

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

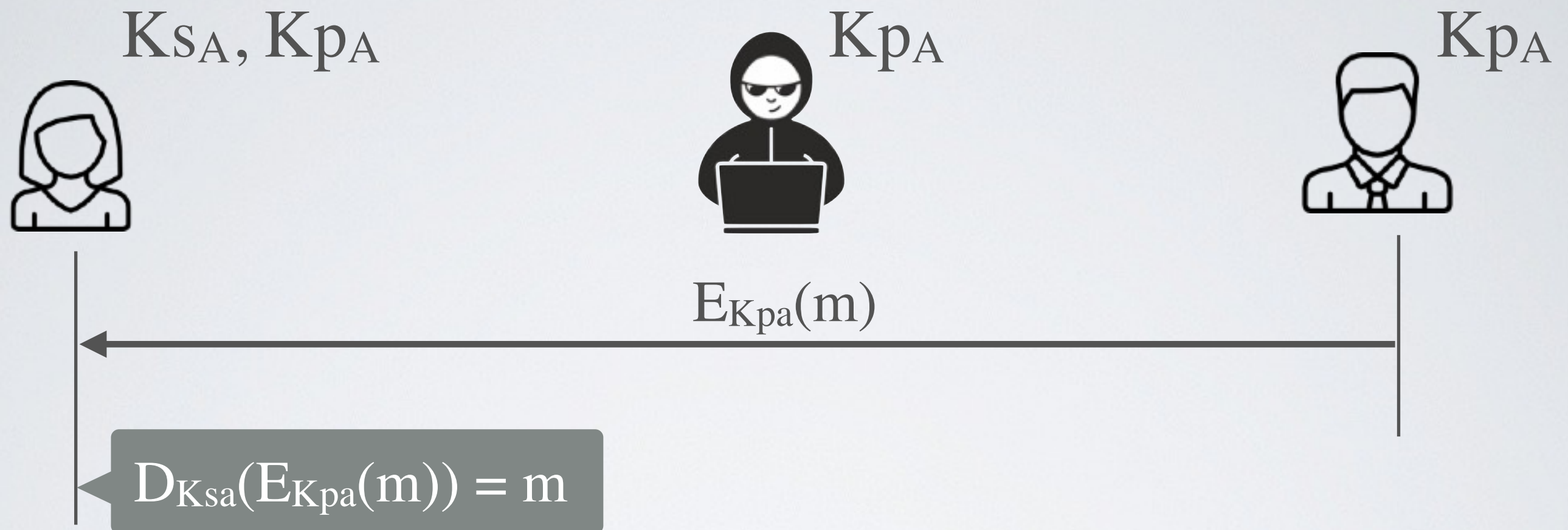





$$E_{Kpa}(n)$$


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

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

Asymmetric encryption: Digital Signature

- ➔ The private key for encryption
- ➔ The public key for decryption

