



- ① C3 encrypts w/ pub1
- ② Sent  $M'$  to Server
- ③ forwards  $M'$  to C1
- ④ C1 decrypts with pri1

If bored over break add the following to stop message spoofing  
 Message from C3 to C1

$$\begin{array}{l} \text{C3a } M \rightarrow M' \text{ w/ pub1} \\ \hline \text{C3b } M' \rightarrow M'' \text{ w/ pri3} \\ \text{send} \end{array}$$

$$\rightarrow \begin{array}{l} \text{C1a } M'' \rightarrow M' \text{ w/ pub3} \\ \hline \text{C1b } M' \rightarrow M \text{ w/ pri1} \end{array}$$

Must have the same  $n$  value