Homework 2

Due Date: February 18, 2009 **Points:** 100

Questions

1. (*25 points*) Consider the construction in Section 3.5.2 that shows how to simulate three-parent joint creation using two-parent joint creation (this is on pp. 80–83 of the text). In the original paper, $cr_C(s,c) = c/R_3$ (that is, the t right was omitted) and $link_2(\mathbf{S},\mathbf{A}_3) = \mathbf{A}_3/t \in dom(\mathbf{S})$ (the second part was omitted). Why won't this work? (*text*, problem 3.9, modified)

2. (*10 points*) A cryptographer once claimed that security mechanisms other than cryptography were unnecessary because cryptography could provide any desired level of confidentiality and integrity. Ignoring availability, either justify or refute the cryptographer's claim. (*text*, problem 4.4)

3. (*25 points*) Prove Theorem 4–1. Show all elements of your proof. (*text*, problem 4.10)

4. (*25 points*) Prove Theorem 5–11. (*text*, problem 5.11, modified)

5. (*15 points*) In the Clark-Wilson model, must the TPs be executed serially, or can they be executed in parallel? If the former, why; if the latter, what constraints (if any) must be placed on their execution? (*text*, problem 6.8. modified)

Extra Credit

1. (*30 points*) One version of Polks implementation of Clark-Wilson on UNIX systems requires transaction procedures to distinguish users in order to determine which CDIs the user may manipulate. This exercise asks you to explore the implementation issues in some detail.
   (a) Polk suggests using multiple copies of a single TP. Show, with examples, *exactly* how to set this up.
   (b) Polk suggests that wrappers (programs that perform checks and then invoke the appropriate TPs) could be used. Discuss, with examples, *exactly* how to set this up. In particular, what checks would the wrapper need to perform?
   (c) An alternative implementation would be to combine the TPs and wrappers into a single program. This new program would be a version of the TP that would perform the checks and then transform the CDIs. How dificult would such a combination be to implement? What would be its advantages and disadvantages compared with multiple copies of a single TP? Compared with the use of wrappers?

   (*text*, problem 6.12)