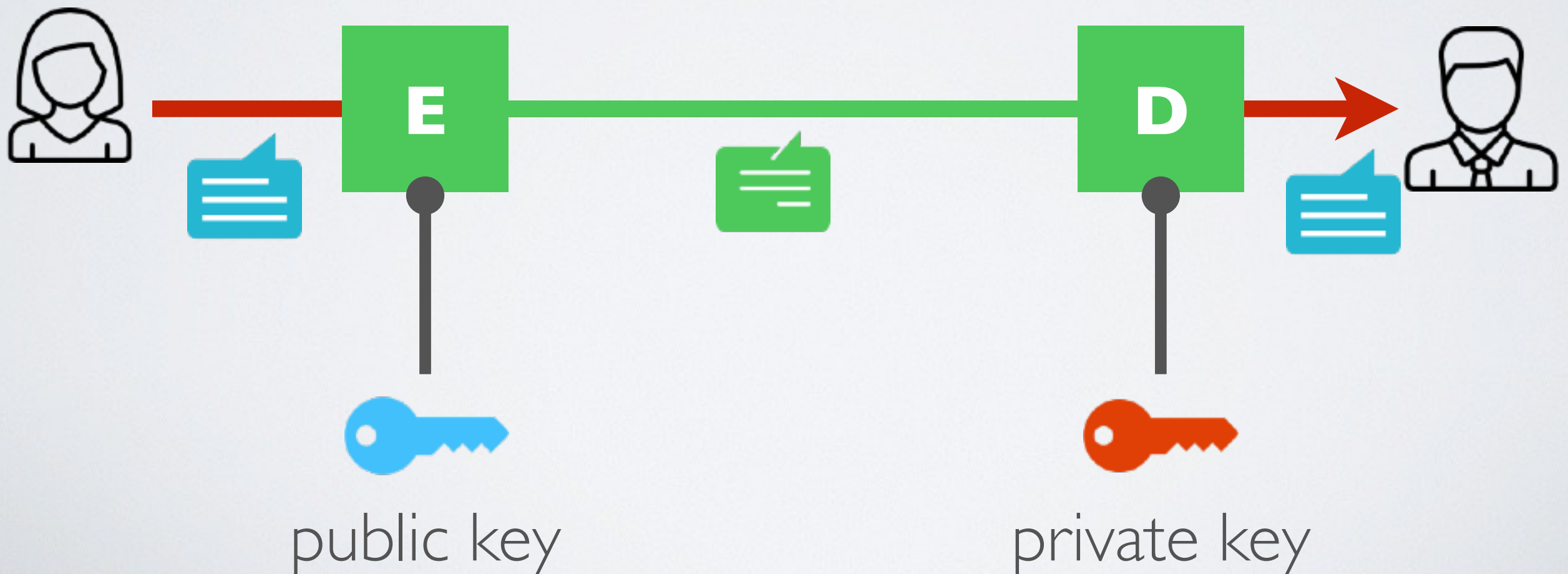
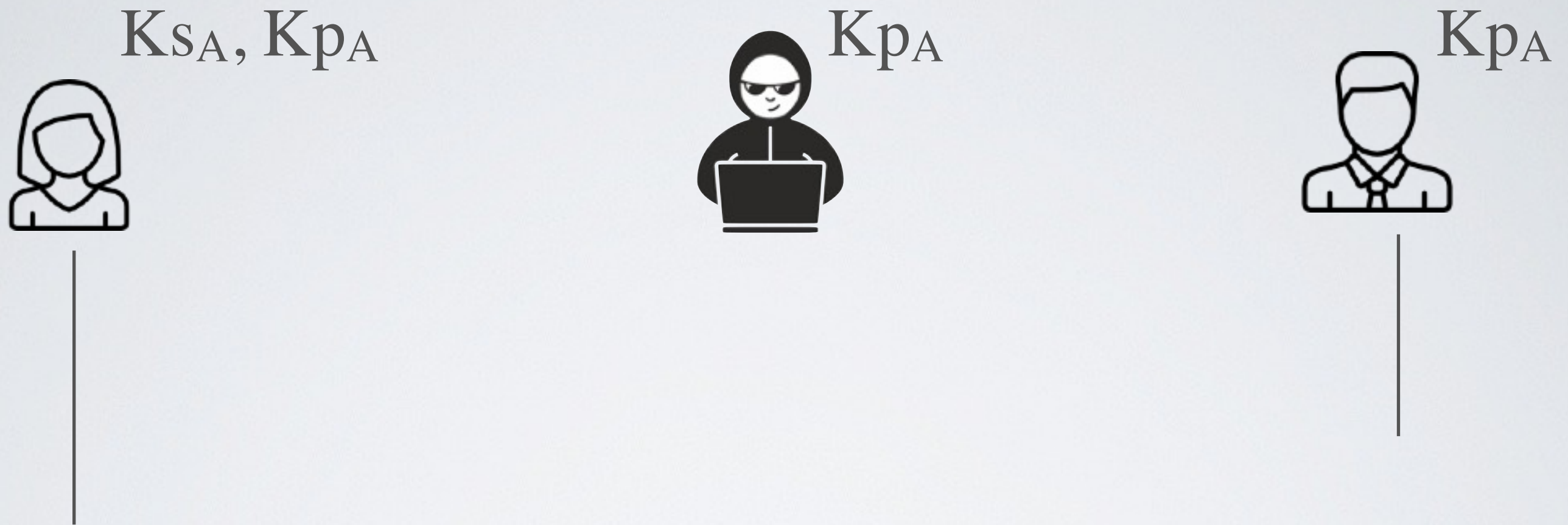


Asymmetric encryption a.k.a Public Key Cryptography

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



Asymmetric encryption for **confidentiality**



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