Not a good solution for key exchange

Ks_A, Kp_A

Kp_A, Kp_B

Ks_B, Kp_B
Kp_A

$E_{KpB}(k_1) \| E_{k_1}(m_1 \| E_{Ksa}(H(m_1)))$

$E_{KpA}(k_2) \| E_{k_2}(m_2 \| E_{KsB}(H(m_1)))$
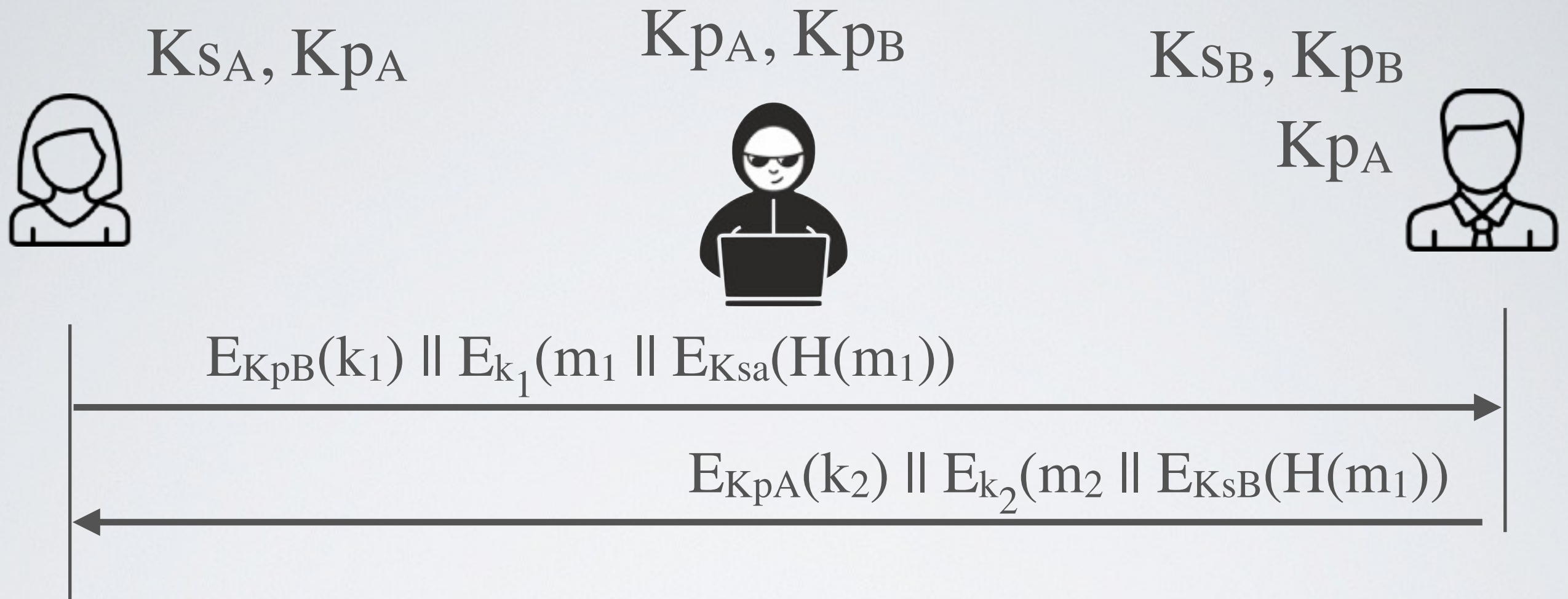
✓ Does ensure the confidentiality of the communication

✓ Does authenticate Alice and Bob

◉ Does not prevent replay attacks

◉ Does not ensure Perfect Forward Secrecy

◉ Does not ensure the authenticity of the public keys