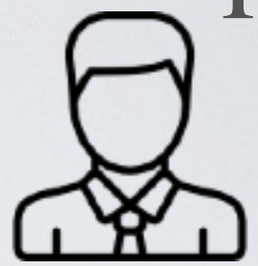
Asymmetric keys

K_{sA}, K_{pA}

K_{pA}

K_{pA}



Alice generates a pair of asymmetric keys

- $\mathbf{K_{sA}}$ is the secret key that Alice keeps for herself
- $\mathbf{K_{pA}}$ is the public key that Alice gives to everyone (even Mallory)

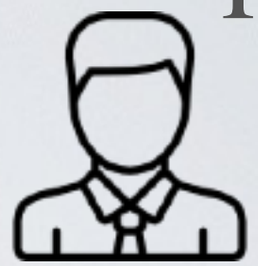
➡ These two keys $\mathbf{K_{sA}}$ and $\mathbf{K_{pA}}$ work together

Asymmetric encryption for **confidentiality**

Ks_A, Kp_A

Kp_A

Kp_A



Bob encrypts a message $\mathbf{m}$ with Alice's public key $\mathbf{Kp_A}$

➡ Nobody can decrypt $\mathbf{m}$, except Alice with her private key $\mathbf{Ks_A}$

✓ Confidentiality without the need to exchange a secret key