

# 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

# AES - Advanced Encryption Standard

## Timeline

- **1996** NIST issues public call for proposal
- **1998** 15 algorithms selected
- **2001** winners were announced