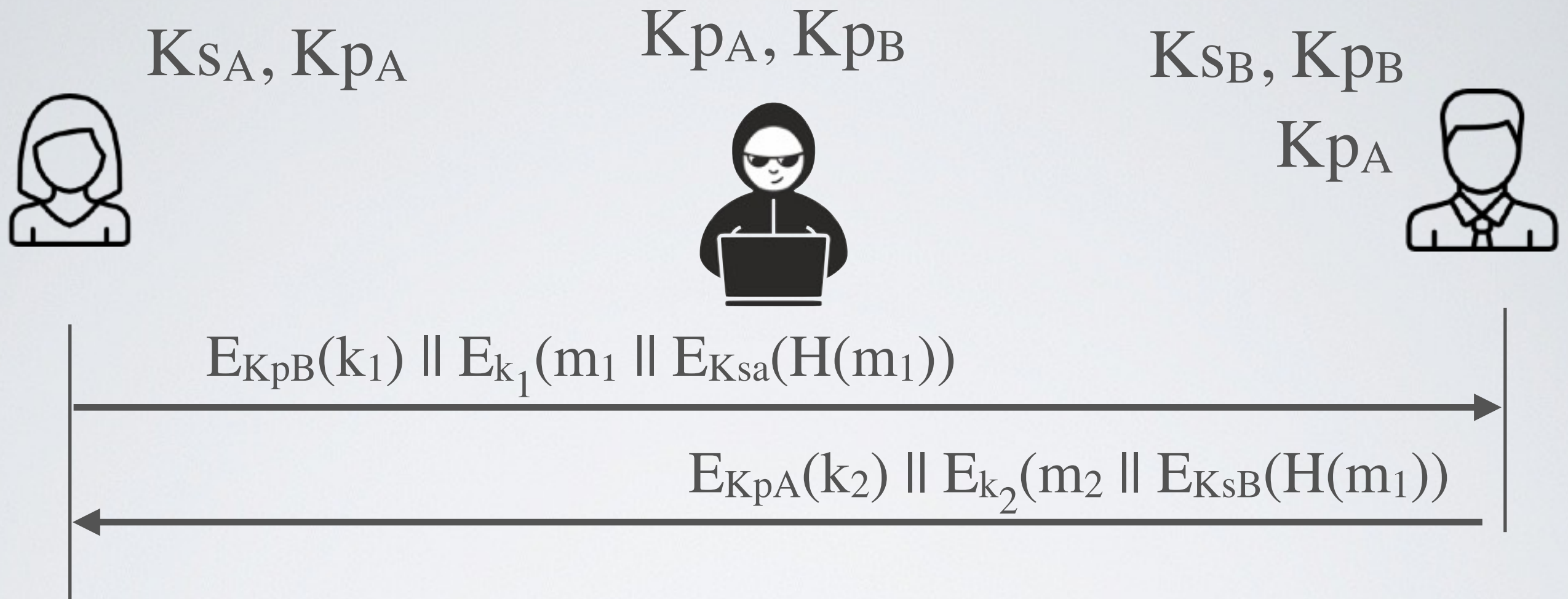


Asymmetric encryption for key exchange

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

Not a good solution for key exchange



- ✓ Does ensure the confidentiality of the communication
- ✓ Does authenticate Alice and Bob
- Does not prevent replay attacks
- Does not ensure Perfect Forward Secrecy
- Does not ensure the authenticity of the public keys