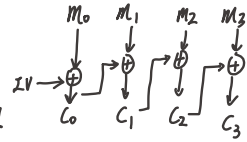
作业： 赵伯侯 20213021 81156

1. CBC 变体

第一次加密时，用随机IV

之后用上一个密文的最后一个分组



试分析其在选择明文攻击下的安全性 $M_n = B_{15} \cdots B_1 B_0$

答：攻击者已知 由为密文与密文的分组 $C_0, C_1 \cdots C_n$

选择明文可以知道其密文

与攻击CBC一样使用填充报错攻击

逐个修改 M_n 中的每个字符直到出现填充错误，设在倒数2位出现

则可知 填充为2位，内容为 0x2，

但由于 IV 和上一密文分组均是在加密过程使用，

并不能通过简单异或关系 利用填充报错攻击解决

由于选择明文攻击可以不断地尝试不同明文并得到其密文分析二者关系进行破解

所以在选择明文攻击下 该CBC模式的变体仍有漏洞，但是没能找出

因此我认为该CBC的变体仍然有安全性问题，但找不到具体方法。

2. 设 F是伪随机函数(PRF)

$F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

问 $F': \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$ 是否是 PRF

① $F'_k(x) \overset{def}{=} F_k(0\|x) \| F_k(0\|x)$

② $F'_k(x) \overset{def}{=} F_k(0\|x) \| F_k(1\|x)$ (定义为; 连接)

③ $F'_k(x) \overset{def}{=} F_k(0\|x) \| F_k(x\|0)$

④ $F'_k(x) \overset{def}{=} F_k(0\|x) \| F_k(x\|1)$

① $F'_k(x)$ 定义为 $F_k(0\|x) \| F_k(0\|x)$ 时 不是PRF

因为 $F_k(0\|x)$ 在相同key与自变量的条件下得到的结果相同

$F'_k(x)$ 将两个相同的结果拼接在一起可以找到其输出规律: 左半与右半相同

②③④中 是PRF

因为已知 F_k 是伪随机函数, 则 $F_k(y)$ 的两个不同输出没有规律

则 $F_k(0\|x)$ 与 $F_k(1\|x)$ 之间, $F_k(0\|x)$ 与 $F_k(x\|0)$ 之间

$F_k(0\|x)$ 与 $F_k(x\|1)$ 之间均不存在规律.

两者拼接在一起后的输出也不会存在规律.

这满足伪随机函数的要求. 所以 ②③④是PRF