But not perfect yet

Ks_A, Kp_A

Kp_A, Kp_B

Ks_B, Kp_B
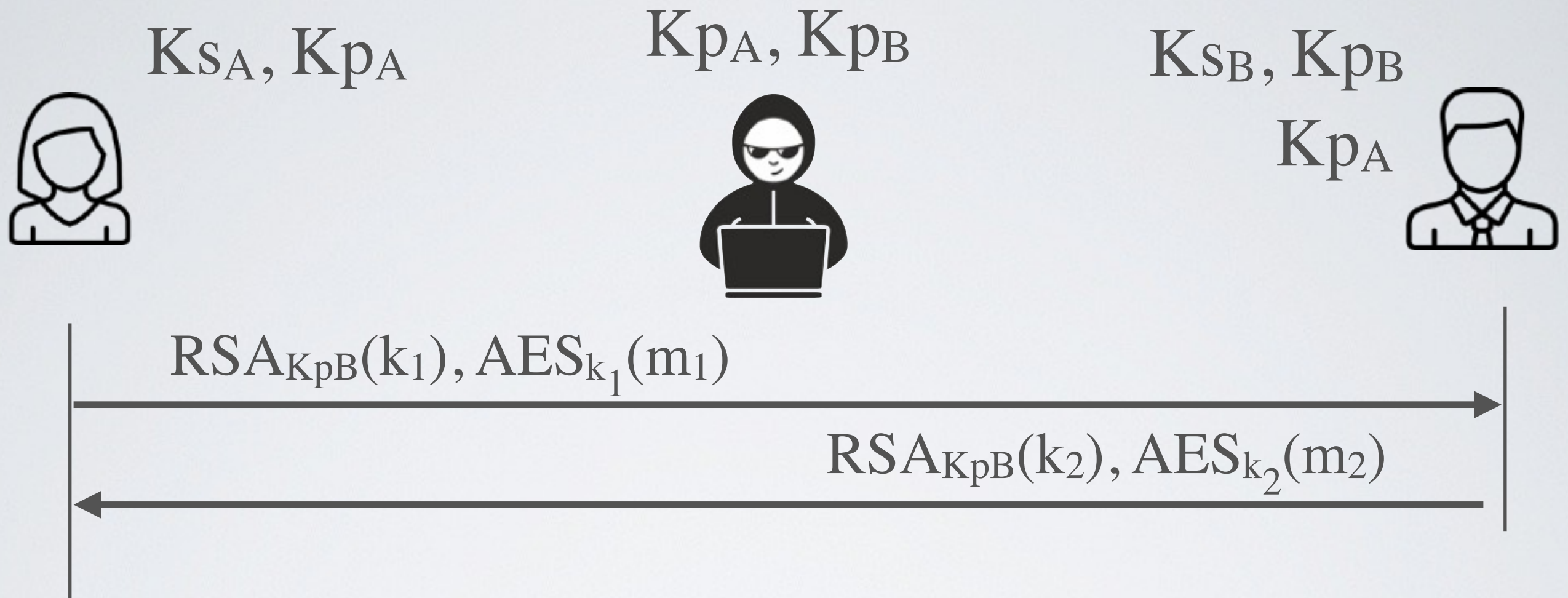
Kp_A

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

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

✓ Does ensure the confidentiality of the communication

◉ Does not authenticate Alice or Bob

Asymmetric encryption: Digital Signature

➡ The private key for encryption
➡ The public key for decryption

private key   public key