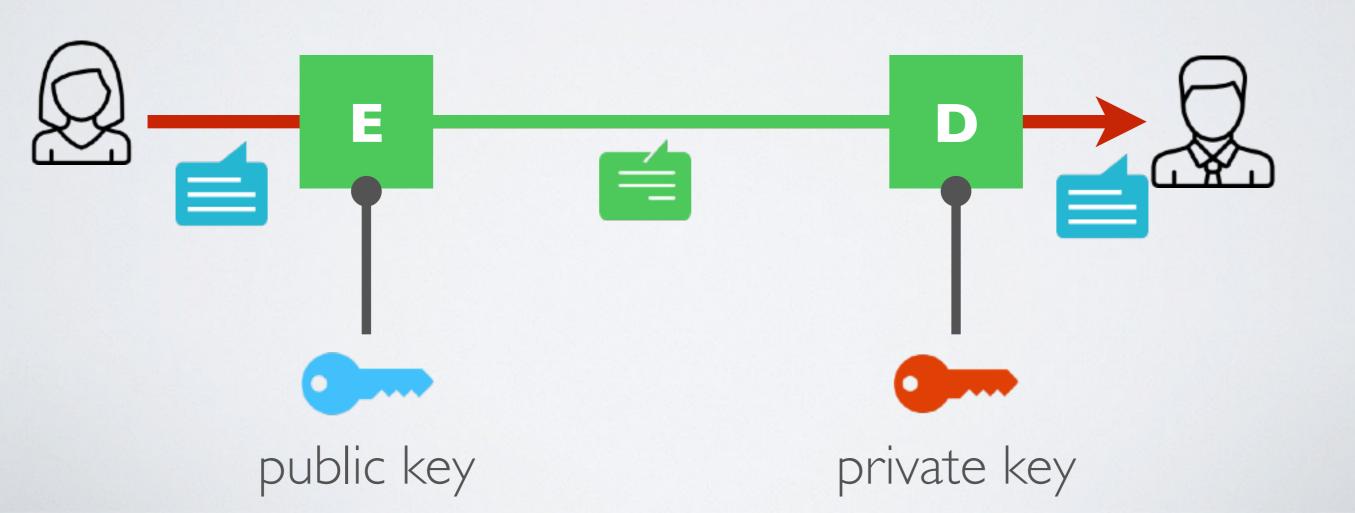
## Asymmetric encryption a.k.a Public Key Cryptography

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



## Message digests

Message digests are meant for creating fingerprints of messages

- Un-keyed message digest: hashes, checksum
- Keyed message digests : MACs