Homework Assignment 3.

Due: September 29, 2004 at class.

Problem 1:

Show that $n > 2t$ processes upto t of which can be faulty, are *necessary* and *sufficient* to solve Consensus in the authenticated Byzantine failure model satisfying (in addition to non-uniform agreement and termination) the *strong* validity condition below:

Strong Validity: If all the correct processes start with the same initial value v, then v is the only possible decision value.

Problem 2:

Use the consistent broadcast primitive to design a binary (i.e., having the value domain of $\{0, 1\}$) consensus algorithm tolerating $t < n/3$ Byzantine failures and satisfying the strong validity property above.