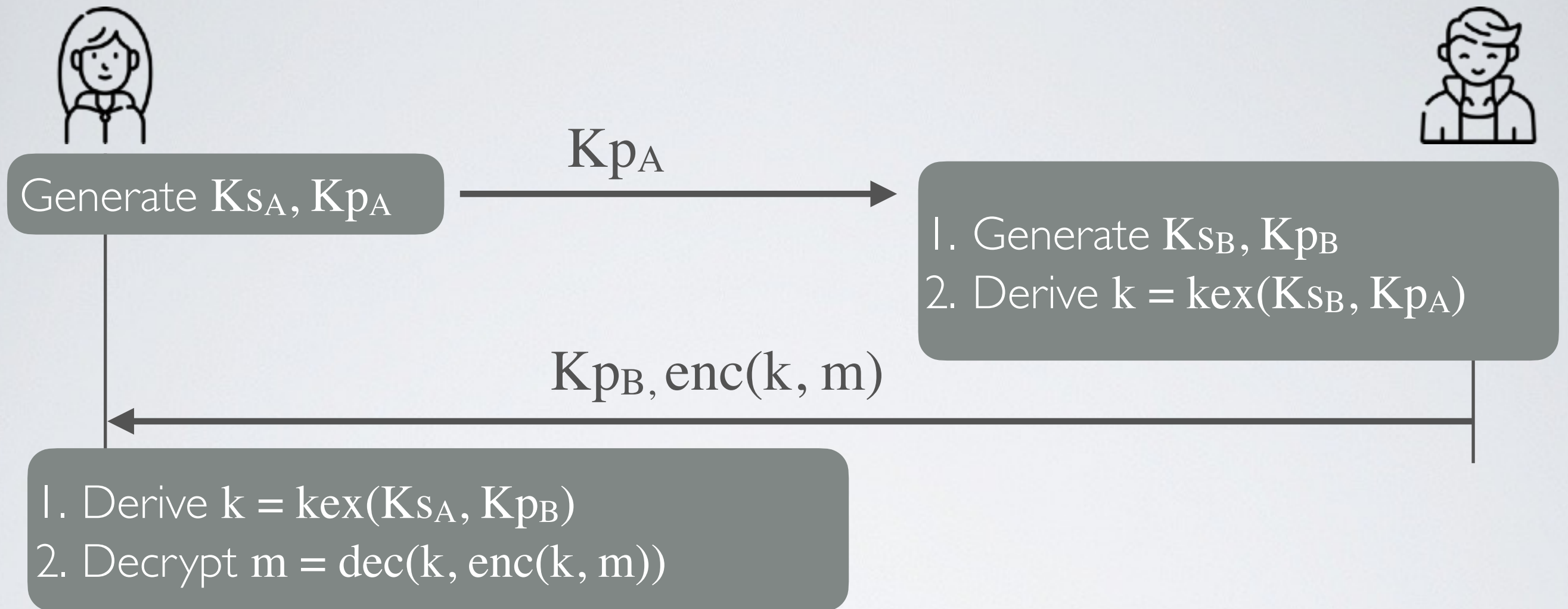


Elliptic Curve Diffie-Hellman-Merkle (ECDH)

- ➔ Generate a symmetric key k from two distinct asymmetric key pairs: K_{pA}, K_{sA} and K_{pB}, K_{sB}

$$k = \text{ECDH}(K_{sA}, K_{pB}) = \text{ECDH}(K_{sB}, K_{pA})$$

ECDH Key exchange



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

$$\text{kex}(K_{sA}, K_{pB}) = \text{kex}(K_{sB}, K_{pA}) = k$$

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