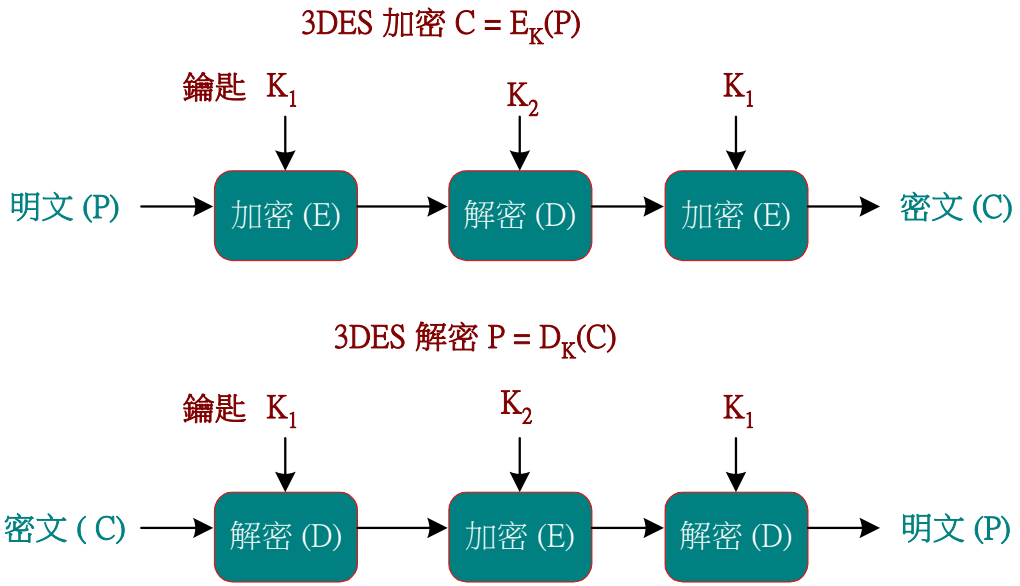
Triple-DES 密碼系統

Two-Keys 3DES

2 把鑰匙：56 bits * 2

- 加密：$C = E_{K1}[D_{K2}[E_{K1}[P]]]$
- 解密：$P = D_{K1}[E_{K2}[D_{K1}[C]]]$
- 鑰匙：$K = K_1 \| K_2$（排列組合）



Three-keys 3DES

- 3 把鑰匙：56 bits *3
  - 加密：$C = E_{K3}[D_{K2}[E_{K1}[P]]]$
  - 解密：$P = D_{K1}[E_{K2}[D_{K3}[C]]]$
  - 鑰匙：K = K1 || K2 || K3