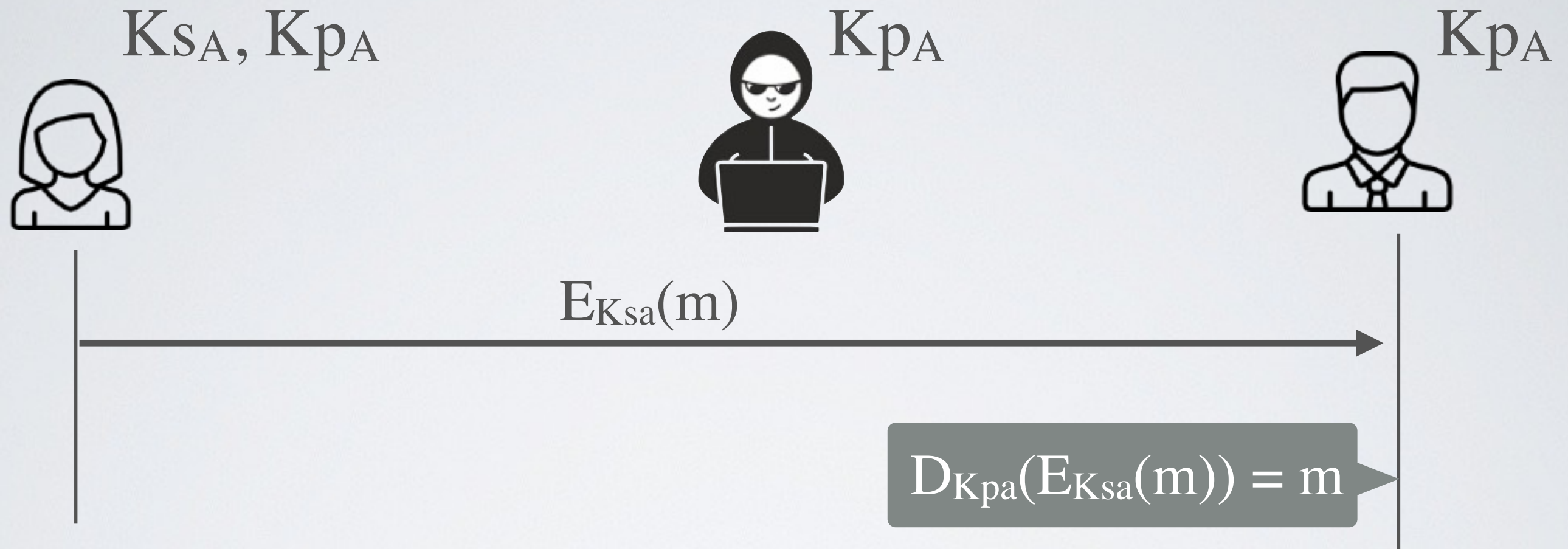


Asymmetric encryption for **integrity**

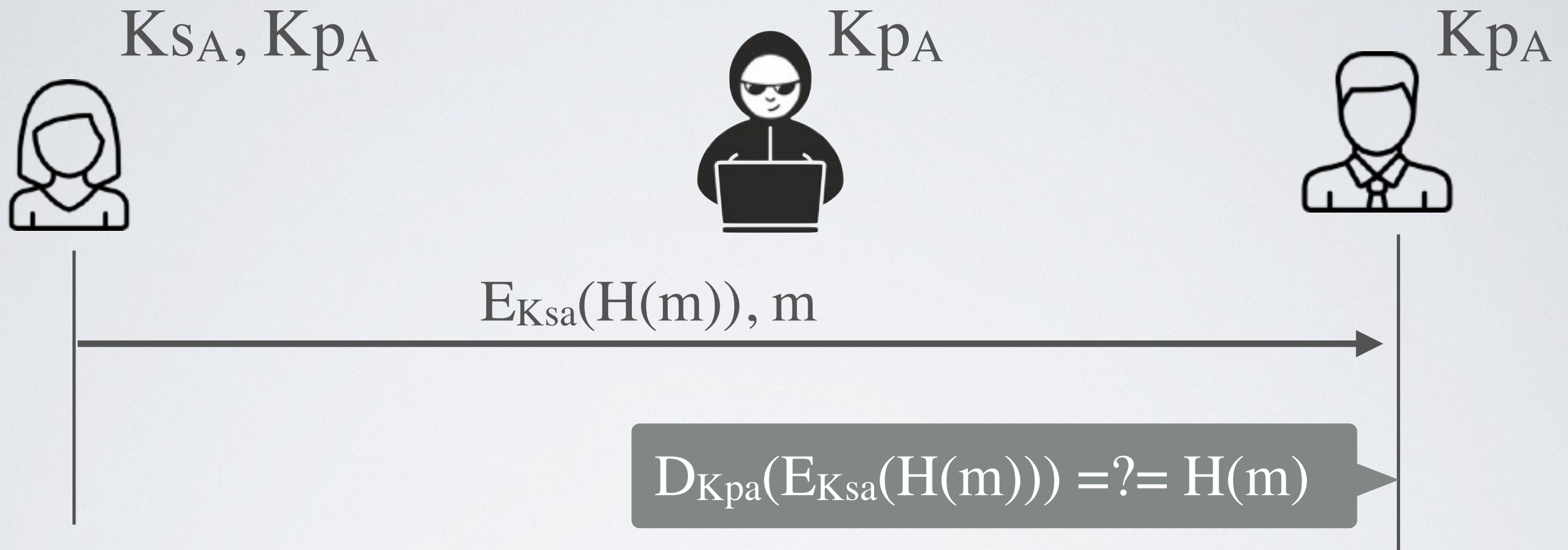


Alice encrypts a message m with her private key K_{SA}

➔ Everybody can decrypt m using Alice's public key K_{PA}

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

The Naive Approach of Digital Signatures



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