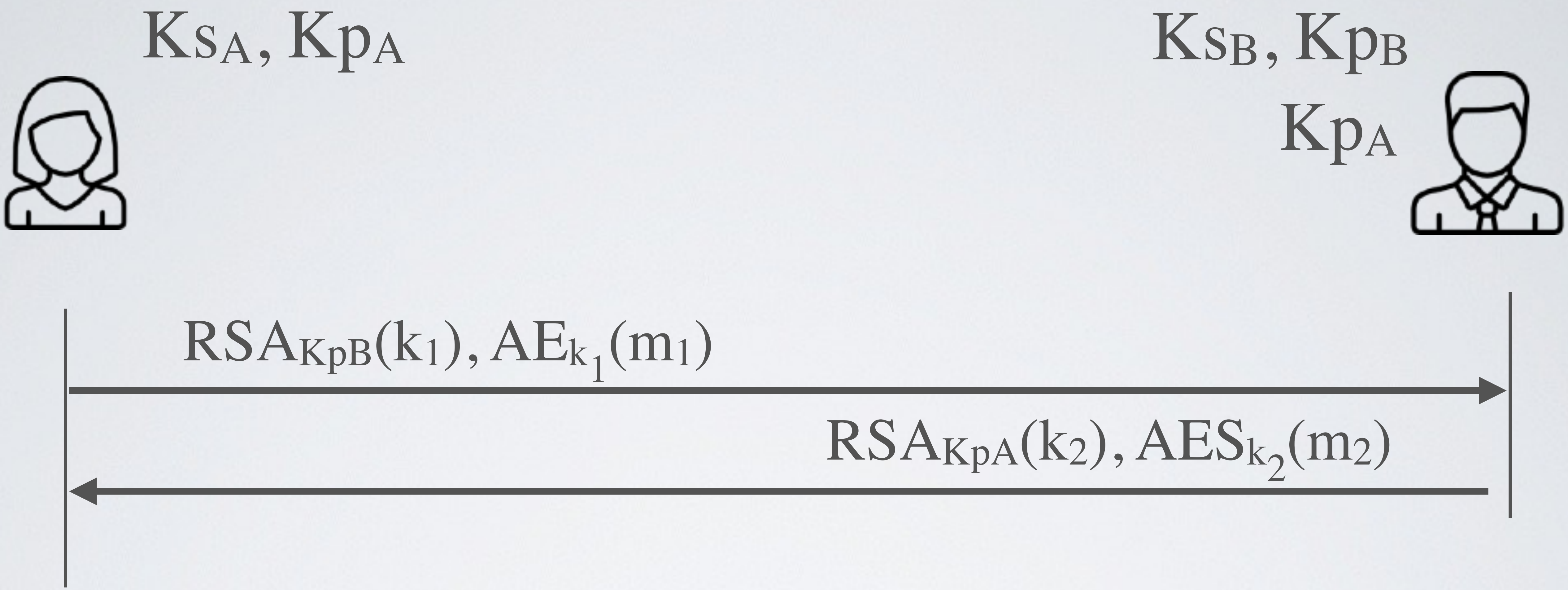
Limitations of using a key distribution centre

The key distribution server is a bootleneck and weak link

- The attacker could record the key exchange and the encrypted session, if one day either **Kas** or **Kbs** is broken, the attacker can decrypt the session

➡ Having a KDC does not ensure **Perfect Forward Secrecy**

Key exchange using asymmetric encryption



Ks_A, Kp_A

Ks_B, Kp_B

Kp_A

$RSA_{KpB}(k_1), AE_{k_1}(m_1)$

$RSA_{KpA}(k_2), AES_{k_2}(m_2)$

- The attacker could record the encrypted session, if one day either Ks_A or Ks_B is broken, the attacker can decrypt part of the session

➡ Using asymmetric encryption for key exchange does not ensure **Perfect Forward Secrecy**