# [broken] Key Derivation using Short-Term Keys

$pk_A$

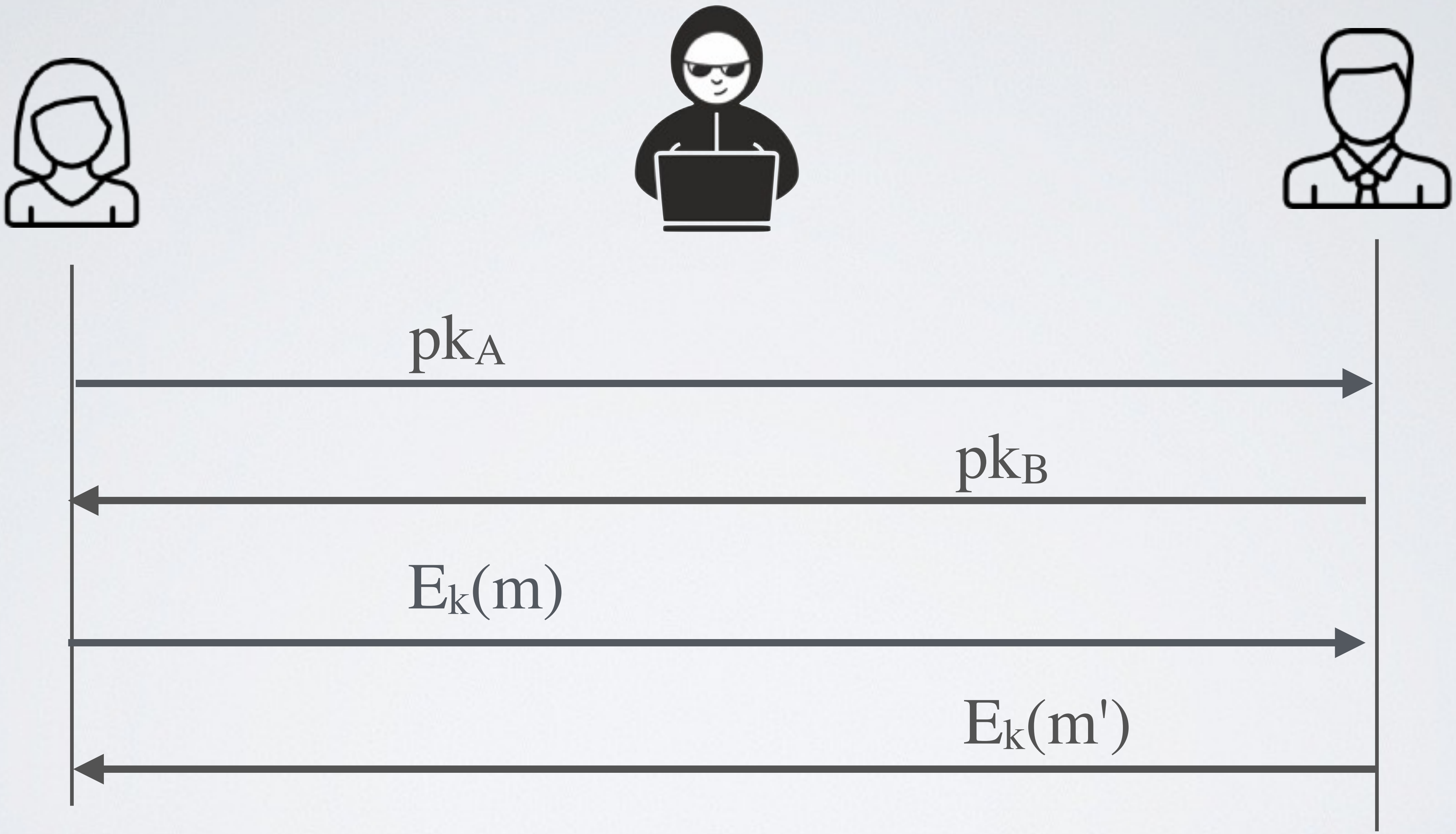
$E_k(m)$

$$\xleftarrow{\qquad\qquad\qquad\qquad\qquad E_k(m') \qquad\qquad}$$

$$\xleftarrow{\mathrm{pk}_B}$$

$$k = \mathrm{ECDH}(sk_A, pk_B) = \mathrm{ECDH}(sk_B, pk_A)$$

# [broken] Key Derivation using Short-Term Keys



$pk_A$

$pk_B$

$E_k(m)$

$E_k(m')$

$$k = ECDH(sk_A, pk_B) = ECDH(sk_B, pk_A)$$