Asymmetric encryption: Digital Signature

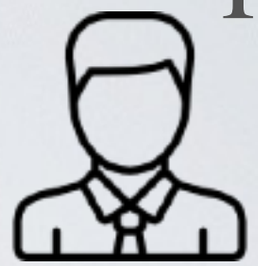
- The private key for encryption
- The public key for decryption

Asymmetric encryption for **integrity**

Ks_A, Kp_A

Kp_A

Kp_A



Alice encrypts a message $\mathbf{m}$ with her private key $\mathbf{Ks_A}$

➡ Everybody can decrypt $\mathbf{m}$ using Alice's public key $\mathbf{Kp_A}$

✓ Authentication with non-repudiation (a.k.a Digital Signature)