Asymmetric encryption for **confidentiality**

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

➡ Nobody 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}

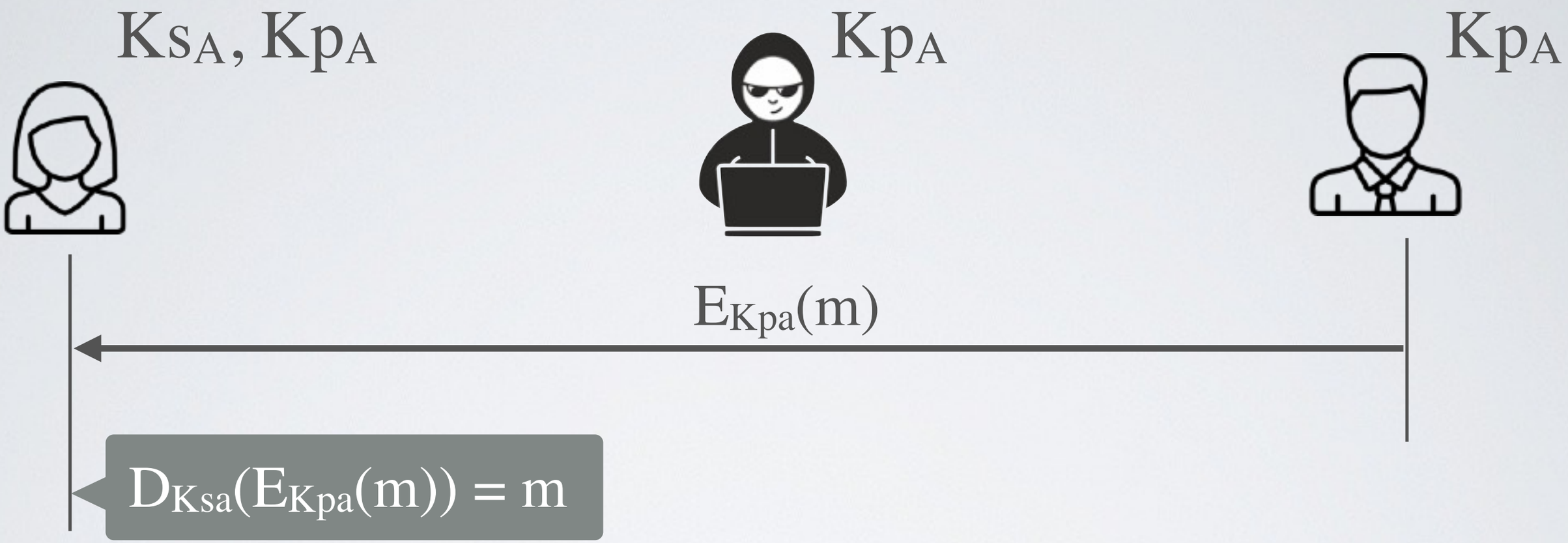

Кра


Кра


$E_{Kpa}(m)$

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

Asymmetric encryption for **confidentiality**



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

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

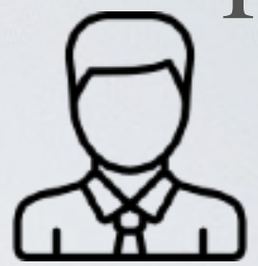
✓ Confidentiality without the need to exchange a secret key

Asymmetric encryption for **integrity**

Ks_A, Kp_A

Kp_A

Kp_A



Alice encrypts a message $\mathbf{m}$ with her private key $\mathbf{Ks_A}$

➡ Everybody can decrypt $\mathbf{m}$ using Alice's public key $\mathbf{Kp_A}$

✓ Authentication with non-repudiation (a.k.a Digital Signature)