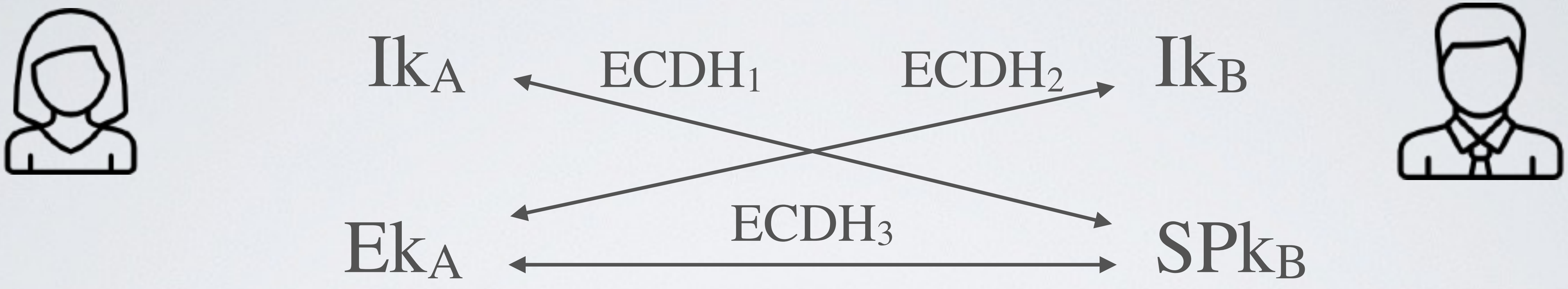
Triple Diffie-Hellman Key Exchange (3DH)



Ik_A ECDH$_1$ ECDH$_2$ Ik_B

Ek_A ECDH$_3$ SPk_B

ECDH(Ik_A, SPk_B)

ECDH(Ek_A, SPk_B)

$$k_{root} = \mathrm{HKDF}(\ \mathrm{ECDH}_1\ , \mathrm{ECDH}_2\ ,\ \mathrm{ECDH}_2\ )$$

ECDH(Ek_A, Ik_B)

Double Ratchet Protocol

- The root key k_{root} **does not encrypt messages**
- Use **for deriving a series of keys** k_1, k_2, k_3 ... that will be used to encrypt (send) and decrypt (receive) each message m_1, m_2, m_3

➡ **Double Ratchet Key Derivation Protocol**
(more details in bonus challenge)