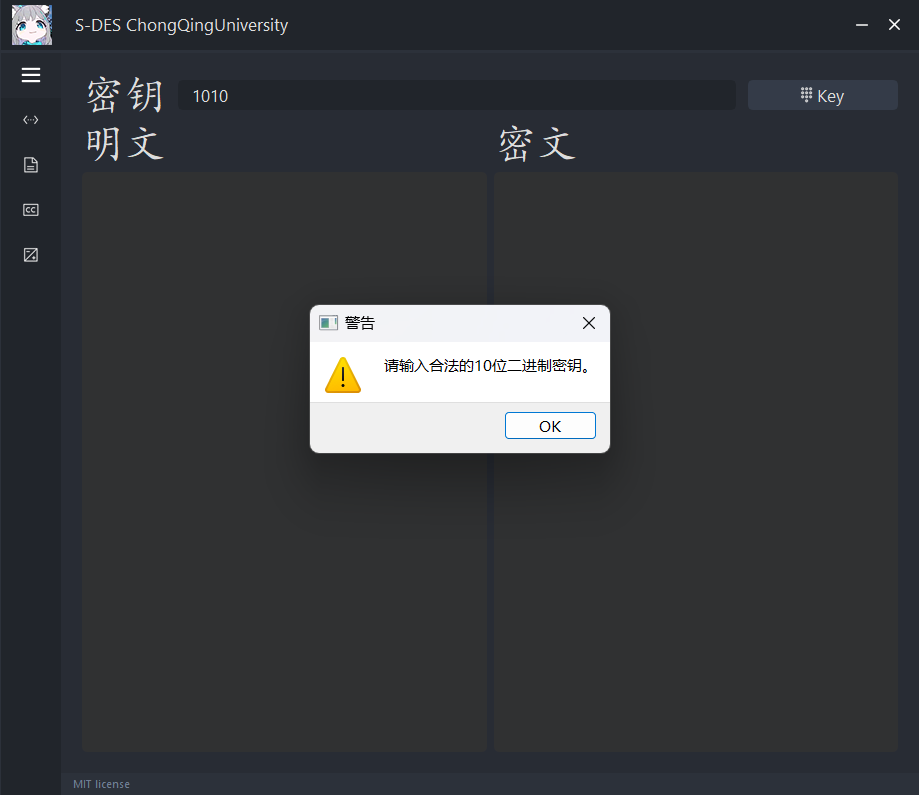
1.基本测试：

根据S-DES算法编写和调试程序，提供**GUI解密**支持用户交互。输入可以是8bit的数据和10bit的密钥，输出是8bit的密文。GUI界面如下所示:



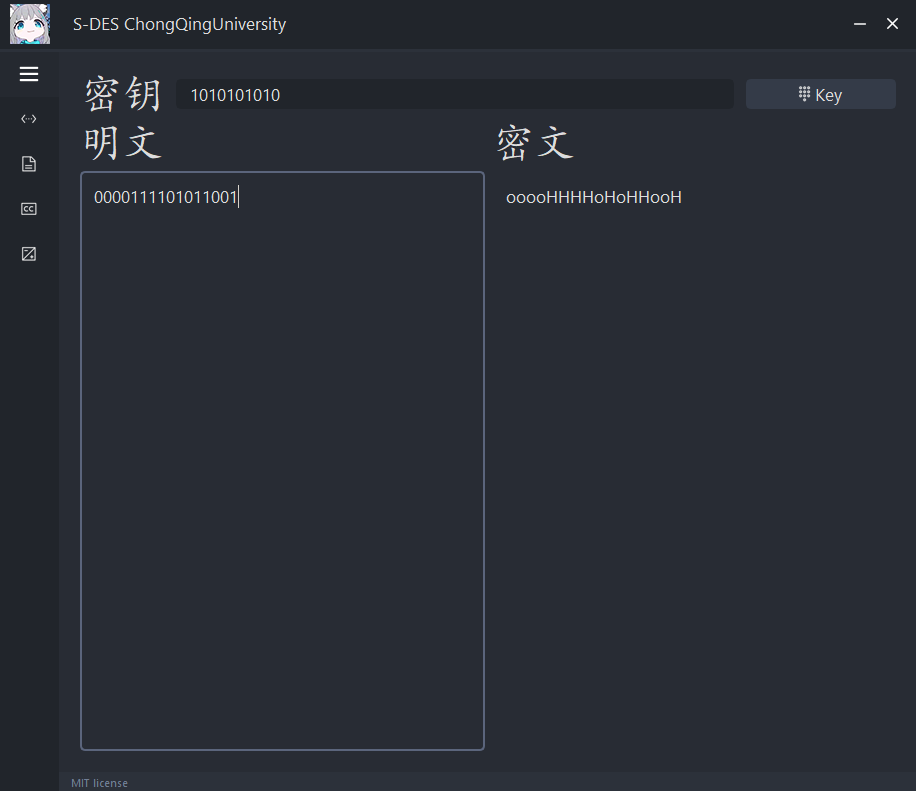
如果密钥的格式不正确(即不是10bit的二进制数)，则会给出如下提醒：



如果输入了合法的密钥，则可以输入明文二进制串，程序会自动将其转化为密文，如下所示：



明文二进制串不限制位数，明文的输入bit数等于密文的输出bit数。

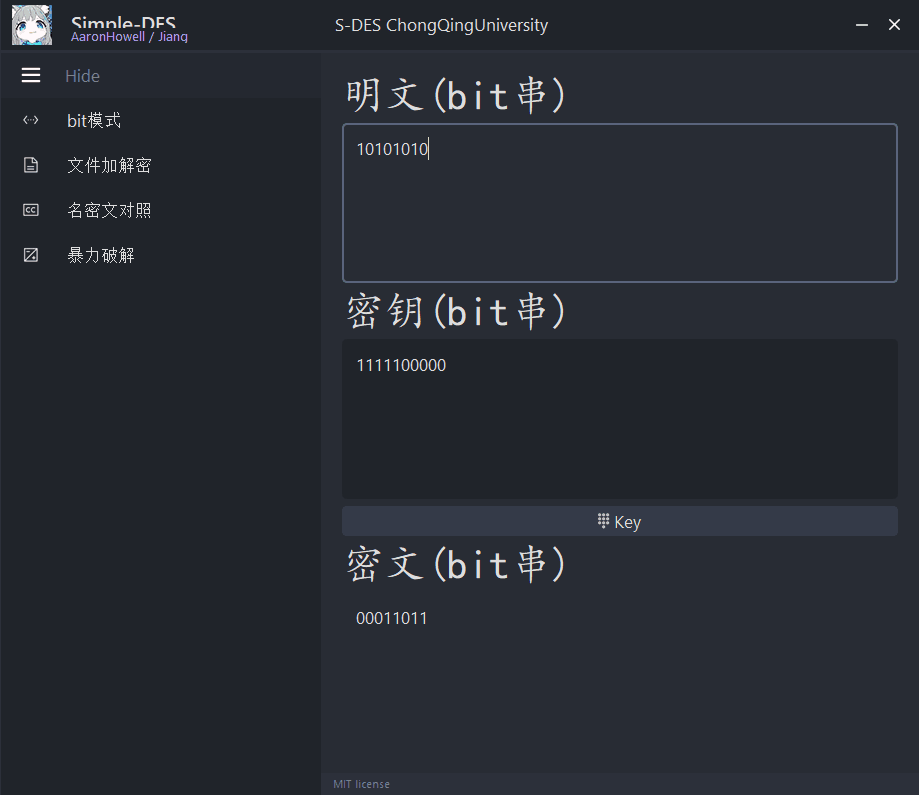


由上可知，本程序提供了**GUI解密**，支持用户交互，要求输入的密钥是10位二进制数，支持输入多位的明文，并自动给出对应的密文。满足基本测试的要求。

2.交叉测试:

考虑到是**算法标准**，所有人在编写程序的时候需要使用相同算法流程和转换单元(P-Box、S-Box等)，以保证算法和程序在异构的系统或平台上都可以正常运行。设有A和B两组位同学(选择相同的密钥K)；则A、B组同学编写的程序对明文P进行加密得到相同的密文C；

采取密钥1111100000.输入明文10101010，两个小组都得到相同的密文00011011

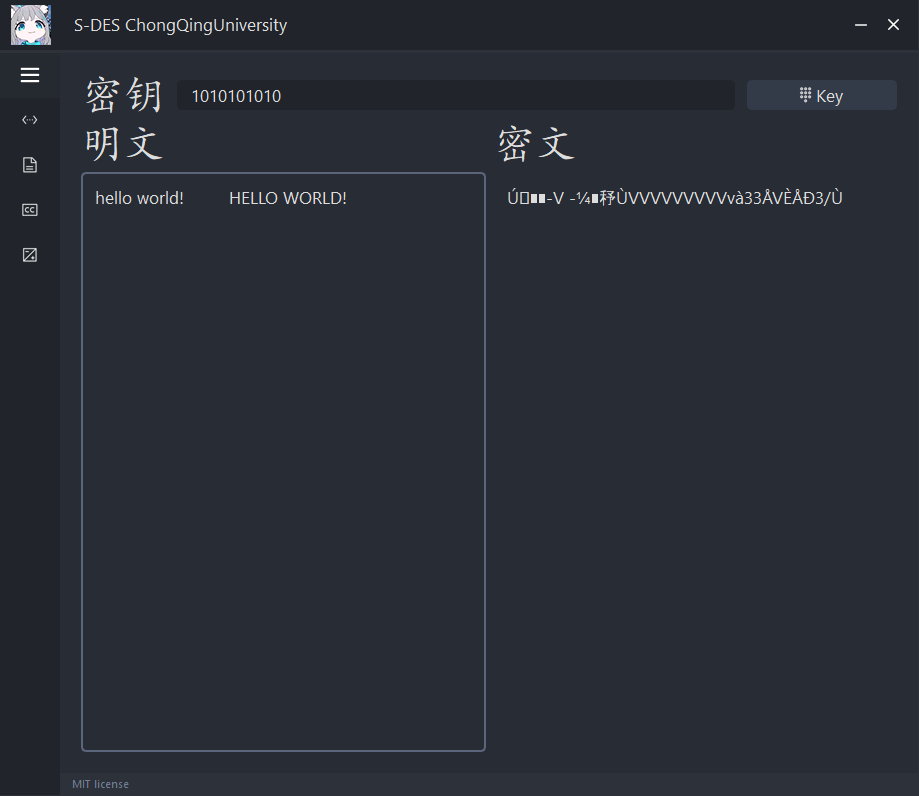




由上可知本程序可以满足交叉测试的功能。

3.扩展功能：

考虑到向实用性扩展，加密算法的数据输入可以是ASII编码字符串(分组为1 Byte)，对应地输出也可以是ACII字符串(很可能是乱码)。



经过测试，本程序可以实现数据输入为ASII编码字符串(字符串的长度不限)，对应的输出是乱码或者ACII字符串。即本程序可以通过扩展功能的测试。

4.暴力破解

暴力破解的GUI如下：



对于以下名密文对，明文：00110101，密文：11001101，密钥1001010011。输入明文：00110101，密文：11001101，线程数量3。得到破解结果如下：



由上图可知，对于随机选择的一对名密文对，存在多个不同的密钥，即会出现密钥碰撞的现象。暴力破解成功。

5.封闭测试

由第四关暴力破解的测试结果可知，对于明密文对，明文：00110101，密文：11001101，有四个不同的密钥1001010011，1010101010，1101010011，1110101010能造成这样的转化。

因此将这四个不同的密钥分别对同一个明文进行加密，观察其对应的密文是否有相同的，若相同，则说明对应明文空间任意给定的明文分组图片，会出现选择不同的密钥图片加密得到相同密文图片的情况。

测试结果如下：

对于不同的密钥1001010011和1101010011，明文输入相同，加密得到相同的密文：





对于不同的密钥1010101010和1110101010，明文输入相同，加密得到相同的密文：





由以上测试结果可知，对应明文空间任意给定的明文分组图片，会出现选择不同的密钥图片加密得到相同密文图片的情况。封闭测试完成。