1）求冒泡排序法的计算复杂度, 该算法是否为多项式的？

2）设 DES 数据加密标准中：

明文 m= 0011 1000 1101 0101 1011 1000 0100 0010 1101 0101 0011 1001 1001 0101 1110 0111

密钥 K= 1010 1011 0011 0100 1000 0110 1001 0100 1101 1001 0111 0011 1010 0010 1101 0011

试求L_1与R_1。

3） 结合 DES 算法，体会混乱、扩散的概念：

选取题目 2）中的明文消息 m 及密钥 K，在以下三种条件下，分别测试轮函数输入改变 1 bit（即任意改变R_0的某一比特），经过 1-6 轮的输出改变情况，与正常的 DES 算法比较，总结 DES 轮函数的混乱、扩散效果。

a) 删除 E 扩散(32-48 填充 0)

b) 删除 S-box(取 S-box 输入的中间 4bit 为输出)

c) 删除 P 置换

4）按照三重 DES 需要的密钥个数，可分为两类，分别为三个密钥和两个密钥，即：（1）$c = E_{k_1}\left(E_{k_2}\left(E_{k_3}(m)\right)\right)$，（2）$c = E_{k_1}\left(D_{k_2}\left(E_{k_1}(m)\right)\right)$。对于这两种三重 DES，分别给出利用中间相遇攻击所需要的时间复杂度及空间复杂度，并说明中间相遇攻击对哪种类型更有效。（提示：针对分组密码算法，一般认为找到比搜索攻击更有效的算法即为有效攻击）