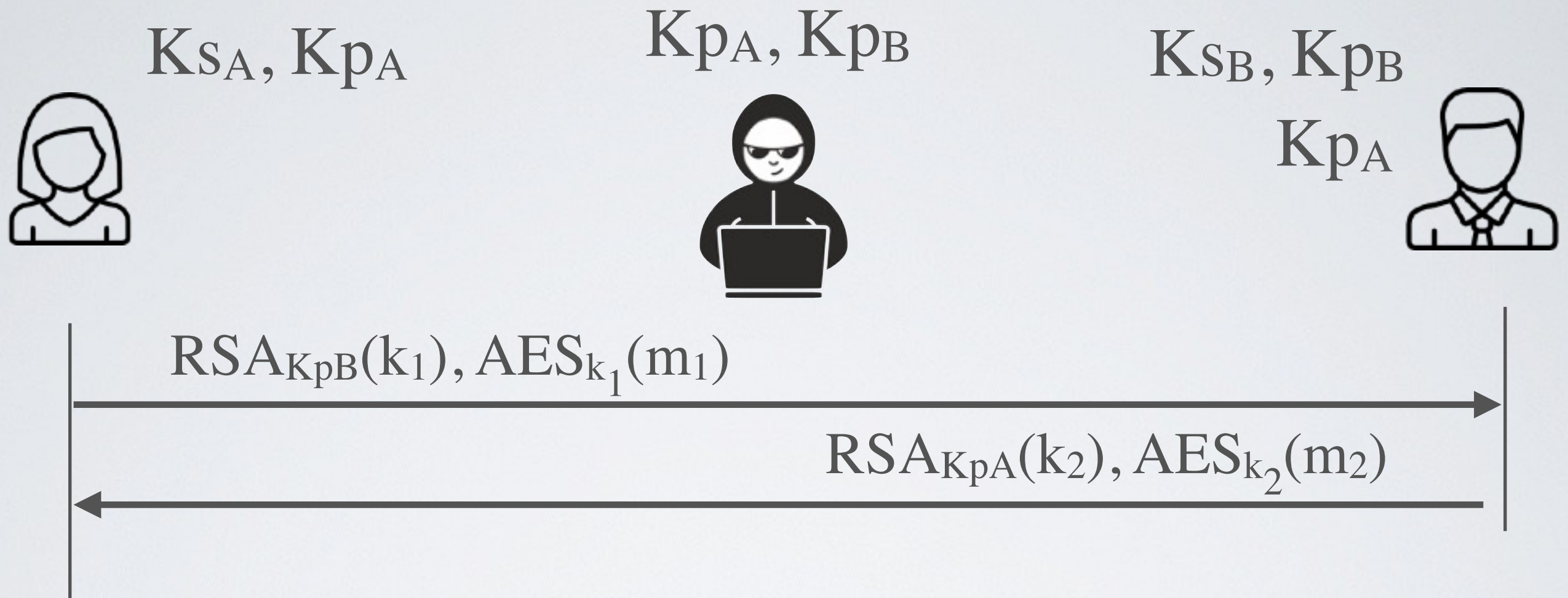


But not perfect yet



- ✓ Does ensure the confidentiality of the communication
- Does not authenticate Alice or Bob

# Asymmetric encryption for key exchange

Should we use asymmetric encryption for key exchange?

- ✓ Simple solution for non-interactive protocol (e.g GPG)
- But not a good solution for interactive protocols