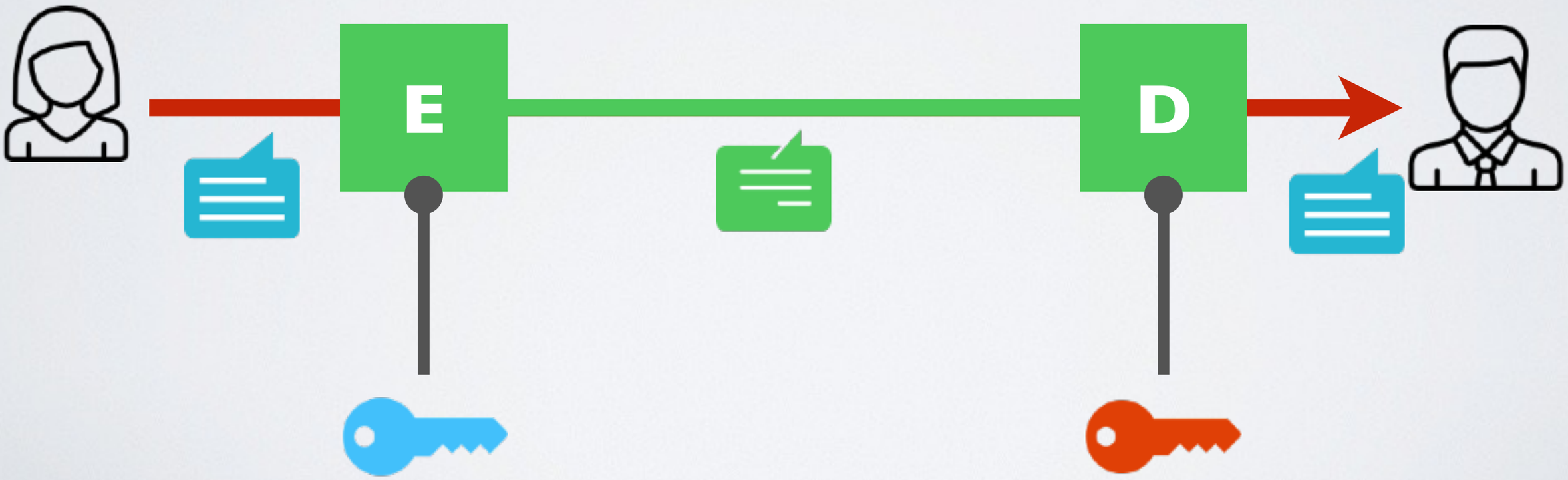
Asymmetric encryption
a.k.a Public Key Cryptography

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

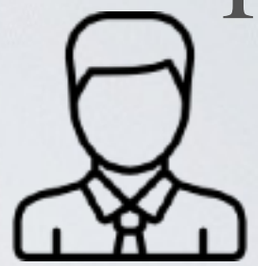


Asymmetric encryption for **confidentiality**

Ks_A, Kp_A

Kp_A

Kp_A



Bob encrypts a message $\mathbf{m}$ with Alice's public key $\mathbf{Kp_A}$

➡ Nobody can decrypt $\mathbf{m}$, except Alice with her private key $\mathbf{Ks_A}$

✓ Confidentiality without the need to exchange a secret key