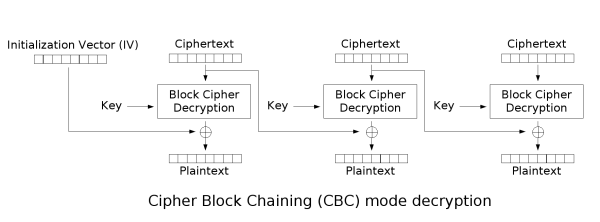
黃禹靖 電機四 b05901172

思路：

1. 得到IV

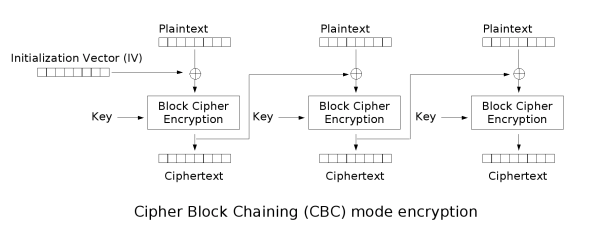
Pt (plain text)是已知的，如果有第一個block的中間值，就可以得到IV。



中間值

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。

1. 利用IV得出想要的Pt對應的Ct



中間值

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!!!!}