

Asymmetric encryption

Bob encrypts a message m with Alice's public key K_{p_A}

➔ Nobody can decrypt m , except Alice with her private key K_{s_A}

✓ Confidentiality without the need to exchange a secret key







KsA, KpA

KpA

KpA

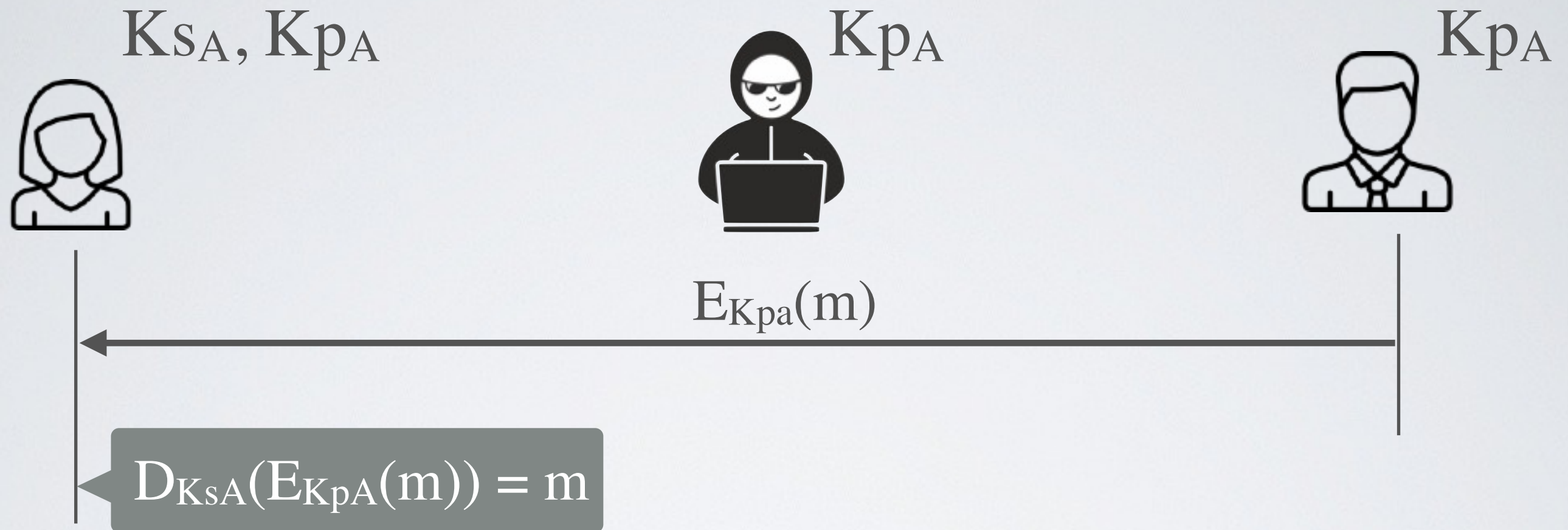





$$E_{Kpa}(n)$$


$$D_{K_{SA}}(E_{K_{PA}}(m)) = m$$

Asymmetric encryption for **confidentiality**



Bob encrypts a message m with Alice's public key K_{pA}

➔ Nobody can decrypt m , except Alice with her private key K_{sA}

✓ Confidentiality without the need to exchange a secret key

Functional Requirements

$D_{K_s}(E_{K_p}(m)) = m$ and $D_{K_p}(E_{K_s}(m)) = m$ for every pair (K_p, K_s)

- ✓ Generating a pair (K_p, K_s) is easy to compute (polynomial)
- ✓ Encryption is easy to compute (either polynomial or linear)
- ✓ Decryption is easy to compute (either polynomial or linear)
- Finding a matching key K_s for a given K_p is hard (exponential)
- Decryption without knowing the corresponding key is hard (exponential)