**2、设有两条明文：**



**取密钥：**



**1）推导DES加密算法中第一轮及第二轮的子密钥 与 ；**

**2）分别求出明文与经DES第一轮加密后的密文；**

**1）**



2）





**4、**

解：







（3）在中，



同理在中：





(5)在不同的有限域中，相同的多项式的和是相同的，而它们的乘积一般是不同的，相同元素的逆也不一定相同。

**5、**





**8、**

