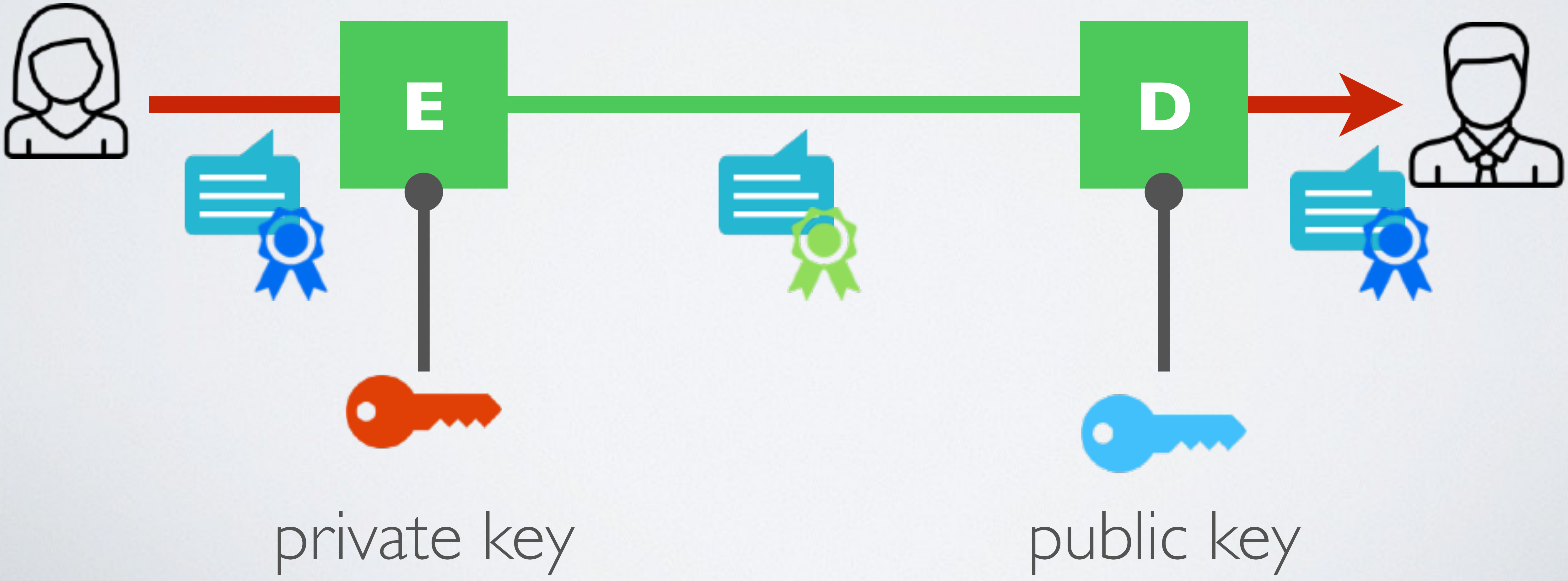
Message digests

Message digests are meant for creating fingerprints of messages

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

Digital Signature

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



E
D
private key
public key