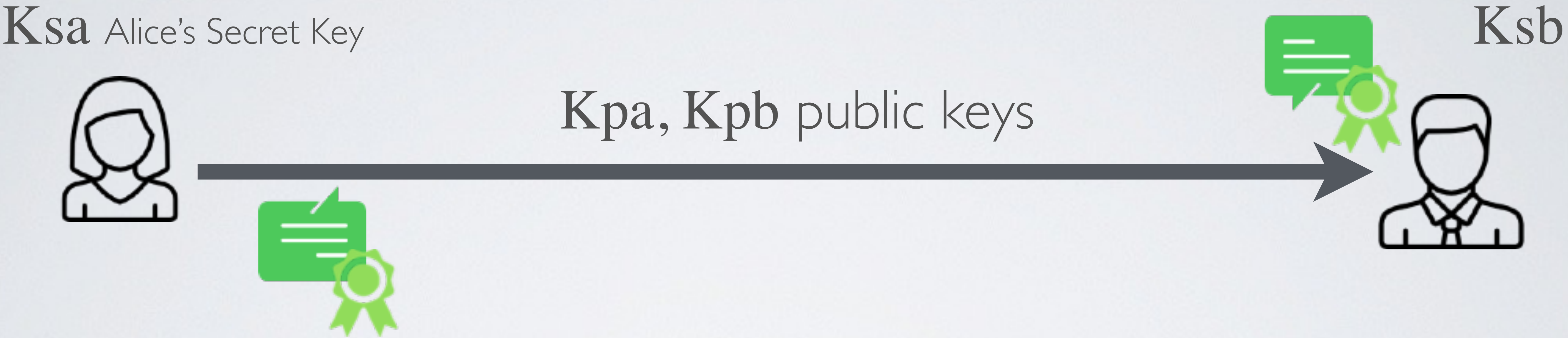
Digital Signatures and Confidentiality



Ksa Alice's Secret Key

Kpa, Kpb public keys

Ksb

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

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

Goals

1. Establish a session key to exchange data while ensuring Perfect Forward Secrecy

   ✓ Use the Diffie-Hellman key exchange protocol

2. Ensure one-way or mutual authentication

   ✓ Use asymmetric encryption