Name:

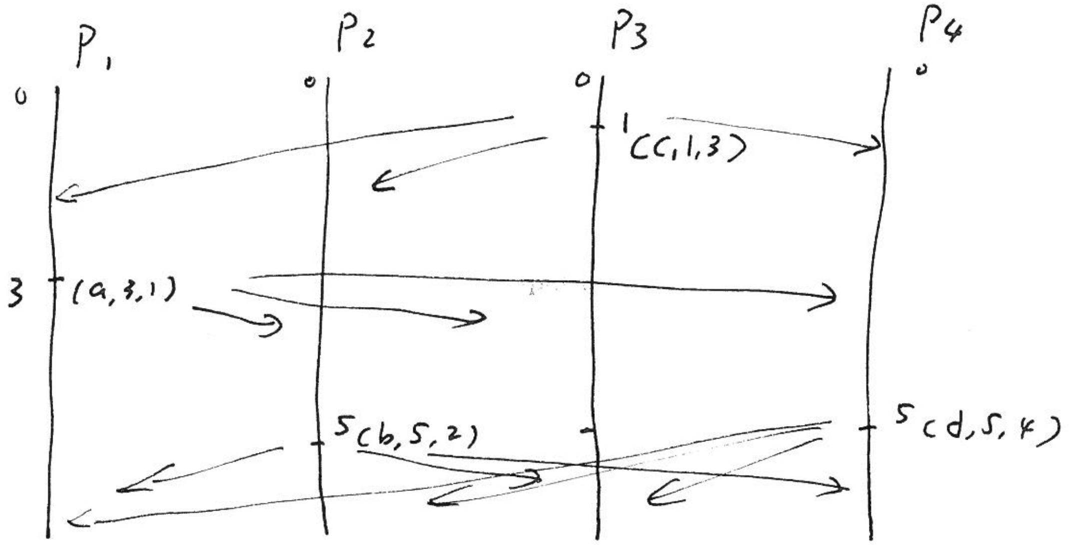
CSCI 460 Operating Systems

Participation Test 6

Instructions: Write your name above. Relax and attempt the problems below. This is NOT a quiz and participation credit will be given for any sincere attempt. (Later, solutions will be posted on the course webpage.) Turn in the sheet at the end of the class to receive your participation credit.

---

(1) This question is on distributed mutual exclusion. Assume that we have a distributed system with four processors P_1, P_2, P_3 and P_4 and each will broadcast a message using Lamport's *timestamp* algorithm. Also assume that the messages sent by P_1, P_2, P_3, P_4 are a, b, c, d at time $3, 5, 1, 5$ respectively and initially we have $C_i = 0$ for all i. Run the timestamp algorithm. What is the eventual ordering of the four messages?



Final ordering: c, a, b, d (b. d have the same timestamp and the tie is broken by their IDS).

(2) This question is on RSA public key cryptography. If $p = 7, q = 17$, $n = pq = 119$ and we choose $e = 5$. What is the public key? What is the private key?

$n = p \times q = 7 \times 17 = 119$

$e = 5$

$e * d = 1 \ \underline{\text{mod}} \ (p-1) * (q-1)$

$5 * d = 1 \ \underline{\text{mod}} \ 96$

$\quad = 1 + k * 96$, for some k

$\Rightarrow d = 77 \quad (\because 5 * 77 = 1 \ \underline{\text{mod}} \ 96 = 1 + 4 * 96)$

public key : $(5, 119)$

private key : $(77, 119)$