**HW2 of Introduction to Information Security 2018**

Deadline: 10/18 23:55

A10615003 張家成 二資工三

1. Please completely describe the encryption procedure of 3DES with three different keys and explain why security of 3DES only reaches 112 bits (not 56x3 bits)?

答：

3DES 即 將 DES演算法執行三次

P = plaintext

C = cipher text

k1 = key1

k2 = key2

k3 = key3

E = encrypt

D = decrypt

3DES加密：

將明文P使用DES 的k1加密得到的中間結果再通過DES 的k2進行解密，最後再使用DES的k3加密得到最終密文。

即：

C = E\_k3((D\_k2((E\_k1(P)))))

3DES解密(於加密相反)：

將密文C使用DES的k3解密得到的中間結果再通過DES的k2進行加密，最後再使用DES的k1解密得到最終明文。

即：

P = D\_k1((E\_k2((D\_k3(C)))))

若

* k1 ≠ k2 ≠ k3

則擁有 3\*56 = 168 bits 長度的密鑰

即：

C = E\_k3((D\_k2((E\_k1(P)))))

* k1 = k3 ≠ k2

則擁有 2\*56 = 112 bits 長度的密鑰

即：

C = E\_k1((D\_k2((E\_k1(P)))))

* k1 = k2 = k3

此時3DES = DES，擁有56 bits長度的密鑰

即：

C = E\_k((D\_k((E\_k(P))))) = E\_k(P)

當我們選擇

k1 ≠ k2 ≠ k3 方式來進行3DES加密時，可以得到

C = E\_k3((D\_k2((E\_k1(P)))))

P = D\_k1((E\_k2((D\_k3(C)))))

由此可知：

如果已經知道了一對明文和密文(P&C)，則可以利用中途相遇攻擊(Meet in the middle attack)，枚舉所有的k1(2^56個)將P加密後得到2^56個P’的結果儲存起來，同樣枚舉k3將C解密後得到的2^56個C’的結果也儲存起來，接著枚舉k2並與剛才的C’運算，此時會運算2^56\*2^56=2^112個位元，得到C’’。最後將C’’和P’兩個結果進行比對，找到相同的結果，那麼我們就可以認為我們找到了k1, k2以及k3。由此可推出，即便是k1 ≠ k2 ≠ k3，3\*56=168 bits 長度的key，最大安全位元數只有112 bits。

中途相遇攻擊(Meet in the middle attack)

流程圖

