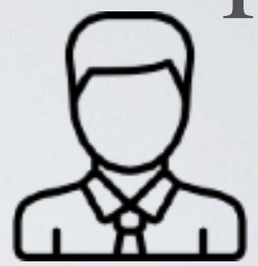
Asymmetric keys

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 Keys - Functional Requirements

$D_{Ks}(E_{Kp}(m)) = m$ and $D_{Kp}(E_{Ks}(m)) = m$ for every pair (Kp, Ks)

- ✓ Generating a pair (Kp, Ks) is easy to compute (polynomial)
- ✓ Encryption is easy to compute (either polynomial or linear)
- ✓ Decryption is easy to compute (either polynomial or linear)
- ◉ Finding a matching key Ks for a given Kp is hard (exponential)
- ◉ Decryption without knowing the corresponding key is hard (exponential)