# 计算机安全 作业1

2018年12月2日 10:57



| | |
|---|---|
| 姓名: | 芮志清 |
| 学号: | 2018Z8020661080 |
| 班级: | 人工智能学院2018级非全日制8班 |
| 邮箱: | ruizhiqing18@mails.ucas.ac.cn |



## 3.2

3.2 考虑分组长度为 128 位、密钥长度为 128 位的 16 轮 Feistel 密码。假设对于给定的 $k$，前 3 个轮密钥 $k_1, \cdots, k_8$ 由密钥扩展算法决定，而设定 $k_9 = k_8, k_{10} = k_7, \cdots, k_{16} = k_1$。假设你有密文 $c$，请解释你如何只向加密 oracle 做一次提问，而解密 $c$ 获得明文 $m$？这表明上述的密码易于被选择明文攻击（可以认为加密 oracle 就是一种装置，给定一个明文，返回相应的密文。装置的内部结构是未知的。当然你也不能打开装置来查看，你所能做的就是对其进行提问而观察相应的输出）。

### 答:

把c输入oracle可以得到明文

### 理由:

Feistel 伪代码描述如下

加密伪代码:

明文:$m_0 m_1$

$for\ i = 2\ to\ r+1\ do$

$\quad m_i = m_{i-2} \oplus f(m_{i-1}, k_{i-1})$

⇒密文:$m_r m_{r+1}$

解密伪代码:

密文: $m_r m_{r+1}$

$for\ i = r+1\ to\ 2\ do$

$\quad m_{i-2} = m_i \oplus f(m_{i-1}, k_{i-1})$

⇒明文:$m_0 m_1$

由于$k_i = k_{r-i+1}$

当把密文进行加密时，每一步的加密密钥实际上于其解密密钥

## 3.8

3.8 这个问题给出了用一轮 DES 加密的具体数值的例子。我们假设明文和密钥 $K$ 有相同的位模式，即

用十六进制表示：0 1 2 3 4 5 6 7 8 9 A B C D E F

用二进制表示： 0000 0001 0010 0011 0100 0101 0110 0111

1000 1001 1010 1011 1100 1101 1110 1111

(a) 推导第一轮的子密钥 $K_1$。

(b) 推导 $L_0$，$R_0$。

(c) 扩展 $R_0$ 得到 $E[R_0]$，其中 $E[\cdot]$ 是表 3.2 的扩展函数。

(d) 计算 $A = E[R_0] \oplus K_1$。

(e) 把(d)的 48 位结果分成 6 位(数据)一组的集合并求对应 S 盒代替的值。

(f) 将(e)的结果连接起来获得一个 32 位的结果 $B$。

(g) 应用置换获得 $P(B)$。

(h) 计算 $R_1 = P(B) \oplus L_0$。

(i) 写出密文。

### 答案：

使用Python编程实现：

https://gist.github.com/ZQRui/df38b5f63139b105e86b6515aa17c538

(a)推导$K_1$

PC1操作后 : F0CCAA0AACCF00

$C_0$ : F0CCAA0

$D_0$ : AACCF00

经过第1次左移

$C_1$ : E199541

$D_1$ : 5599E01

$K_1$:0B02679B49A5

(b)初始置换后

$L_0$: CC00CCFF

$R_0$: F0AAF0AA

**进行第1次加密,Key=0B02679B49A5

(c) 扩展后:7A15557A1555

(d) 异或运算后711732E15CF0

(e) S盒替换

第0组:011100 -> 0000

第1组:010001 -> 1100

第2组:011100 -> 0010

第3组:110010 -> 0001

第4组:111000 -> 0110

第5组:010101 -> 1101

第6组:110011 -> 0101

第7组:110000 -> 0000

(f)连接成32位整数B

B : 0C216D50

(g)P(B) : 921C209C

计算R1=P(B) XOR L0 -> 5E1CEC63

(h)065162832C277242

## 3.9

**3.9　证明 DES 解密算法实际上是 DES 加密算法的逆。**

公式证明

加密过程：

LE_i表示第i轮加密得到的左16位数，RE_i是第i轮加密得到的右16位数。

$$LE_i = RE_{i-1}$$
$$RE_i = LE_{i-1} \oplus F(RE_{i-1}, K_i)$$

经过变换可得：

$$RE_{i-1} = LE_i$$
$$LE_{i-1} = RE_i \oplus F(RE_{i-1}, K_i) = RE_i \oplus F(LE_i, K_i)$$

令LDi是解密的第i轮得到的左16位数，RDi则是右16位数。

$$LD_i = RD_i = LE_{17-i} = RE_{16-i}$$
$$RD_i = LD_i \oplus F(RD_{i-1}, K_{17-i})$$
$$= RE_{16-i} \oplus F(RE_{17-i}, K_{17-i})$$
$$= [LE_{15-i} \oplus F(RE_{17-i}, K_{17-i})] \oplus F(RE_{17-i}, K_{17-i})$$
$$= LE_{15-i}$$

可见经过解密运算之后

$$LD_i = RE_{16-i}$$
$$RD_i = E_{16-i+1}$$

则此解密过程成立，且是加密过程的逆过程