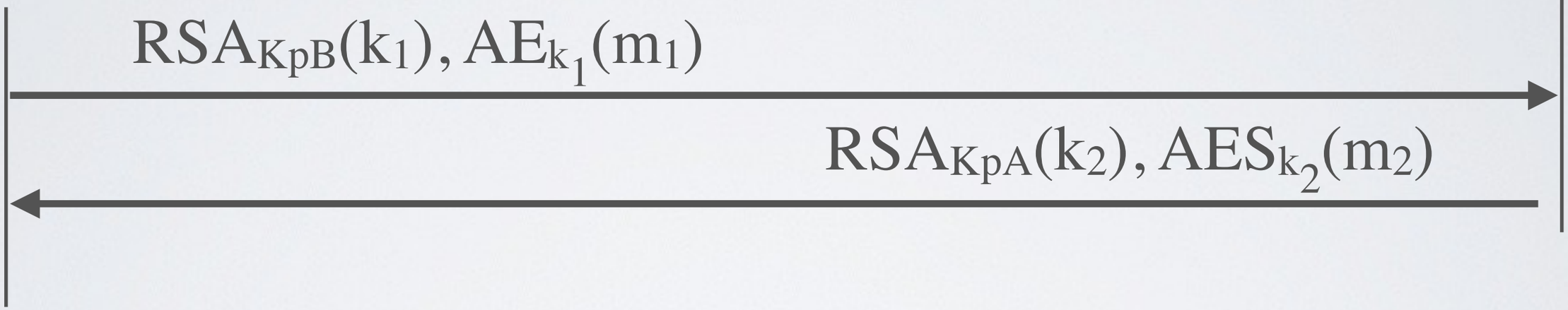
Key exchange using asymmetric encryption

Ks_A, Kp_A

Ks_B, Kp_B

Kp_A



- 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**

What is the solution?

Could Alice and Bob could magically come up with a key without exchanging it over the network?

➡ The magic is called **Diffie-Hellman-Merkle Protocol**