# Elliptic Curve Diffie-Hellman-Merkle (ECDH)
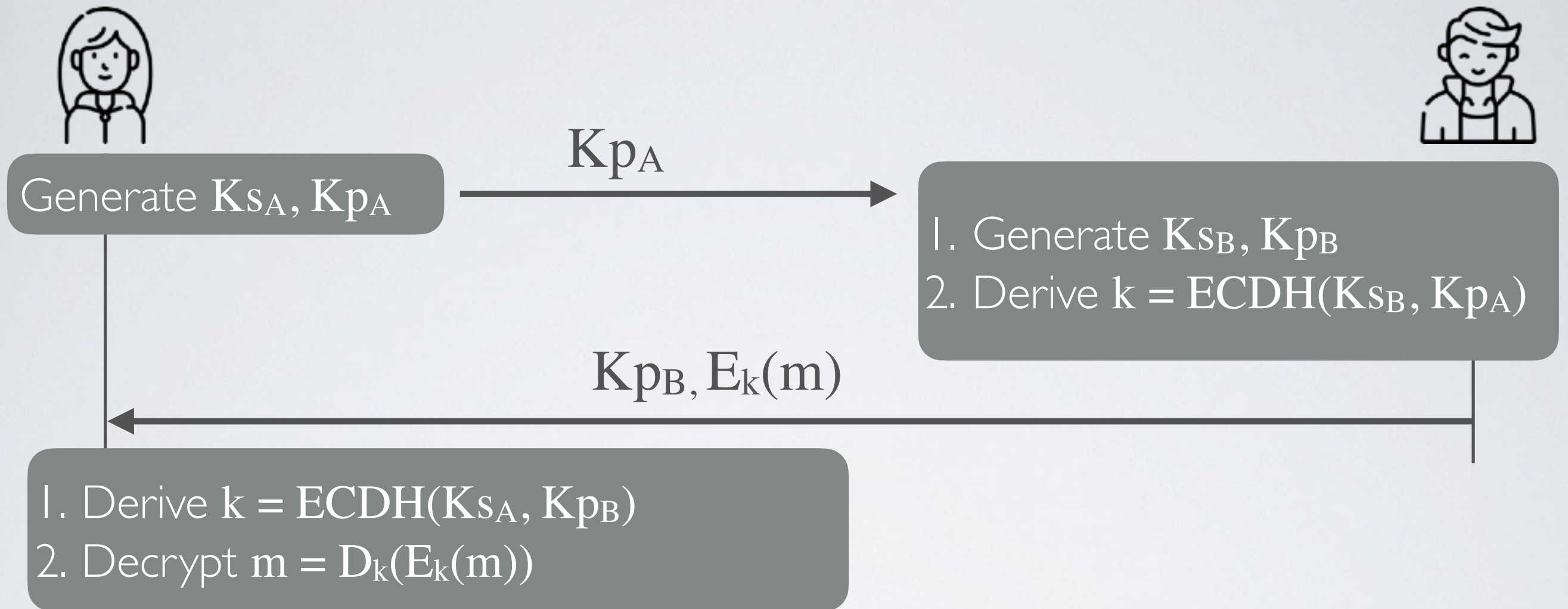
➡ Generate a symmetric key $k$ from two distinct asymmetric key pairs: $K_{pA}$, $K_{sA}$ and $K_{pB}$, $K_{sB}$

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

# ECDH Key exchange

Generate $Ks_A, Kp_A$

$Kp_A$ →

1. Generate $Ks_B, Kp_B$
2. Derive $k = ECDH(Ks_B, Kp_A)$

$Kp_B, E_k(m)$ ←

1. Derive $k = ECDH(Ks_A, Kp_B)$
2. Decrypt $m = D_k(E_k(m))$

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

$$ECDH(Ks_A, Kp_B) = ECDH(Ks_B, Kp_A) = k$$

✓ Mutual contribution to the key generation

✓ No need to send the encrypted shared key