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 FPGAs

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

3DES (Triple DES)

$$3DES_{k1,k2,k3}(m) = E_{k3}(D_{k2}(E_{k1}(m)))$$

- ➡ Uses three keys; some same or all distinct
- ➡ Effective key length (entropy) : 112 bits or 168 bits
- ✓ Very popular, used in PGP, TLS (SSL) …
- ◉ But terribly slow