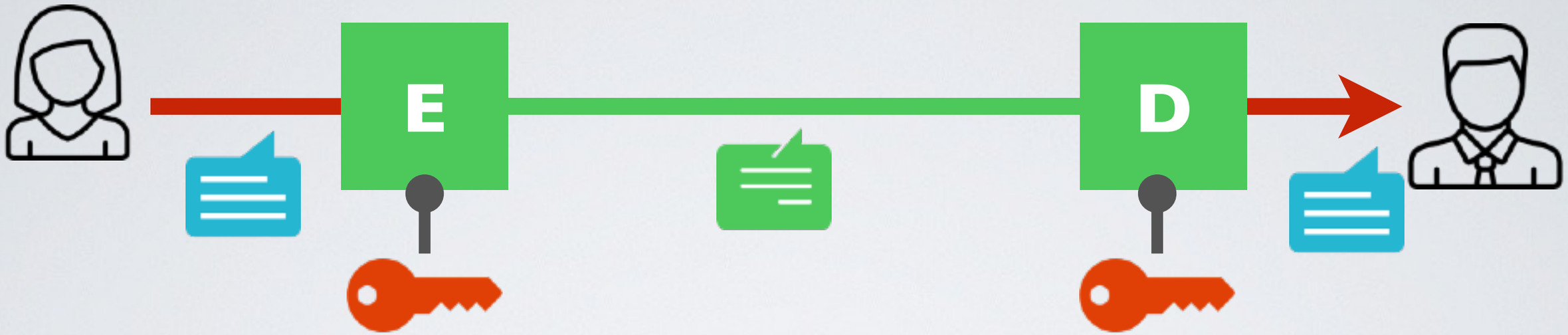
Definitions

One way algorithms
Also known as message digests. No keys involved. Encryption cannot be reversed.

Symmetric Key algorithms
The keys used for encryption and decryption are the same OR two-way mathematically related (can be derived from the other reliably)

Public Key algorithms
Also known as asymmetric algorithms. The keys used for encryption and decryption are different but one-way mathematically related.

Symmetric Key Encryption



➡ 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)