

# 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**

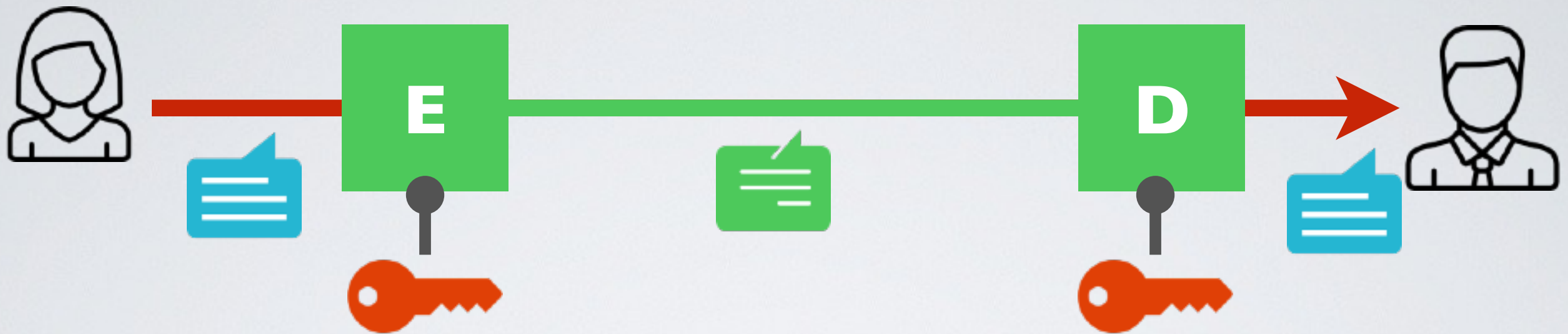
You know one or several pairs of chosen plaintext and their corresponding ciphertexts

- **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  $k$  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)