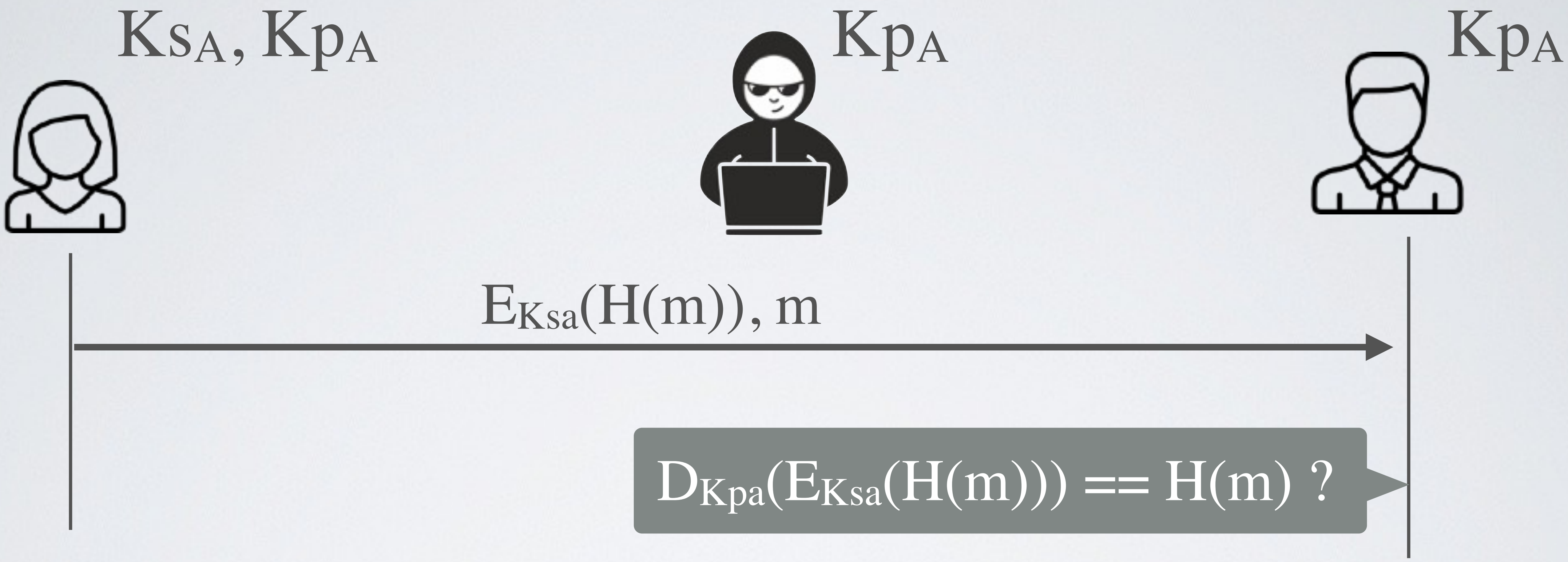
The Naive Approach of Digital Signatures



Ks_A, Kp_A

Kp_A

Kp_A

$E_{Ksa}(H(m)), m$

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

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

Digital Signatures Schemes in Practice

The precursors

- *ElGamal signature*
- *Schnorr signature*

The standards

- *DSA - Digital Signature Algorithm* (RSA-based)
- *ECDSA - Elliptic Curve Digital Signature Algorithm* (ECC-based)

The newcomer

- *EdDSA - Edwards-curve Digital Signature Algorithm* (ECC-based)