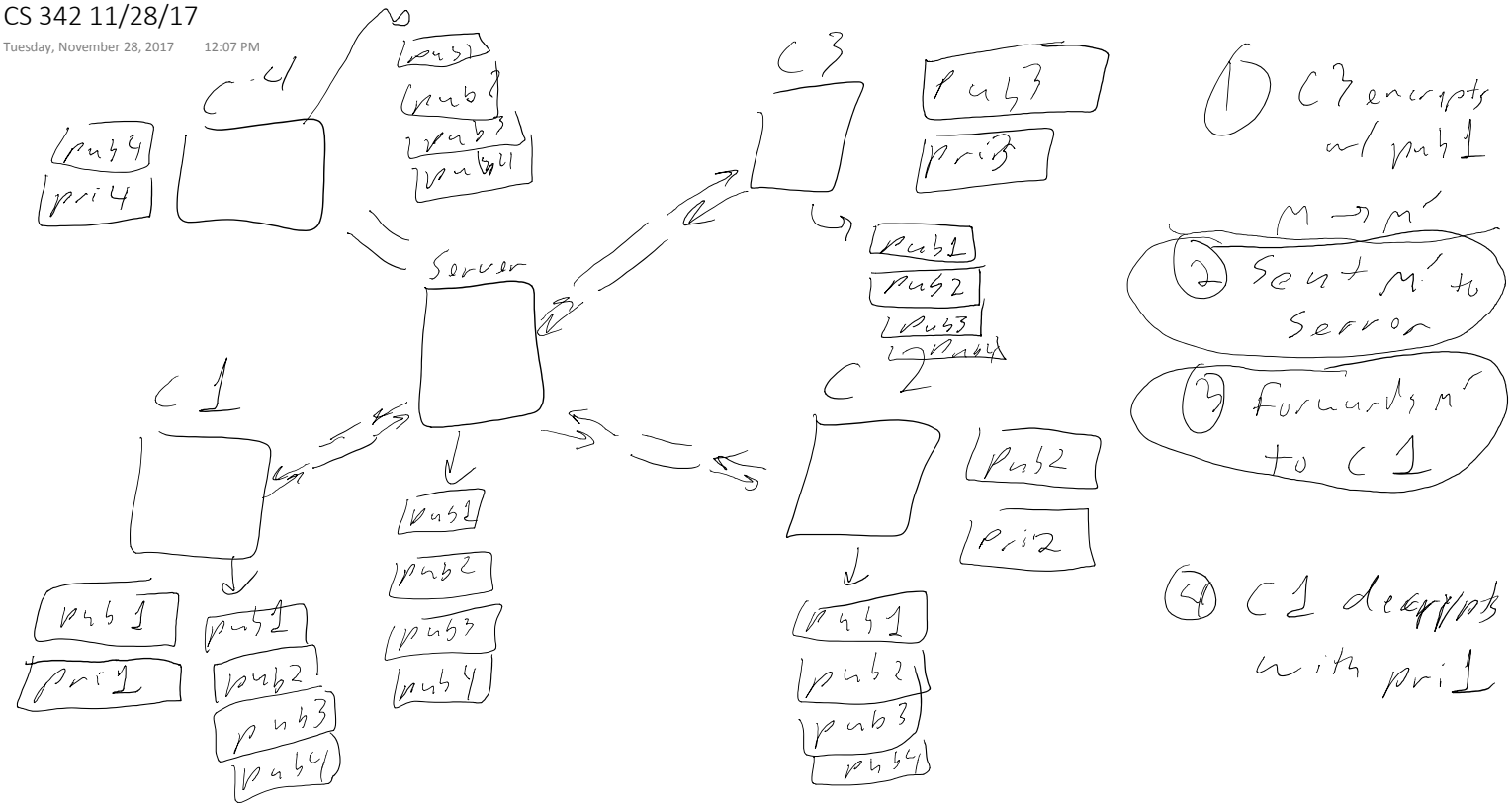
CS 342 11/28/17

Tuesday, November 28, 2017 12:07 PM



If bored over break add the following to stop message spoofing

Message from C3 to C1

C3a $M \rightarrow M'$ w/ pub1

C3b $M' \rightarrow M''$ w/ pri3

— send —

→ C1a $M'' \rightarrow M'$ w/ pub3

C1b $M' \rightarrow M$ w/ pri1

must have the same M value