ECE 151 HW6 - Solutions

1. (a) Yes it satisfies FIFO multicast. P1 sends m1 followed by m3 and P2 sends m2 followed by m4. They are received in the same order by P3 and P4, i.e., m3 after m1 and m4 after m2.

(b) No because all processes have to receive the messages in the same order. P1, P2 and P4 receive m1-m2-m3-m4 while P3 received m1-m2-m4-m3.

2. Figures for :
   1. A detects D has failed and sends a view change message.
   2. B sends unstable messages followed by a flush message to A & C.
   3. B installs the new view when it receives a flush message from all other processes.
   4. Repeat 2 and 3 for A,C.

3. C12-C22-C32 and C14-C24-C34

4. e=29, d=5

Symbol	Number	p^e mod n	c^d mod n	Symbol
A	1	1	1	A
B	2	32	2	B
C	3	48	3	C

5. (a) Without the nonce, the message 3 in Needham-Schroeder Protocol can be replayed by Chuck to set up a channel with Bob. Thus, using the nonce, we relate message 1 to 3 so that Bob can be sure that he is talking to Alice.

(b) The KDC puts B into its reply message so that Alice, on decrypting the message from KDC using the key $K_{A,KDC}$, knows that the ticket should be used for setting up the communication with Bob.

It puts A into the ticket so that Bob, on decrypting the ticket with the key $K_{B,KDC}$, knows that the message was from Alice.

(c) Yes it is necessary to encrypt the message with the key so that only Alice can set up the communication with Bob. Without encryption, anyone who has this message from KDC can set up the channel pretending to be Alice.