# Asymmetric encryption for **confidentiality**

Bob encrypts a message $\mathbf{m}$ with Alice's public key $\mathbf{Kp_A}$

➡ <u>Nobody</u> can decrypt $\mathbf{m}$, except Alice with her private key $\mathbf{Ks_A}$

✓ Confidentiality without the need to exchange a secret key

$K_{SA}, K_{PA}$

$Kp_A$

$Kp_A$

$$E_{Kpa}(m) \longleftarrow$$

$$D_{Ksa}(E_{Kpa}(m)) = m$$

# Asymmetric encryption for **confidentiality**

$Ks_A, Kp_A$          $Kp_A$                    $Kp_A$

$E_{Kpa}(m)$

$D_{Ksa}(E_{Kpa}(m)) = m$

Bob encrypts a message $m$ with Alice's public key $Kp_A$

➡ <u>Nobody</u> can decrypt $m$, except Alice with her private key $Ks_A$

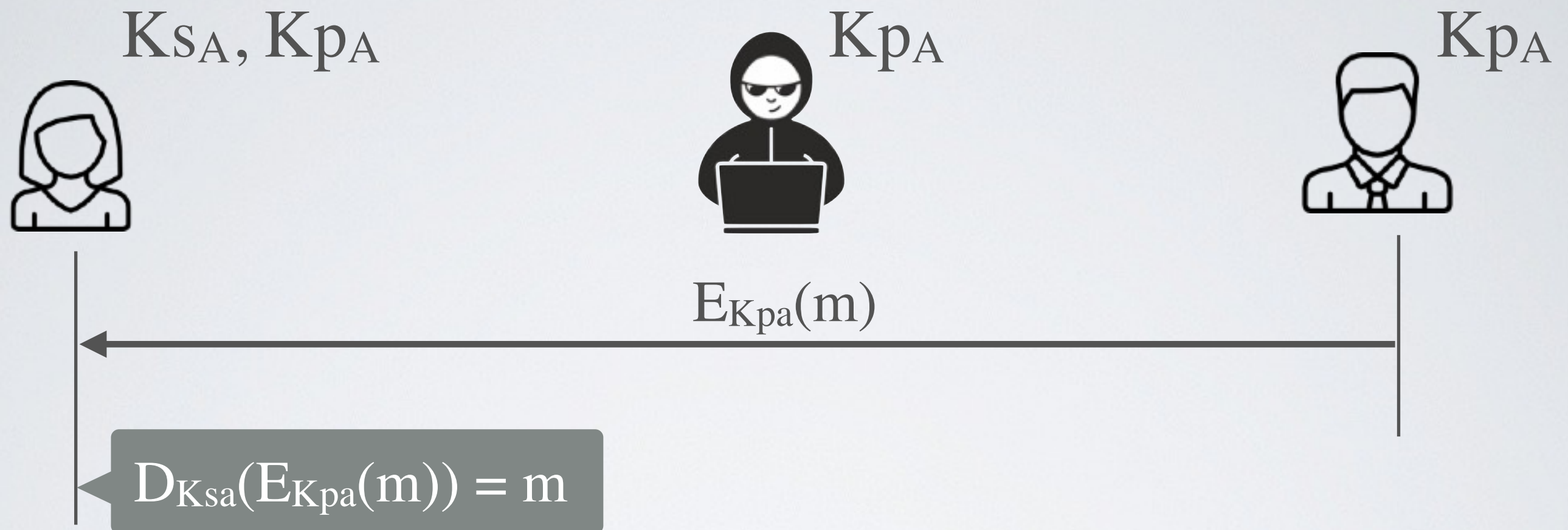✓ Confidentiality without the need to exchange a secret key