Asymmetric encryption for **integrity**

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)

K_{sA}, K_{pA}

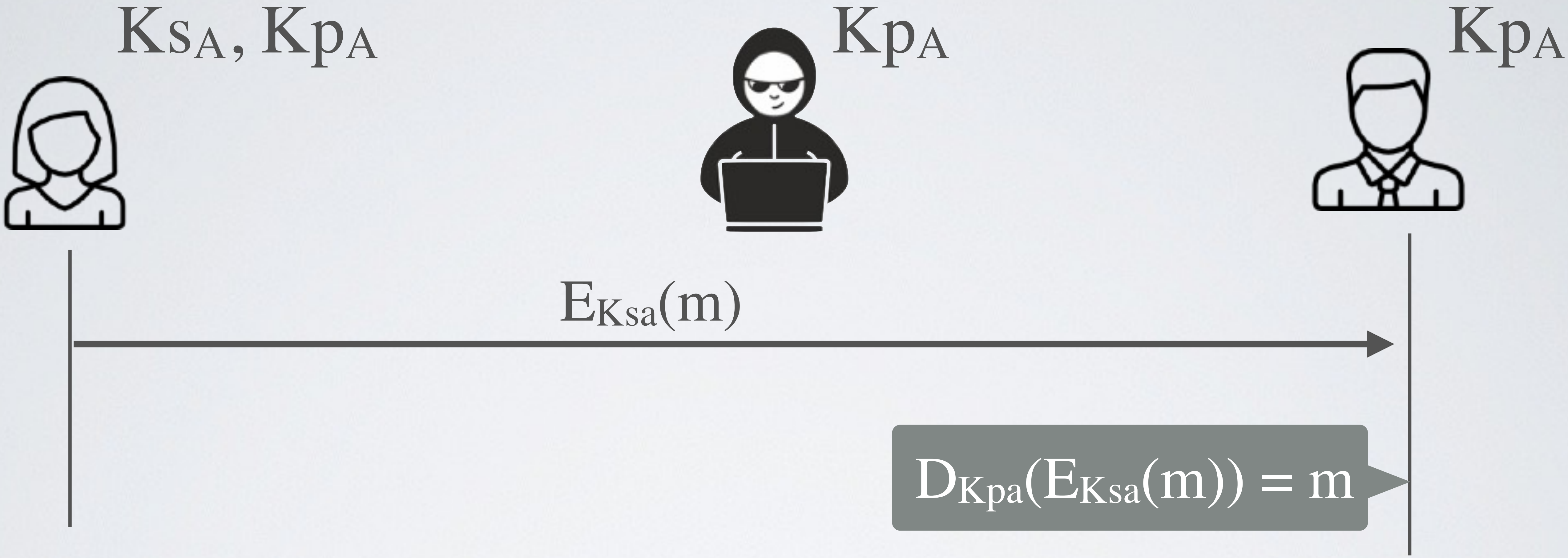
Kp_A

Kp_A

$$\xrightarrow{E_{Ksa}(m)}$$

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

Asymmetric encryption for **integrity**



Ks_A, Kp_A

Kp_A

Kp_A

$E_{Ksa}(m)$

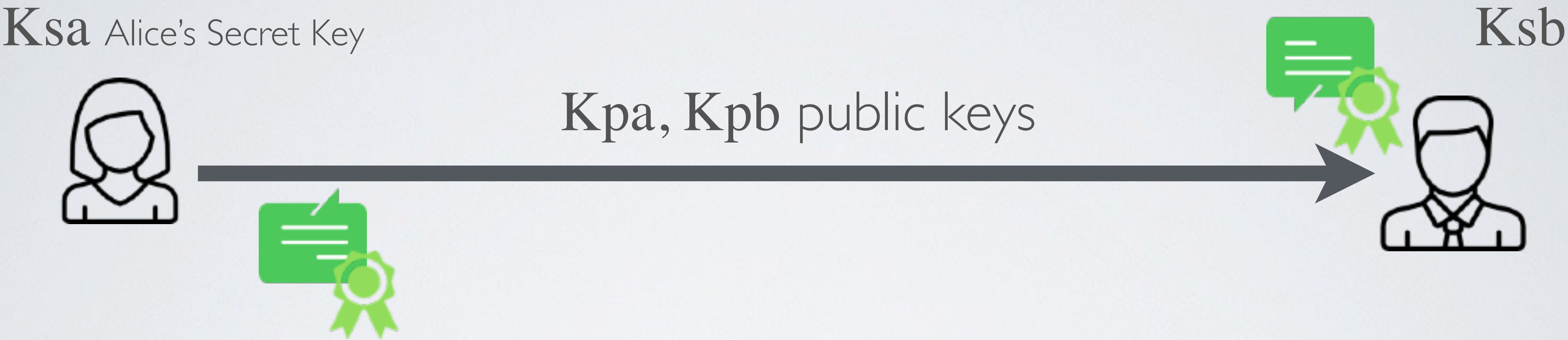
$D_{Kpa}(E_{Ksa}(m)) = m$

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)

Digital Signature



- ➡ Use public cryptography to **sign and verify**

$$m \,\|\, SIG_{Ksa}(m)$$

$$SIG_{Ksa}(m) = E_{Ksa}(H(m))$$