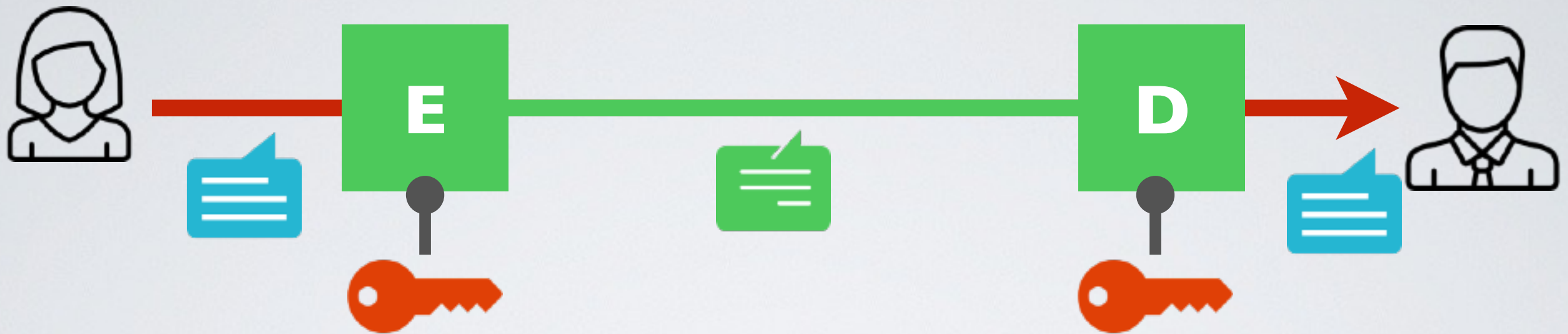


Symmetric Key Encryption



➡ The same key k is used for encryption E and decryption D

1. $D_k(E_k(m))=m$ for every k , E_k is an injection with inverse D_k
2. $E_k(m)$ is easy to compute (either polynomial or linear)
3. $D_k(c)$ is easy to compute (either polynomial or linear)
4. $c = E_k(m)$ finding m is hard without k (exponential)

Protocols