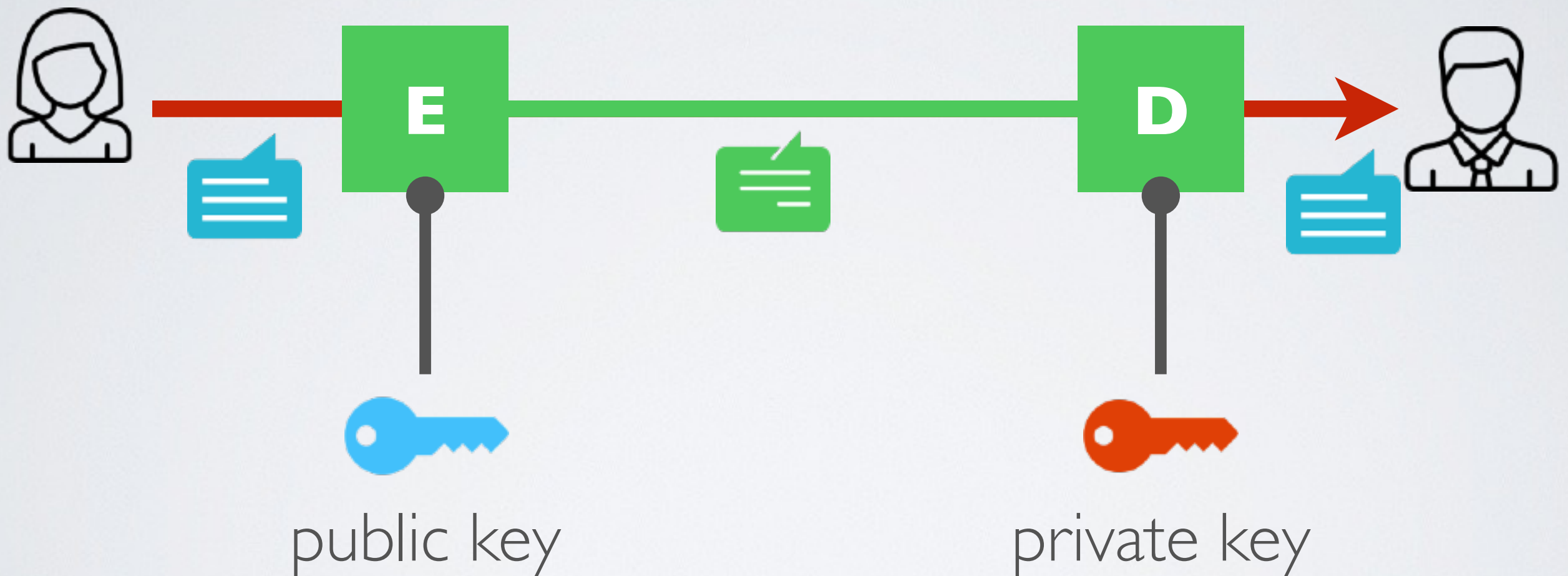


Asymmetric encryption a.k.a Public Key Cryptography



Asymmetric Keys - Functional Requirements

$D_{K_s}(E_{K_p}(m)) = m$ and $D_{K_p}(E_{K_s}(m)) = m$ for every pair (K_p, K_s)

- ✓ Generating a pair (K_p, K_s) 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 K_s for a given K_p is hard (exponential)
- Decryption without knowing the corresponding key is hard (exponential)