**课堂作业2**

抗碰撞性是指哈希函数的一种特性，涵盖了抗强碰撞性和抗弱碰撞性两个方面。具体来说，抗强碰撞性指的是对于任意给定的消息，寻找另一条消息使得两者的哈希值相同的计算难度很高；而抗弱碰撞性则是指寻找任意两条消息，使它们的哈希值相同的计算难度很高。

哈希函数通常接受任意长度的输入，并输出固定长度的结果。例如，一个输出为 n 位的哈希函数理论上只能产生2n种不同的哈希值。因此，当输入的可能性超过2n时，根据鸽巢原理，必然存在至少两个不同的输入值映射到相同的输出值，即发生碰撞。在实际应用中，尽管存在这种理论上的可能性，抗碰撞性主要指的是在当前计算能力下，发现这样的碰撞对应的计算工作量是不可行的。因此，哈希函数的抗碰撞性并不意味着碰撞的绝对不存在，而是指在实际计算条件下碰撞的概率极低，从而保证了哈希函数在实际使用中的安全性。

**鸽巢原理**，又称抽屉原理或狄利克雷原理，是组合数学中的一个重要原理。该原理的基本形式非常直观：如果你有更多的物品而要将它们放入较少的容器中，至少有一个容器必须包含不止一个物品。更严格地说，鸽巢原理表明，如果n+1个或更多的物体被放入 n 个容器中，那么至少有一个容器包含两个或两个以上的物体。这个原理可以扩展到更一般的情况，即如果将 k \* m + 1 个物体放入 k 个容器中，则至少有一个容器包含至少 m + 1 个物体。