Homework #4

UC Davis Students: Due June 6, 1997 at 5:00PM; ***absolutely no extensions will be given due to the end of the term***

NTU Students: Due June 13, 1997 at 5:00PM

1. (*40 points*) (text, problem 13.8) Compare the Clark-Wilson model rules to typical software engineering approaches for protecting abstract data types from program routines.
2. (*20 points*) (text, problem 16.6) Identify any potential single points of failure in the auditing scheme depicted in Figure 16.4 of the text.
3. (*20 points*) (text, problem 27.2, modified) Some computer security experts claim that cryptography is all that is necessary to provide network security. Explain why this is false; in particular, explain why encryption protocols do not provide adequate protection in the absence of trusted hosts.
4. (*80 points*) Suppose someone wrote a file system scanner that computed cryptographic checksums of files, and compared them to a master list, reporting differences. The first program scans the files, computes the checksums, and transmits them to a second program, which compares the newly-computed checksums to the master list and reports differences. What considerations would the author need to take into account to make this security tool as useful as possible? Discuss attacks and countermeasures. Note that the tool can be used either on a single system or over a network (where the server is the second program and the client, which resides on the system being checked, is the first program).