[broken] Key Derivation using Long-Term Keys

N_A


$E_k(m)$

$E_k(m')$


N_B

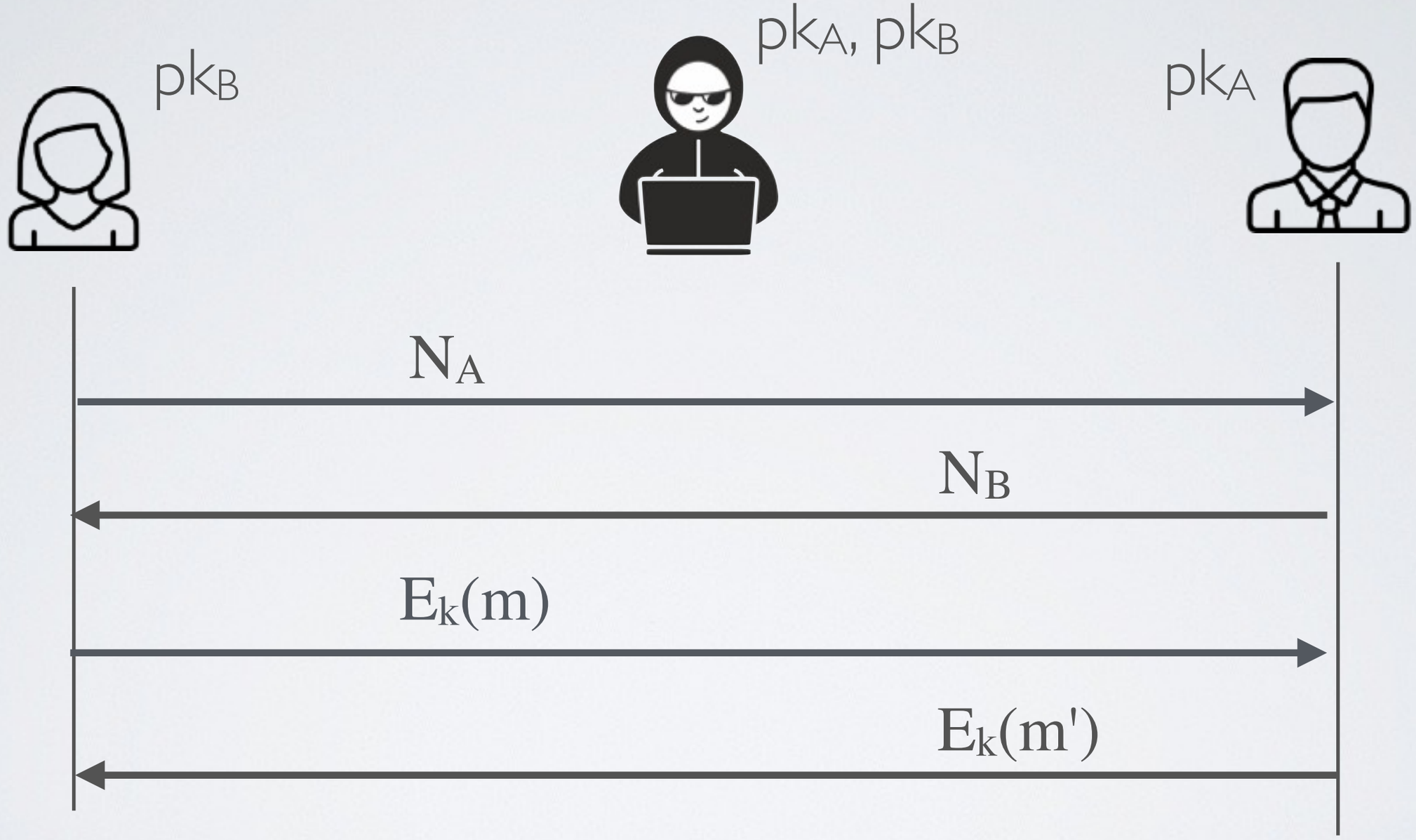

pkB


pKA

pK_A, pK_B

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

[broken] Key Derivation using Long-Term Keys



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

[broken] Key Derivation using Short-Term Keys

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