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：

(一)

3DES 即 將 DES 演算法執行三次

P = plaintext

C = cipher text

k_1 = key1

k_2 = key2

k_3 = 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：

$C = E\_k_3((D\_k_2((E\_k_1(P)))))$

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：

$P = D\_k_1((E\_k_2((D\_k_3(C)))))$

若

- $k_1 \neq k_2 \neq k_3$
  則擁有 3*56 = 168 bits 長度的密鑰
  即：
  $C = E\_k_3((D\_k_2((E\_k_1(P)))))$

- $k_1 = k_3 \neq k_2$
  則擁有 2*56 = 112 bits 長度的密鑰
  即：
  $C = E\_k_1((D\_k_2((E\_k_1(P)))))$

- $k_1 = k_2 = k_3$
  此時 3DES = DES，擁有 56 bits 長度的密鑰
  即：
  $C = E\_k((D\_k((E\_k(P))))) = E\_k(P)$

(二)

當我們選擇
$k_1 \neq k_2 \neq k_3$ 方式來進行 3DES 加密時，可以得到
$C = E\_k_3((D\_k_2((E\_k_1(P)))))$
$P = D\_k_1((E\_k_2((D\_k_3(C)))))$

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 k_1(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 k_3 將 C 解密後得到的 2^56 個 C'的結果也儲存起來，接著枚舉 k_2 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 k_1, k_2 以及 k_3。由此可推出，即便是 $k_1 \neq k_2 \neq k_3$，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