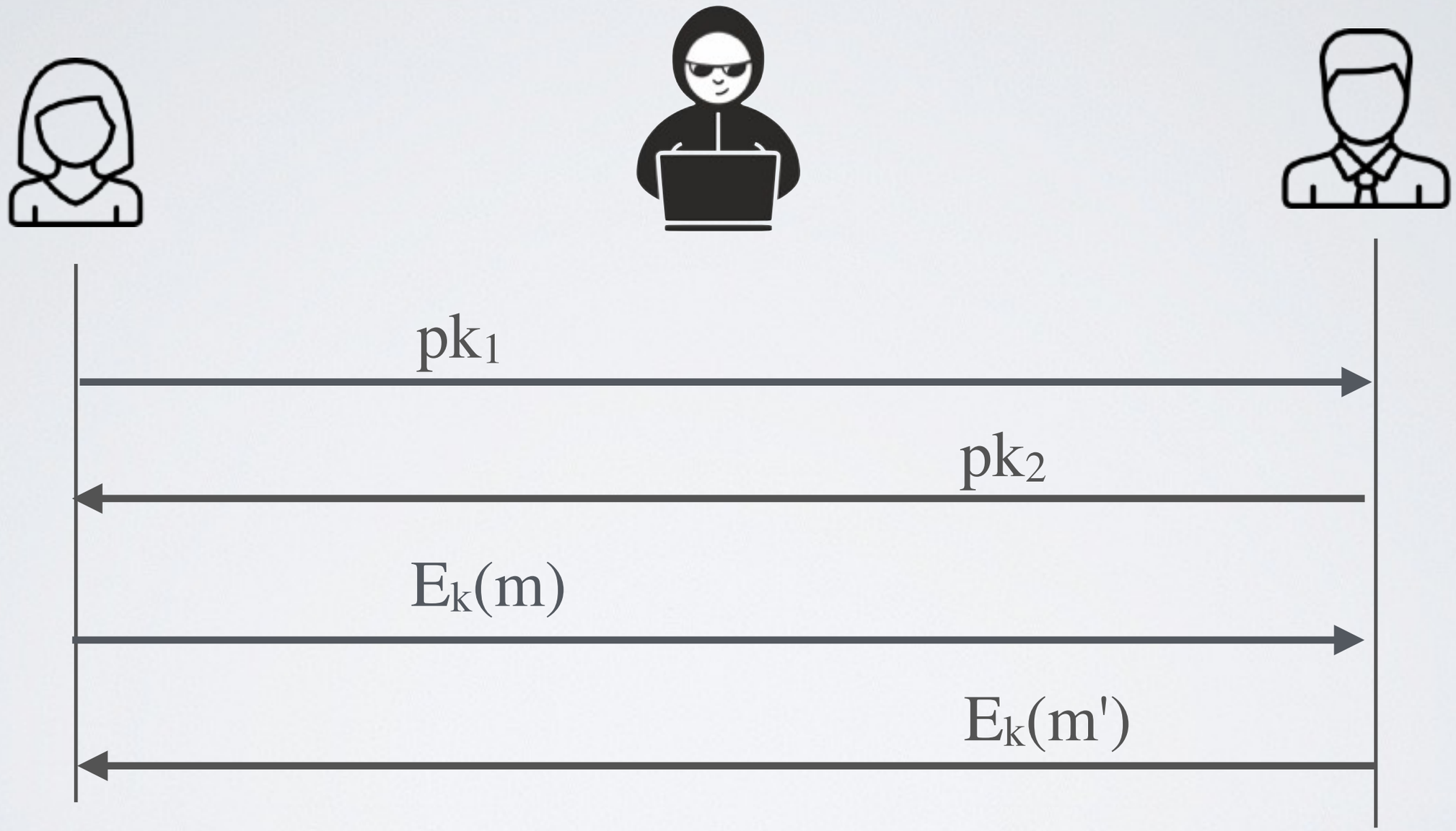
[broken] Key Derivation using Short-Term Keys



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

The key exchange is not authenticated