Opening a channel between Alice and Bob

A, B,

Ik_B, SPk_{B1}

$Ek_A, E_{K1}(m_1)$

Ephemeral Key (public)

What's up?

$Ek_A, E_{K1}(m_1)$

$E_{K2}(m_2)$

$E_{K3}(m_3)$

What's up?

$E_{K2}(m_2), E_{K3}(m_3)$

$E_{K4}(m_4)$
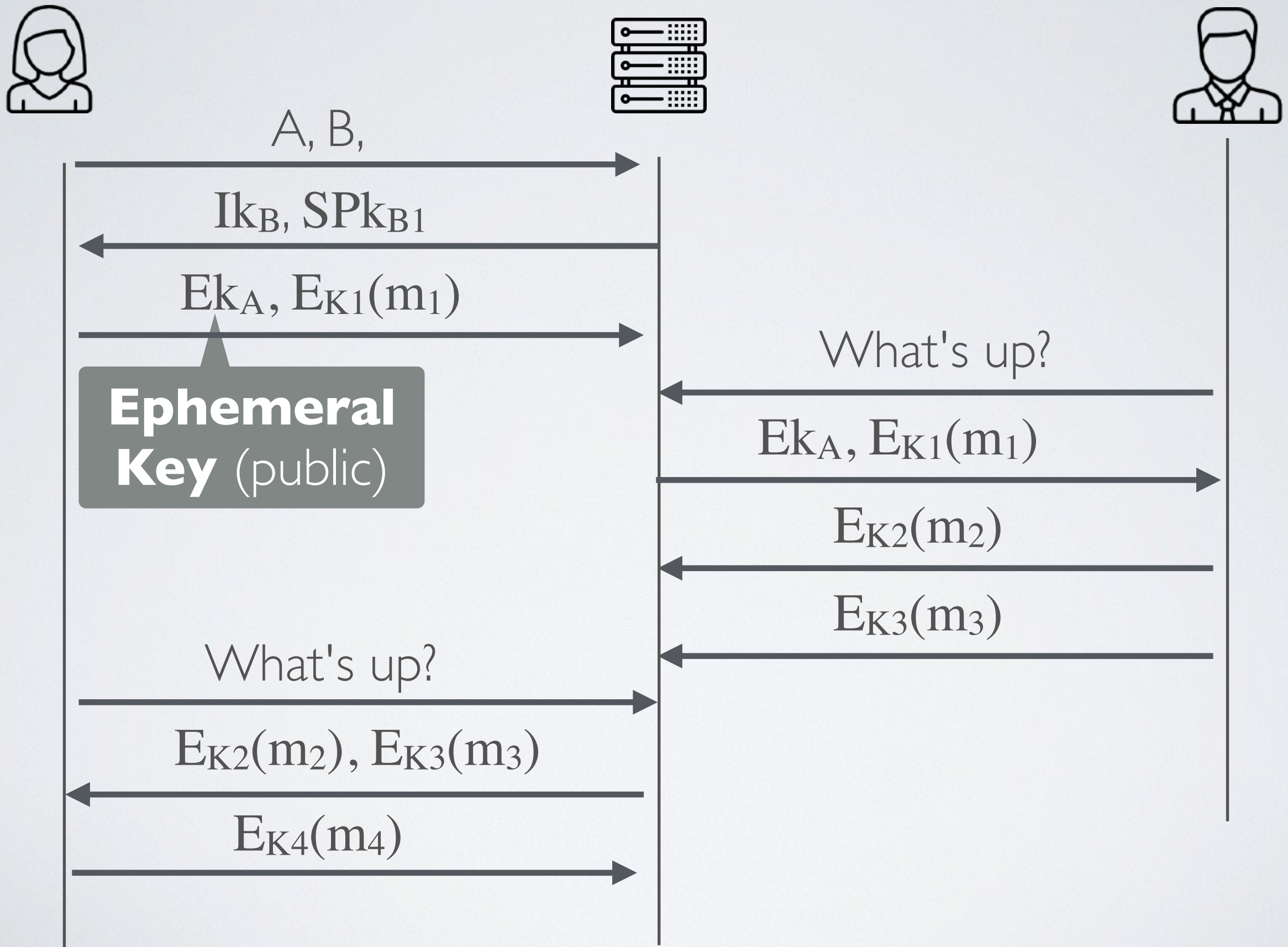
Triple Diffie-Hellman Key Exchange (3DH)

$$\text{Ik}_A \xleftarrow{\text{ECDH}_1} \quad \xrightarrow{\text{ECDH}_2} \text{Ik}_B$$

$$\text{Ek}_A \xleftrightarrow{\text{ECDH}_3} \text{SPk}_B$$

$\text{ECDH}(\text{Ik}_A, \text{SPk}_B)$

$\text{ECDH}(\text{Ek}_A, \text{SPk}_B)$

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

$\text{ECDH}(\text{Ek}_A, \text{Ik}_B)$