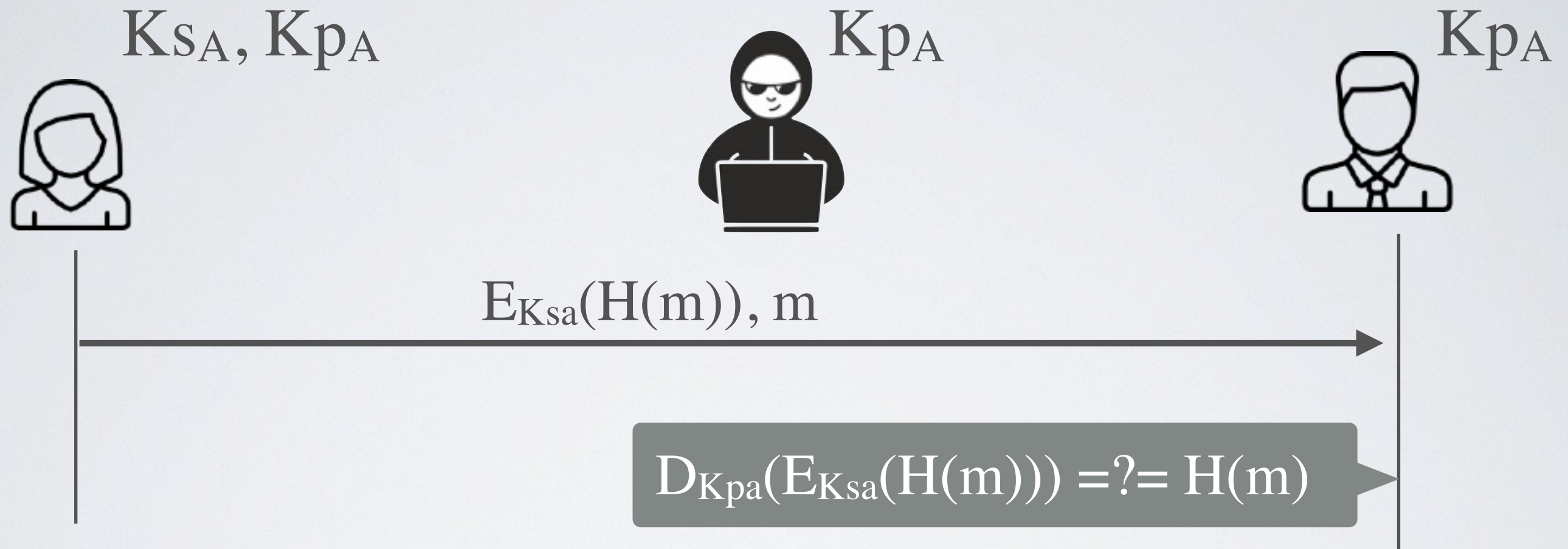


The Naive Approach of Digital Signatures



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

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)*