

DES算法练习(1)

1. 为什么S盒一定要为非线性变换?

①增强抗分析攻击能力: 若S盒线性, 那么加密过程中输入和输出之间的关系就会变得简单而预测。

②防止差分分析和线性分析: 非线性S盒有效打破了这些攻击方法的基础。

③提供混淆作用: 在香农的密钥管理理论中, 混淆是加密算法的一个重要特性, 它指的是加密算法应该使得密文尽可能地与密钥和明文之间的关系变得复杂。

2. 任何块密码本质上是一个非线性函数, 这对安全来说是至关重要的。这样看来, 有一个线性的分组密码来把128比特的明码文本块加密到128比特的密码文本块, 让且 (K, m) 指出在密钥 K 下的128比特信息 m 的安全加密。因此,

$$E(K, [m_1 \oplus m_2]) = E_K(m_1) \oplus E_K(m_2)$$

所有128比特格式的 m_1, m_2 描述用128个进中的密码文本, 敌人怎样能在不知道密钥 K 的情况下解密任何密码。

敌人可以构造128个进中的密码文本, 每个密码文本只包含一个比特为1, 其余比特为0。这样, 敌人可以得到128个



明文和密文对，每对对应一个比特的位置。故
人可以利用这 128 对明文和密文对来解密丘密文。

14 如图 3.9 所示，对下列值使用 RSA 算法加密和解密

a. $p=3; q=11; e=7; M=5$

$$n = p * q = 33 \quad \varphi(n) = (p-1)*(q-1) = 20$$

加密 $C = m^e \bmod n = 5^7 \bmod 33 = 14$

解密 $m = C^{\varphi} \bmod n = 14^3 \bmod 33 = 5$

$$\begin{cases} a = 3 \\ \text{公钥 } KV = \{7, 33\} \end{cases}$$

$$\begin{cases} \text{私钥 } KR = \{3, 33\} \end{cases}$$

b. $p=5; q=11; e=3; M=9$

$$n = p * q = 55 \quad \varphi(n) = 40 \quad e = 3$$

加密 $C = m^e \bmod n = 9^3 \bmod 55 = 14$

解密 $\begin{cases} m = C^{\varphi} \bmod n = 14^{27} \bmod 55 = 9 \\ a = 27 \end{cases}$

$$\begin{cases} \text{公钥 } KV = \{3, 55\} \end{cases}$$

$$\begin{cases} \text{私钥 } KR = \{27, 55\} \end{cases}$$



CS 扫描全能王

3亿人都在用的扫描App

c. $p=7$, $q=11$, $e=17$; $M=8$

$$n = p * q = 77 \quad \phi(n) = (p-1) * (q-1) = 60 \quad e=17$$

加密 $C = m^e \bmod n = 8^{17} \bmod 77 = 57$

解密 $\begin{cases} m = C^d \bmod n = 57^{53} \bmod 77 = 50 \\ d = 53 \end{cases}$

公钥 $KV = \{17, 77\}$

私钥 $KR = \{53, 77\}$

d. $p=11$, $q=13$, $e=11$, $M=7$

$$n = p * q = 143 \quad \phi(n) = (p-1) * (q-1) = 120 \quad e=11$$

加密 $C = m^e \bmod n = 7^{11} \bmod 143 = 106$

解密 $\begin{cases} m = C^d \bmod n = 106^{11} \bmod 143 = 7 \\ d = 11 \end{cases}$

$\therefore KV = \{11, 143\}$

私钥 $KR = \{11, 143\}$



CS 扫描全能王

3亿人都在用的扫描App