }$k_{session}$

   Show that this protocol solves the problem of replay due to stolen session keys.