[broken] Key Derivation using Long-Term Keys

pk$_B$

pk$_A$, pk$_B$

pk$_A$

A, N_A

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

N_B

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

$E_k(m)$

$E_k(m')$
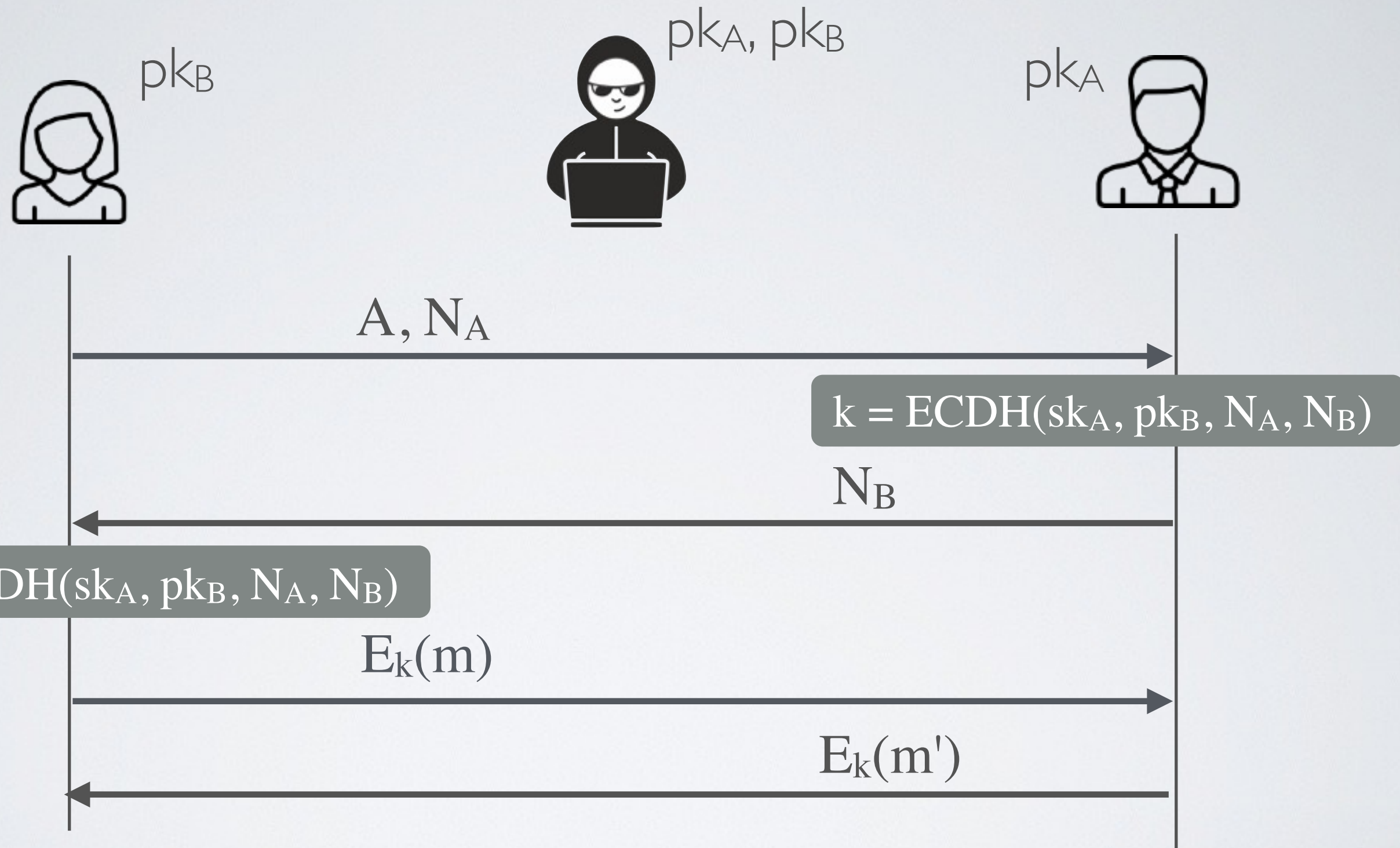
◉ No Forward Secrecy

[broken] Key Derivation using Short-Term Keys

$$pk_1$$

$$pk_2$$

$$E_k(m)$$

$$E_k(m')$$

$$k = ECDH(sk_1, pk_2) = ECDH(sk_2, pk_1)$$