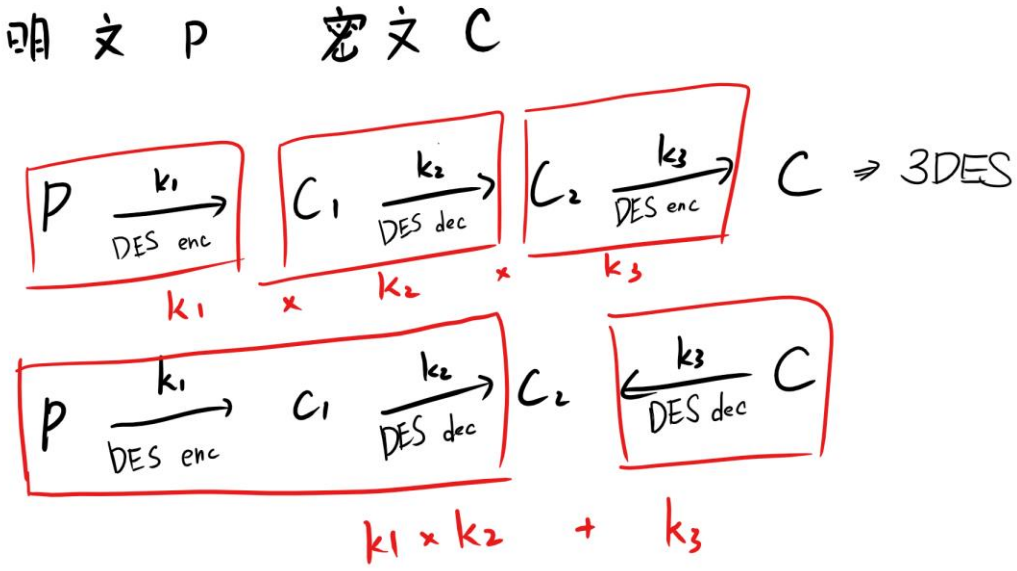
B10415049 資訊安全導論 HW2

3DES 就是 先用 k_1 做 DES 加密，再把結果用 k_2 做 DES 解密，最後再用 k_3 做一次 DES 加密。



當攻擊者已知明文與密文時，由於是對稱式加密的關係，我們可以用空間換取時間，把前面兩把金鑰算出的結果存起來，與最後一把金鑰解密的結果存起來，最後再去比較 C_2 是否一致就可以破解出金鑰了，使得原本暴力破解法

$k_1 \times k_2 \times k_3$ 和 1 個 C 做比對

變成

$k_1 \times k_2$ 和 k_3 做比對

從要算 3 次 DES 算法相乘變成只要算 2 次 DES 算法相乘加上 1 次 DES 算法，難度形同少了一把金鑰。