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}

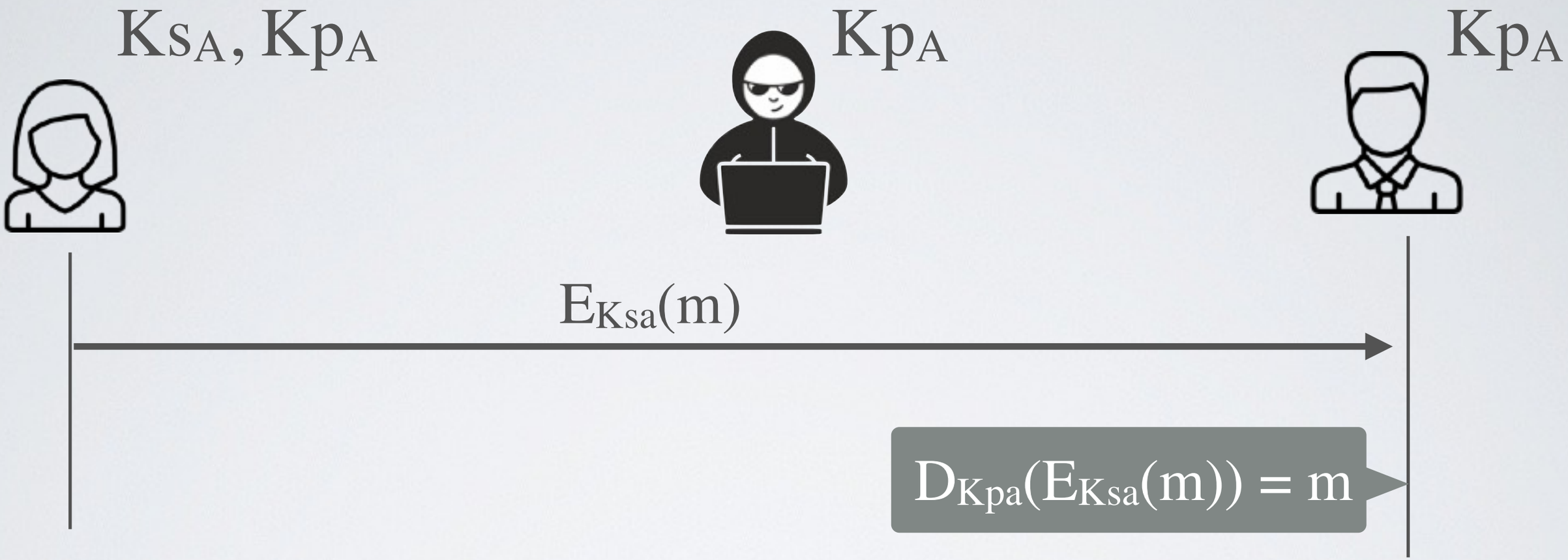

Кра


Кра


$E_{Ksa}(m)$

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

Asymmetric encryption for **integrity**

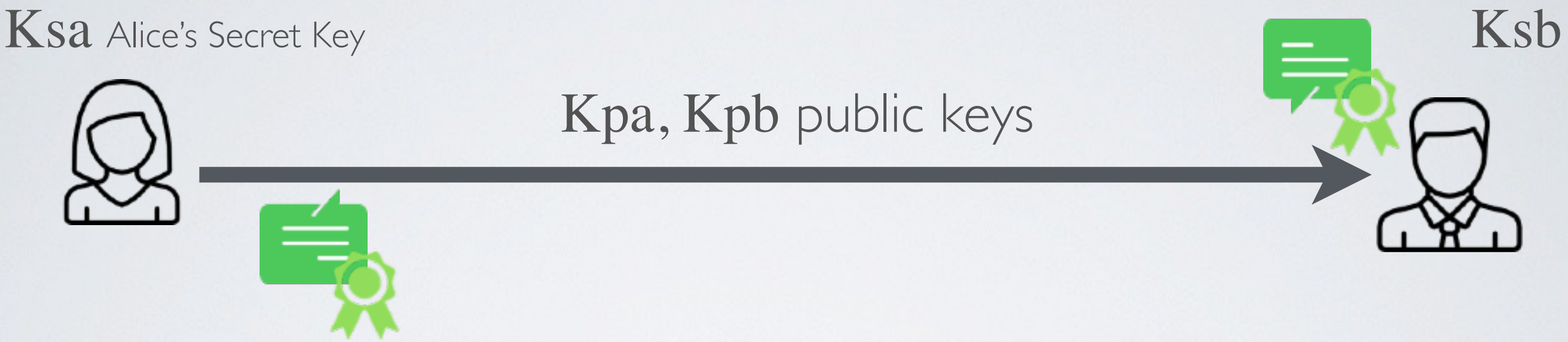


Alice encrypts a message **m** with her private key $\mathbf{Ks_A}$

➡ Everybody can decrypt **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**

$$m \parallel SIG_{Ksa}(m)$$

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