Asymmetric vs Symmetric

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

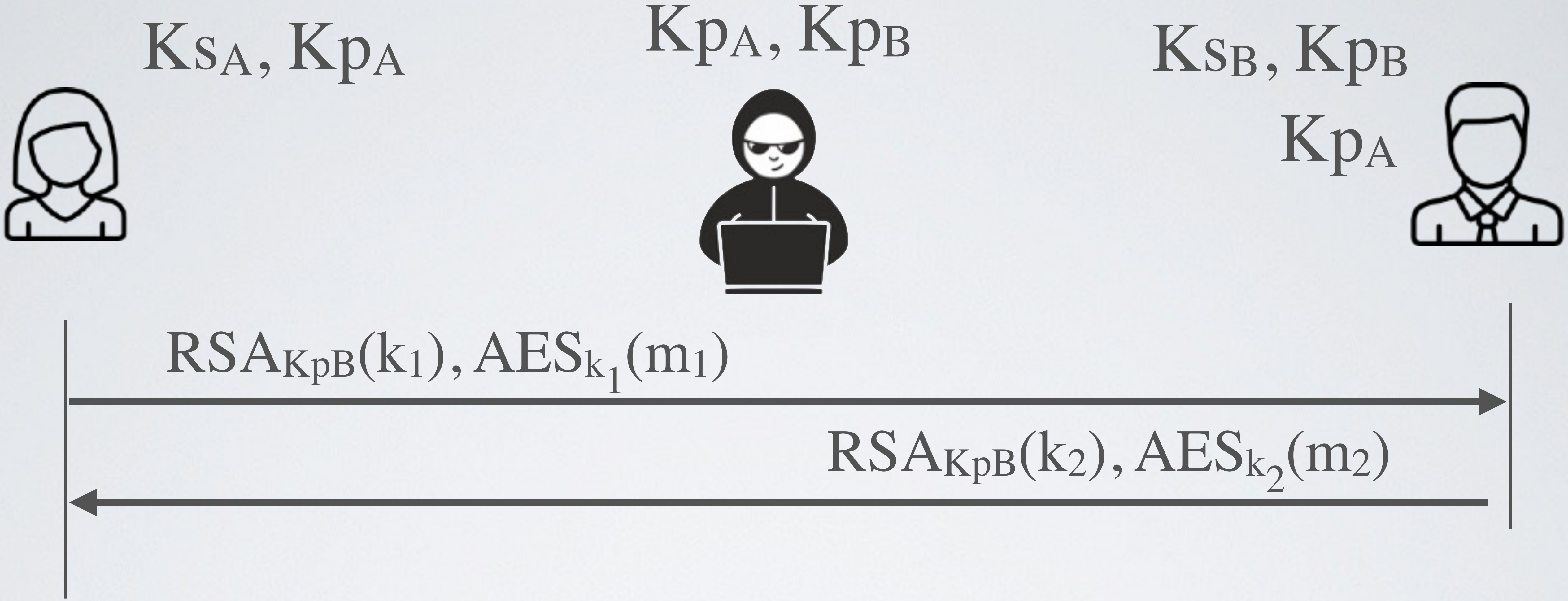
The best of both worlds

- Use RSA to encrypt a shared key
- Use AES 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

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

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

✓ Does ensure the confidentiality of the communication

◉ Does not authenticate Alice or Bob