**第1关：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。

二进制加解密

图形用户界面, 应用程序

描述已自动生成

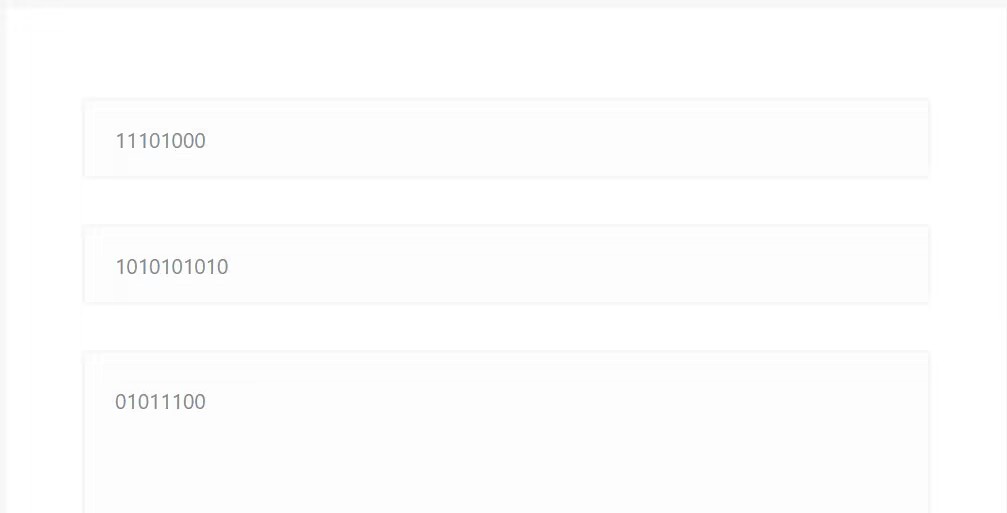


**第2关：交叉测试**

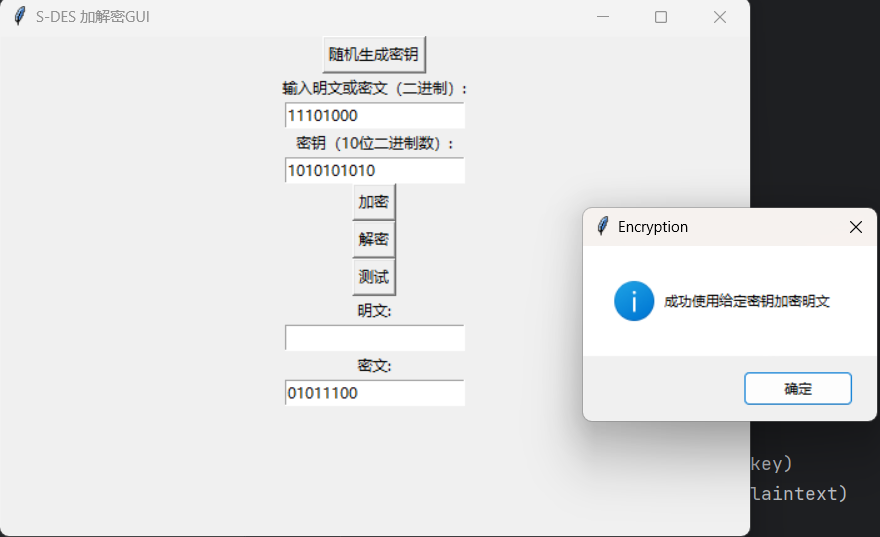
考虑到是**算法标准**，所有人在编写程序的时候需要使用相同算法流程和转换单元(P-Box、S-Box等)，以保证算法和程序在异构的系统或平台上都可以正常运行。

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；或者B组同学接收到A组程序加密的密文C，使用B组程序进行解密可得到与A相同的P。

使用某组同学相应明文与密钥加密：



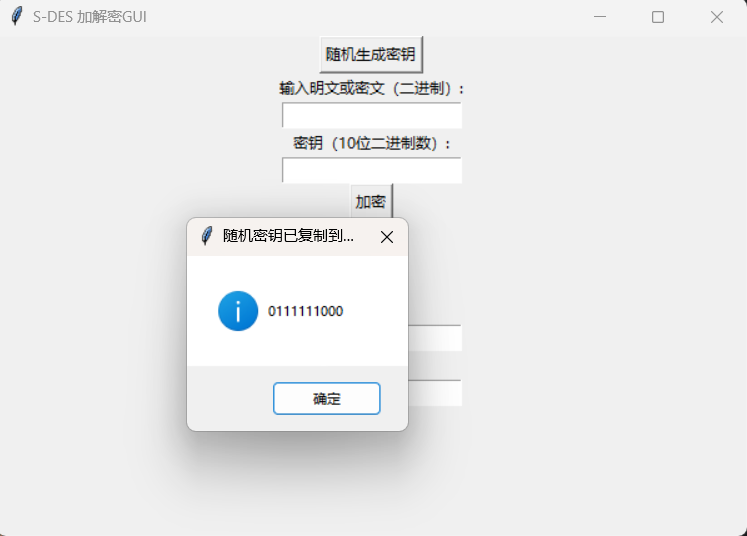
得到相同密文，通过交叉测试



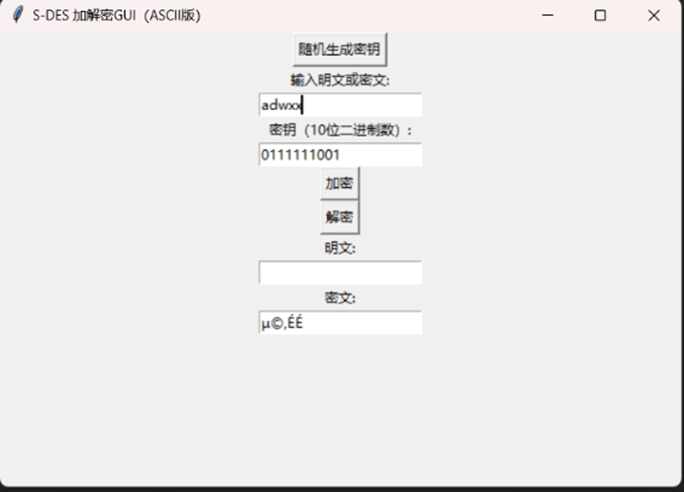
**第3关：扩展功能**

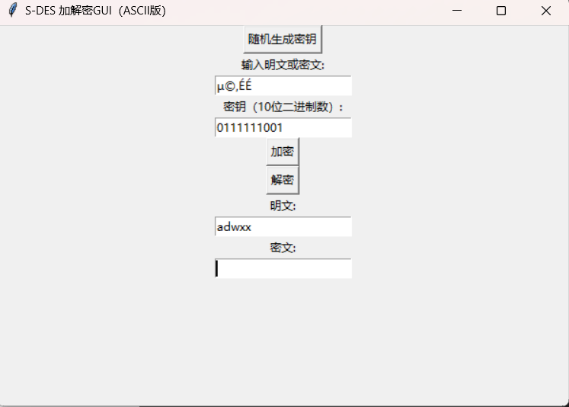
考虑到向实用性扩展，加密算法的数据输入可以是ASII编码字符串(分组为1 Byte)，对应地输出也可以是ACII字符串(很可能是乱码)。

点击顶部按钮随机生成密钥（密钥直接复制到剪切板，如需使用，粘贴到密钥输入框中即可）

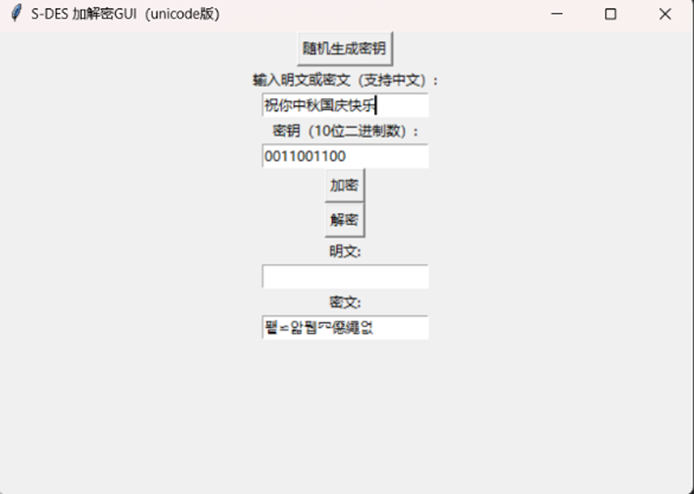


ASCII加解密





中文（UTF-16字符）加解密



图形用户界面, 应用程序

描述已自动生成

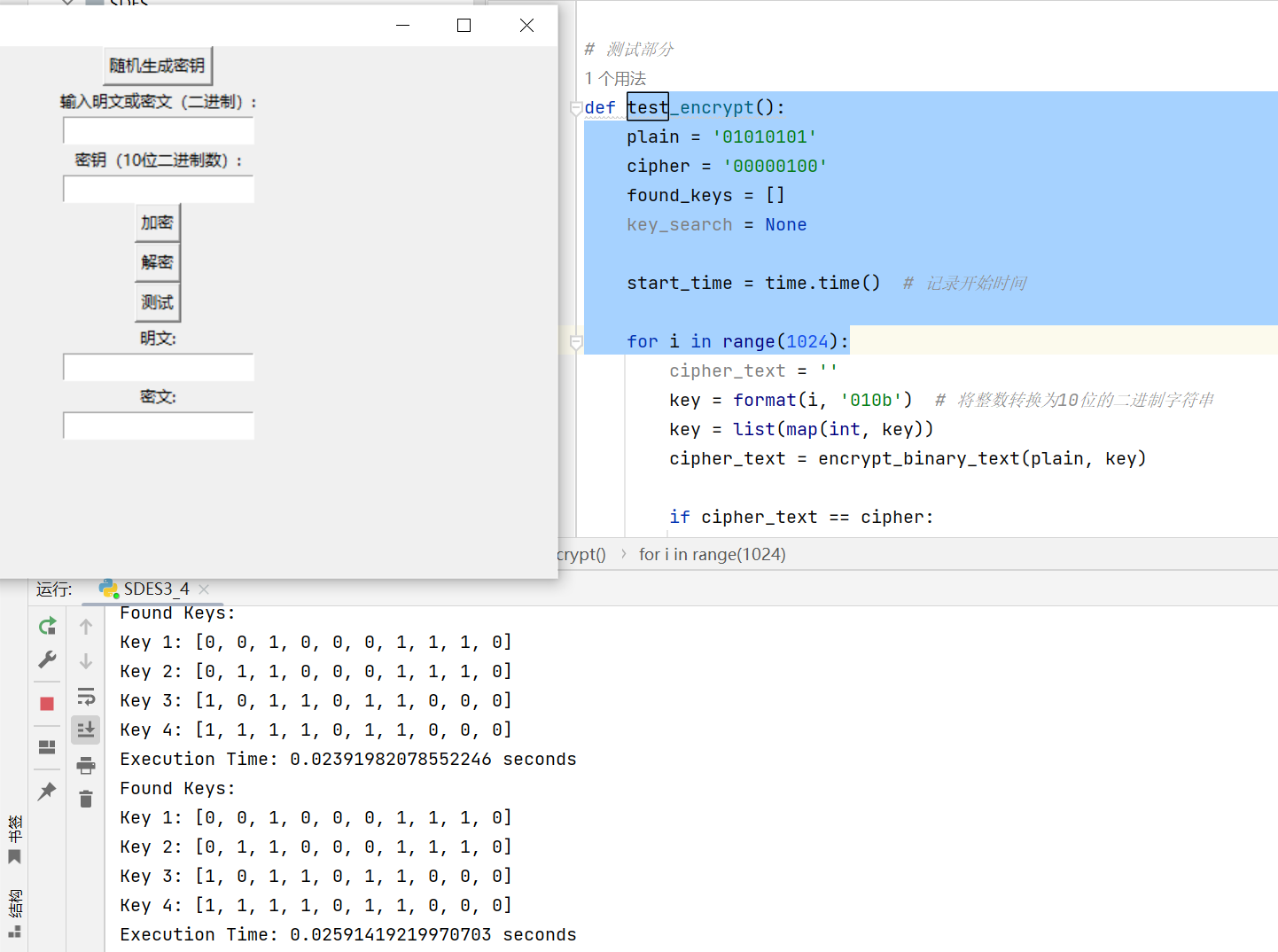
**3.4 第4关：暴力破解**

假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用暴力破解的方法找到正确的密钥Key。在编写程序时，你也可以考虑使用多线程的方式提升破解的效率。请设定时间戳，用视频或动图展示你在多长时间内完成了暴力破解。

&

**3.5 第5关：封闭测试**

根据第4关的结果，进一步分析，对于你随机选择的一个明密文对，是不是有不止一个密钥Key？进一步扩展，对应明文空间任意给定的明文分组P\_{n}，是否会出现选择不同的密钥K\_{i}\ne K\_{j}加密得到相同密文C\_n的情况？



点击测试按钮，可以找到“test\_encrypt”方法中给定的明密文对的所有密钥，并显示验证密钥数量和所花费的时间，具体操作演示可见github项目内的“演示.mp4”文件