

# Asymmetric keys

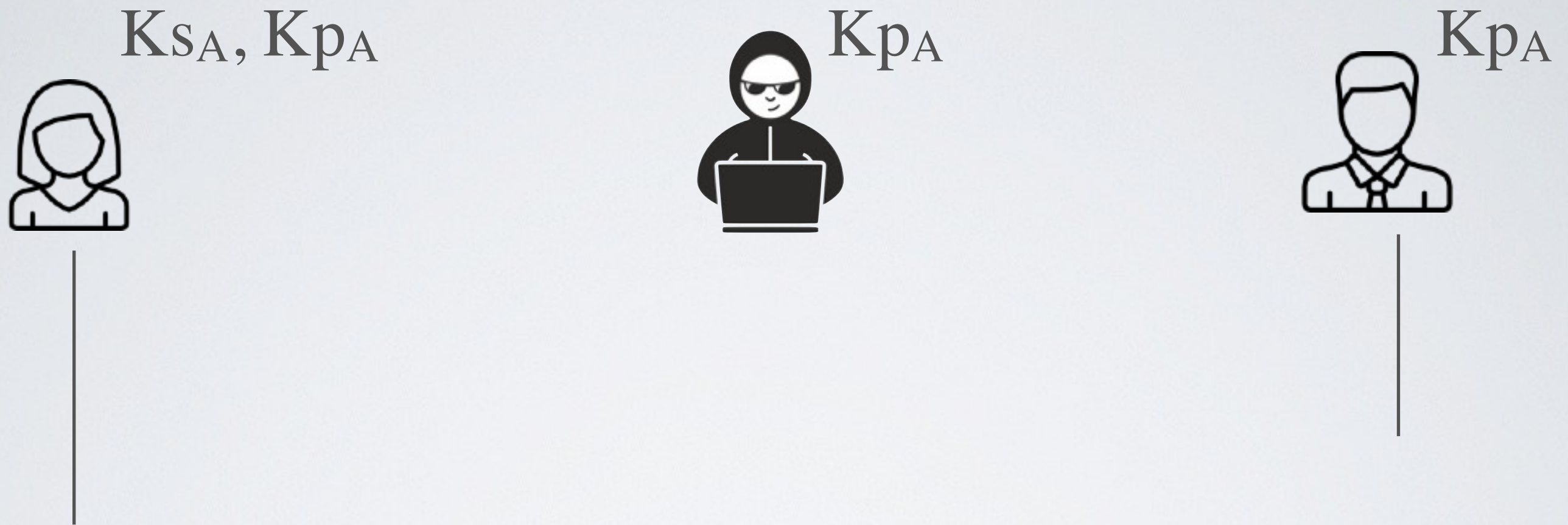


Alice generates a pair of asymmetric keys

- $K_{s_A}$  is the secret key that Alice keeps for herself
- $K_{p_A}$  is the public key that Alice gives to everyone (even Mallory)

➔ These two keys  $K_{s_A}$  and  $K_{p_A}$  work together

# Asymmetric encryption for **confidentiality**



Bob encrypts a message  $m$  with Alice's public key  $K_{p_A}$

➔ Nobody can decrypt  $m$ , except Alice with her private key  $K_{s_A}$

✓ Confidentiality without the need to exchange a secret key