Asymmetric vs Symmetric

	Symmetric	Asymmetric
pro	Fast	No key agreement
cons	Key agreement	Very slow

The best of both worlds

- Use asymmetric encryption to encrypt a shared key (or hash)
- Use symmetric encryption to encrypt message

$$E_{Kp}(m) = RSA_{Kp}(k), AES_k(m)$$

Naive approach

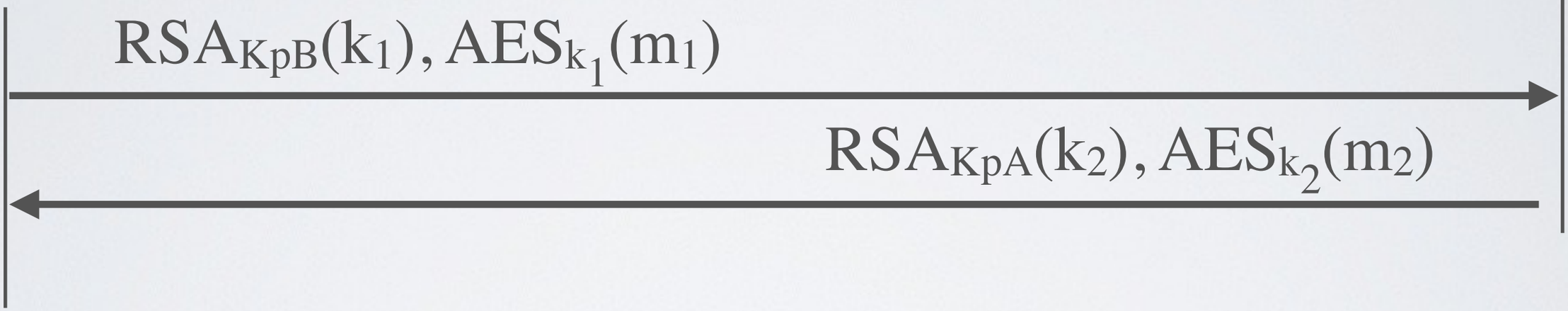
But not perfect yet

Ks_A, Kp_A

Kp_A, Kp_B

Ks_B, Kp_B

Kp_A



- ✓ Does ensure the confidentiality of the communication
- ◉ Does not authenticate Alice or Bob