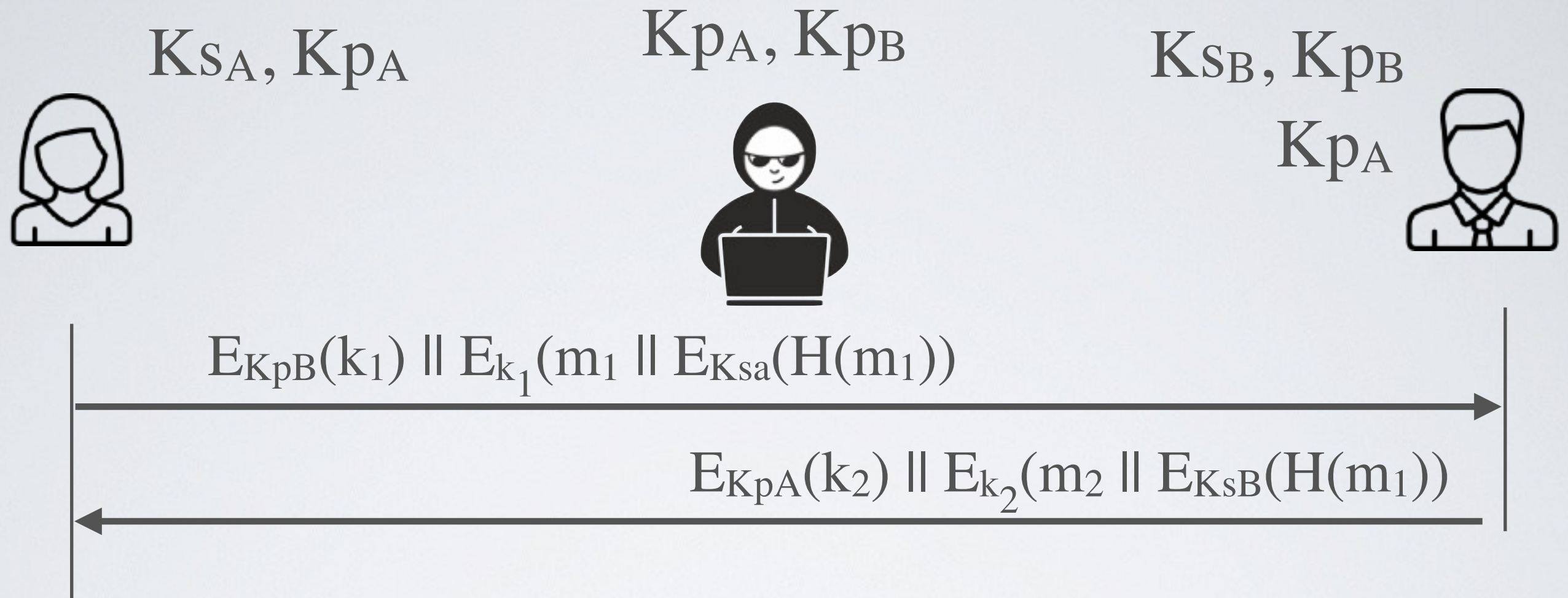


Not a good solution for key exchange



- ✓ 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

