

Asymmetric vs Symmetric

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

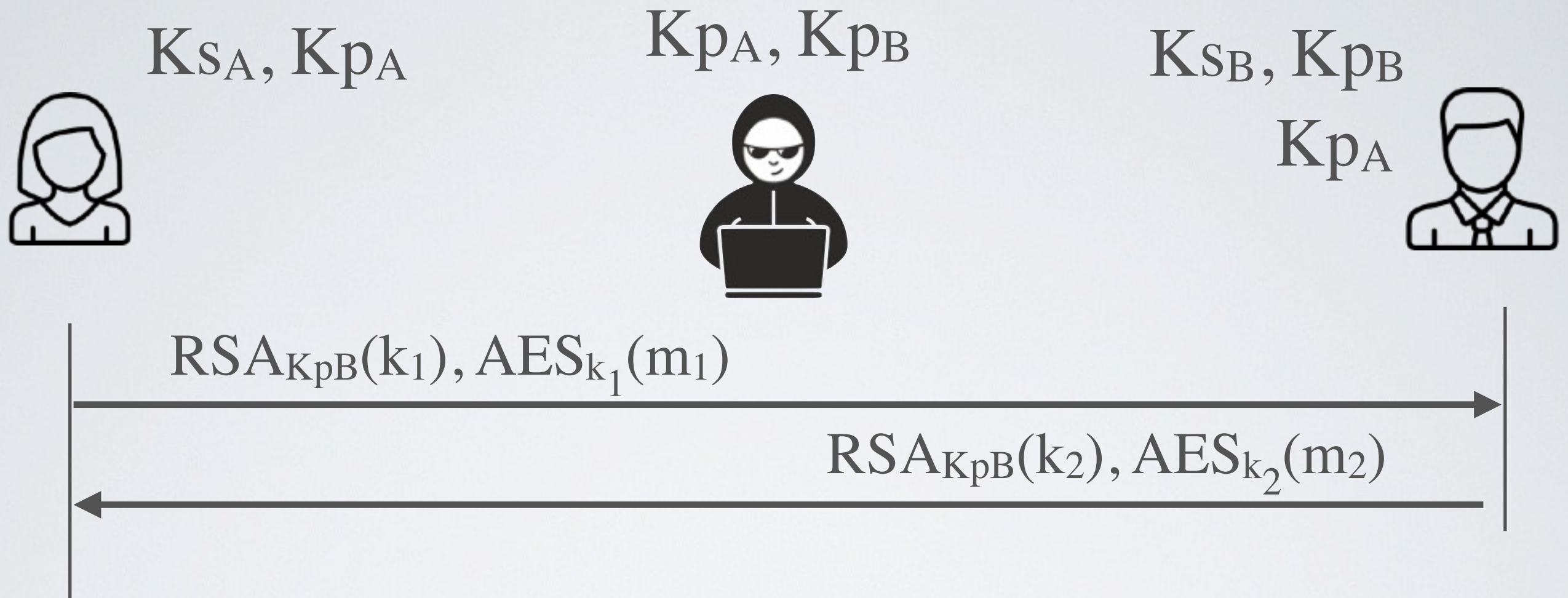
The best of both worlds

- ➡ Use RSA to encrypt a shared key
- ➡ Use AES to encrypt message

$$E_{K_p}(m) = \text{RSA}_{K_p}(k), \text{AES}_k(m)$$

Naive
approach

But not perfect yet



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