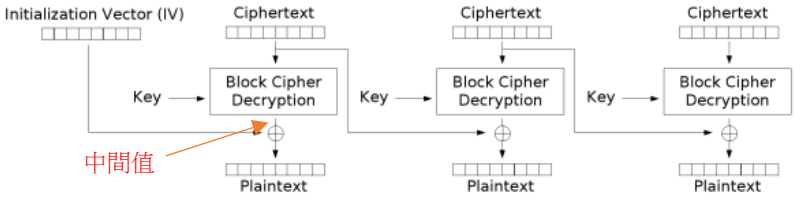
黃禹靖 電機四 b05901172

思路：

1. 得到 IV

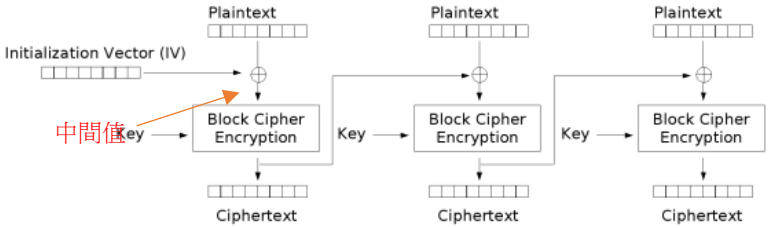
   Pt (plain text)是已知的，如果有第一個 block 的中間值，就可以得到 IV。



Cipher Block Chaining (CBC) mode decryption

   並且 Ct (cipher text)是可以控制的，把要解的第一個 block 丟到最後，使用 padding oracle attack，控制前一個 block 的 Ct，則可以慢慢解出中間值，並 xor 第一個 block 的 Pt 得到 IV。

2. 利用 IV 得出想要的 Pt 對應的 Ct



Cipher Block Chaining (CBC) mode encryption

   golden_Pt: 想要的 Pt {“milk”: -1, “name”: “admin” }\x03\x03\x03
   golden_Pt[i]: golden_Pt 的第 i 個 block
   golden_Ct: golden_Pt 對應的 Ct
   golden_Ct[i]: golden_Ct 的第 i 個 block

   目標是 golden_Ct。

   先解 golden_Ct[1]。
   想要知道 golden_Ct[1]，必須塞對應的 golden_Pt[1]到 block cipher 裡。
   已知 IV 和 golden_Pt[1]，xor 起來可以知道中間值。若可以在某個 block 塞中間值，就可以得到 golden_Ct[1]。
   由於 name 是可以控制的 Pt，則控制 name 對應的 Pt[j]使其和 Ct[j-1] xor 起來剛好是想要的中間值，故 Pt[j] = IV xor golden_Pt[1] xor Ct[j-1]。

由此方法可以得到 golden_Ct[1]。

解 golden_Ct[2]相當於把 golden_Ct[1]當成 IV 解第二塊，Pt[j] = golden_Ct[1] xor golden_Pt[2] xor Ct[j-1]，故用類似的方法可以解出全部的 golden_Ct。

Flag：

NMLab{C0w_Says_human_iS_tHe_wOr5t_anIma1_iN_Th3_w0 r1d!!!!}