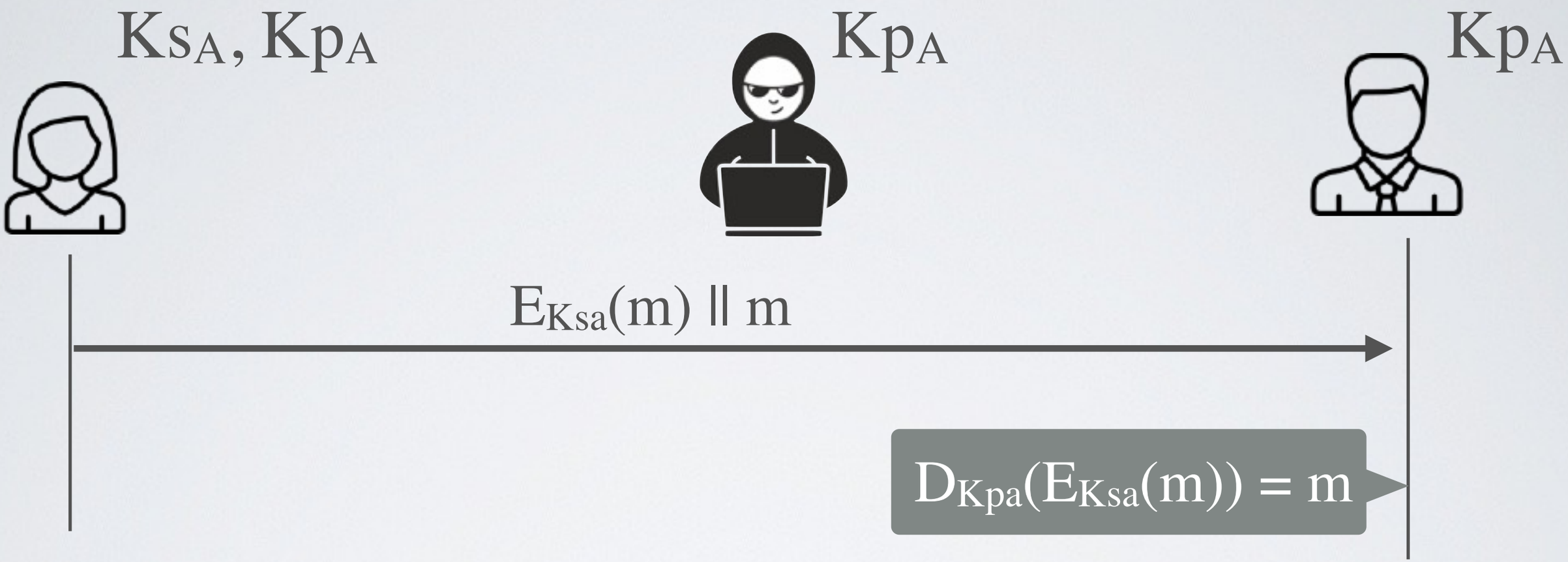
Asymmetric encryption for **integrity**

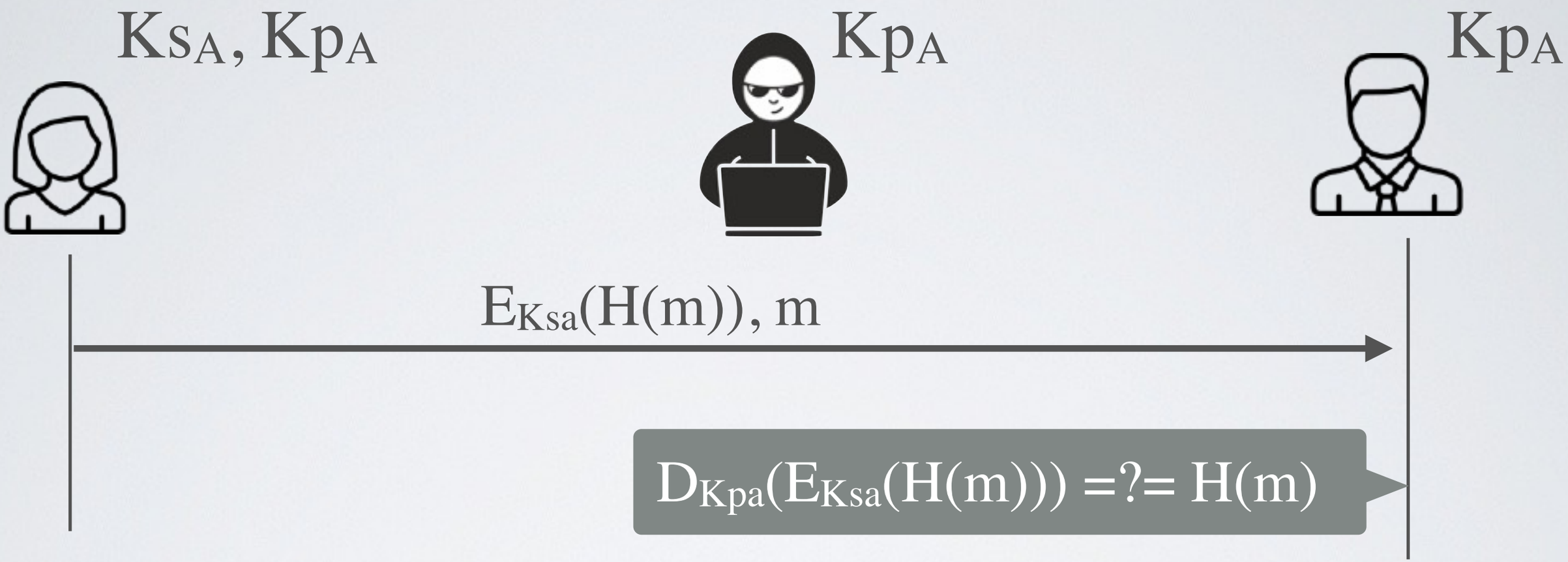


Alice encrypts a message **m** with her private key $\mathbf{Ks_A}$

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

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

The Naive Approach of Digital Signatures



1. Alice signs the message $\mathbf{m}$ by encrypting the hash of $\mathbf{m}$ with her private key $\mathbf{Ks_A}$
2. Alice sends the message $\mathbf{m}$ (in clear) and the encrypted hash to Bob
3. Bob decrypts $\mathbf{H(m)}$ using Alice's public key $\mathbf{Kp_A}$
   and verifies that it matches the hash of the message $\mathbf{m}$ received