Key Exchange Protocols

Naive key exchange using asymmetric encryption

Generate Ks_A, Kp_A

Kp_A

Generate k

$E_{KpA}(k), E_k(m)$

1. Decrypt $k = D_{KsA}(E_{KpA}(k))$
2. Decrypt $m = D_k(E_k(m))$
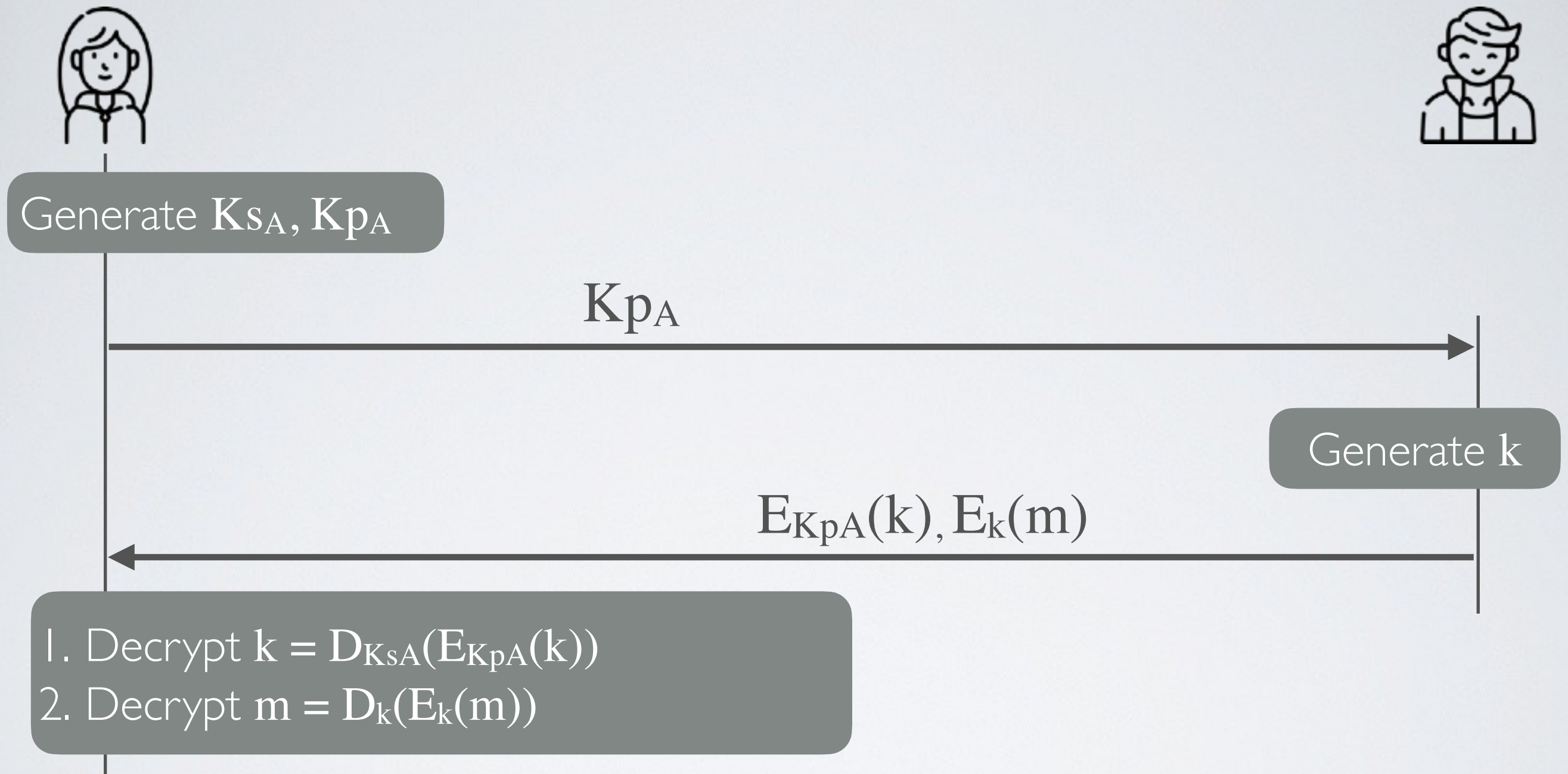
⊙ Protecting the shared key is the **responsibility of Alice only**

⊙ Generating the shared key is the **responsibility of Bob only**