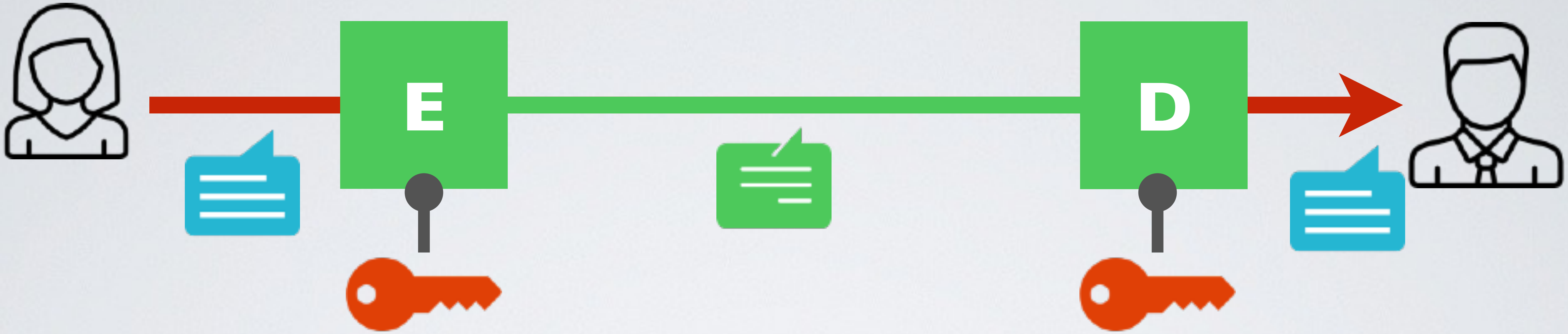
Functional Requirements



➡ The same key $\mathbf{k}$ is used for encryption $\mathbf{E}$ and decryption $\mathbf{D}$

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)

Outline

Stream cipher

RC4 - Rivest Cipher 4 (now deprecated)

Salsa20

Block cipher

- Encryption standards

  DES (and 3DES) - Data Encryption Standard (now deprecated)

  AES - Advanced Encryption Standard

- Block cipher modes of operation