1901210488 时绍森

我在作业中实现了SM4的ECB模式和CBC模式的加解密，首先讲解下两种模式的原理。

### 1.ECB模式

在ECB模式中，将明文分组加密之后的结果直接成为密文分组。当最后一个明文分组的内容小于分组长度时，需要用一些特定的数据进行填充（padding）。使用 ECB 模式加密时，相同的明文分组会转换为相同的密文分组，也就是说，我们可以将其理解为是一个巨大的“明文分组->密文分组”的对应表，因此 ECB 模式也称为电子密码本模式。

ECB模式是所有模式中最简单的一种。ECB的明文分组与密文分组是一一对应的关系，因此，如果明文中存在多个相同的明文分组，则这些明文分组最终都会将被转换为相同的密文分组。这样一来，只要观察一下密文，就可以知道明文中存在怎样的重复组合，并可以以此为线索来破译密码，因此ECB模式是存在风险的。ECB可以在不破坏译密文的情况下操纵明文。如：假如存在主动攻击者Mallory，它能够改变密文分组的顺序。当接收者对密文进行解密时，由于密文分组的顺序被改变了，因此相应的明文分组的顺序也会改变。也就是说，攻击者Mallory无需破译密码就能够操纵明文。

### 2.CBC模式

CBC模式，全称Cipher Block Chaining模式，译为密文分组链接模式，即加密算法的输入是上一个密文分组和下一个明文分组的异或。因为是将上一个密文分组和下一个明文分组的内容混合加密，因此可以避免ECB模式的缺陷。当加密第一个明文分组时，由于不存在上一个密文分组，因此需要准备与分组等长的初始化向量IV，来代替上一个密文分组。

明文分组在加密之前一定会与“前一个密文分组”进行XOR运算，因此即便明文分组1和2的值是相等的，密文分组1和2的值也不一定是相等的。这样ECB模式的缺陷在CBC模式中就不存在了。在CBC模式中，无法单独对一个中间的明文分组进行加密。例如，如果要生成密文分组3，则至少需要凑齐明文分组1、2、3才行。如果密文分组中有一些比特缺失了，即便只缺失了1比特，那么缺失比特的位置之后的密文分组也就全部无法解密了。

对CBC模式的攻击，假设主动攻击者Mallory的目的是通过修改密文来操纵解密后的明文。如果Mallory能够对初始化向量中任意比特进行反转，则解密后得到的明文分组中相应的比特也会被反转。

### 实验过程为：

Sm4加密算法的CBC模式和ECB模式实验的设计思路一致，所有步骤的注释均写在代码里。这里进行简要讲解。

首先下载一张北大logo图标，将.jpeg转换成字节流，在进行SM4加密，得到加密后的字节流，再将该字节流转化为图片，得到加密后的图片。加密之前必须指定128bit（16个字节）的密钥，用于解密时提供，我在程序中默认是1234567812345678

若要解密，将密钥和图片加密后的字节流提供给sm4的解密算法，即可获得加密前的字节流，在转化成图片即可显示原北大logo

CBC模式和ECB模式的一个不同之处在于CBC模式要提供一个IV16字节128位的初始向量，格式为字符格式。程序中为

b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'