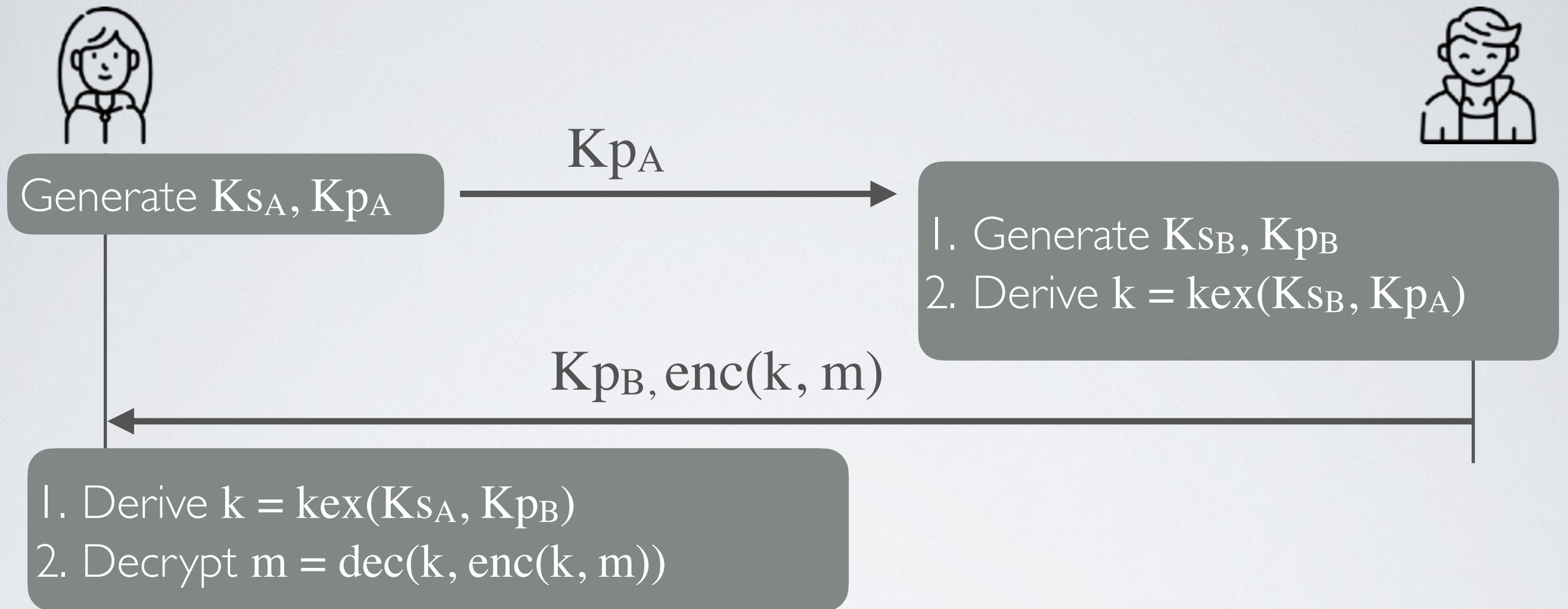


# ECDH Key exchange



**Diffie-Hellman-Merkle** provides a way to generate a shared key from two asymmetric key pairs

$$\text{kex}(K_{S_A}, K_{P_B}) = \text{kex}(K_{S_B}, K_{P_A}) = k$$

- ✓ Mutual contribution to the key generation
- ✓ No need to send the encrypted shared key

# A widely used key exchange protocol

ECDH is in many protocols

- SSH
- TLS (used by HTTPS)
- Signal (used by most messaging apps like Whatsapp)
- and so on ...

✓ It is fast and requires two exchanges only

- ⦿ But how to make sure Alice is talking to Bob and vice-versa?  
Diffie-Hellman-Merkle alone **does not ensure authentication**