Are we secure yet?

Two major issues:

1. **Key distribution**
   If A1, A2 … A5 want to talk, then **n . (n-1) / 2** keys must be exchanged physically using a secure channel

2. Does not ensure **Perfect-Forward Secrecy**
   If somehow Mallory is able to compromise one of the participant at some point in time, she can decrypt all previous communications between Alice and Bob

Session Keys