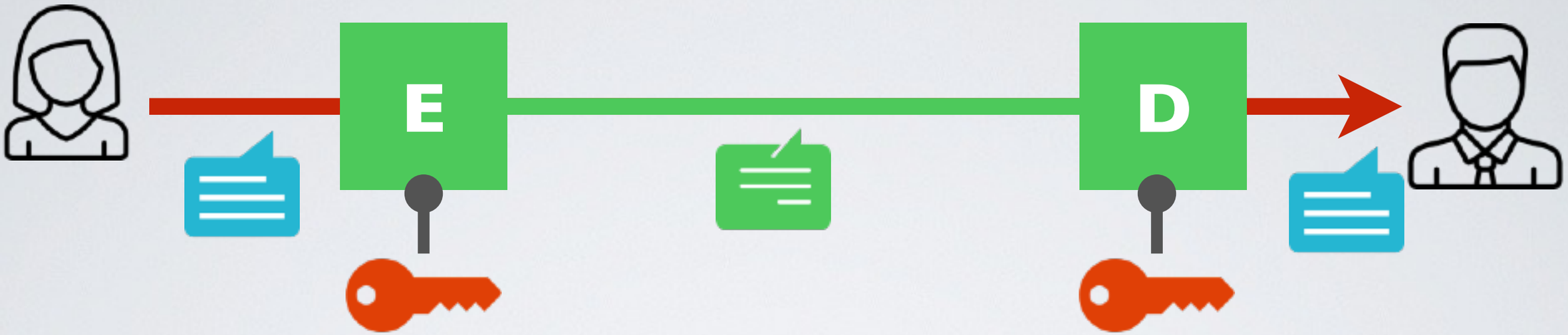
Functional Requirements



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

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

Two Families of Symmetric Encryption Schemes

Stream cipher

RC4 - Rivest Cipher 4 (now deprecated)

Salsa20 (and ChaCha20)

Block cipher

- Encryption standards

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

  AES - Advanced Encryption Standard

- Block cipher modes of operation