

# Security of DES - DES Challenges (brute force contests)

**1998** *Deep Crack*, the EFF's DES cracking machine used 1,856 custom chips

- Speed : matter of days
- Cost : \$250,000

**2006** *COPACOBANA*, the COst-optimized Parallel COdeBreaker used 120 FCPGAs

- Speed : less than 24h
- Cost : \$10,000

# How about 2DES ?

$$2DES_{k_1, k_2}(m) = E_{k_2}(E_{k_1}(m))$$

**Meet-in-the-middle attack** - known-plaintext attack

1. Brute force  $E_{k_1}(m)$  and save results in a table called TE ( $2^{56}$  entries)
2. Brute force  $D_{k_2}(c)$  and save results in a table called TD ( $2^{56}$  entries)
3. Match the two tables together to get the key candidates
  - ➡ The more plaintext you know, the lesser key candidates
  - ➡ Effective key-length (entropy) is **57 bits**
  - ➡ This attacks applies to every encryption algorithm used as such