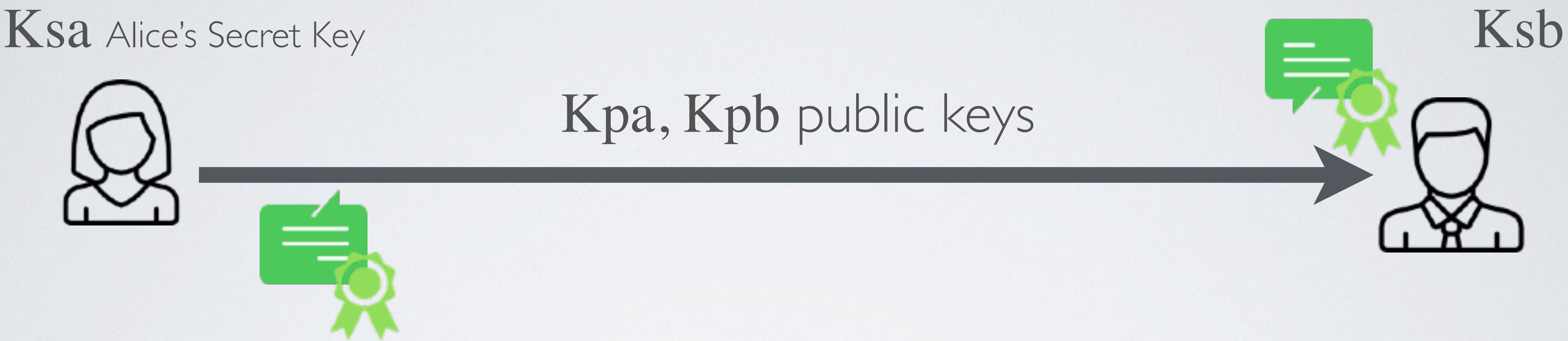
Digital Signatures and Confidentiality



Ksa Alice's Secret Key

Kpa, **Kpb** public keys

Ksb

1. Alice generates an asymmetric session key **k**
2. Use both symmetric and asymmetric cryptography to **encrypt, sign and verify** the message and the key

$$E_{Kpb}(k) \,||\, E_{k}(m \,||\, E_{Ksa}(H(m)))$$

Message digests

Message digests are meant for creating fingerprints of messages

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