Session Keys

Interactive Protocol

System Hypothesis

- Synchronous communication channel
- **Each participant has a public key pair and everybody knows everyone's public keys**
- Mallory can read, modify and forge message send over the network

Goals

- When two participant exchange a message, the system should protect the confidentiality, integrity **and perfect forward secrecy** of the messages