The attacker's model

- **Exhaustive Search**
  Try all possible n keys (in average it takes n/2 tries)

- **Ciphertext only**
  You know one or several random ciphertexts

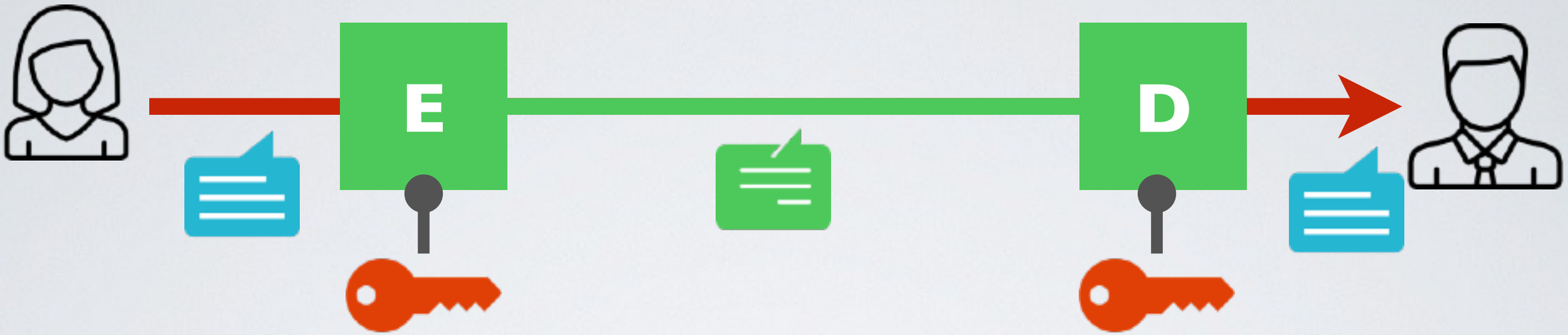
- **Known plaintext**
  You know one or several pairs of random plaintext and their corresponding ciphertexts

- **Chosen plaintext**
  You know one or several pairs of chosen plaintext and their corresponding ciphertexts

- **Chosen ciphertext**
  You know one or several pairs of plaintext and their corresponding chosen ciphertexts

➡ **A good crypto system resists all attacks**

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)