#### **1. 引言**

****目的****：该文档的目的在于提供清晰、简洁的说明，帮助用户有效地使用S-AES加解密程序，帮助用户了解软件的主要功能和使用场景，提供逐步的操作指导，使用户能够轻松上手，完成输入、输出和设置等操作。本项目实现了S-AES算法，具备以下基本功能：用户可以通过图形用户界面（GUI）输入16bit的数据和16bit的密钥，输出是16bit的密文；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2 Bytes)，对应地输出也可以是ACII字符串(很可能是乱码)；双重加密：将S-AES算法通过双重加密进行扩展，分组长度仍然是16 bits，但密钥长度为32 bits；中间相遇攻击：假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用中间相遇攻击的方法找到正确的密钥Key(K1+K2)；三重加密：将S-AES算法通过三重加密进行扩展：(1)按照32 bits密钥Key(K1+K2)的模式进行三重加密解密，(2)使用48bits(K1+K2+K3)的模式进行三重加解密；基于S-AES算法，使用密码分组链(CBC)模式对较长的明文消息进行加密。在CBC模式下进行加密，并尝试对密文分组进行替换或修改，然后进行解密。

****目标用户****：信息安全学习者

#### **2. 系统要求**

****硬件要求****：

**最低硬件配置：**

处理器：最低1 GHz单核处理器

内存：至少1 GB RAM

存储：至少100 MB可用硬盘空间

显示：分辨率最低800x600的显示器

**推荐硬件配置：**

处理器：双核处理器或更高

内存：2 GB RAM或更多

存储：至少500 MB可用硬盘空间

显示：分辨率1920x1080的显示器或更高

****软件要求****：

#### ****操作系统：****

#### Windows：Windows 10或更高版本

**依赖库：**

Python：Python 3.10及以上

Qt：Qt 5.12及以上

图形界面库：Tkinter

#### **3. 安装说明**

从官网上下载软件并安装。

#### **4. 功能说明**

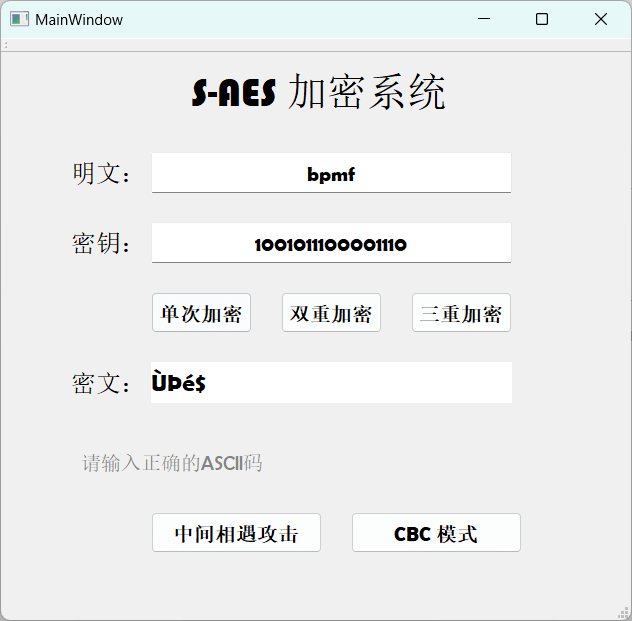
****主要功能****：

1. **基本加解密功能：**

根据S-AES算法编写和调试程序，提供GUI解密支持用户交互。输入是16bit的数据和16bit的密钥，输出是16bit的密文。

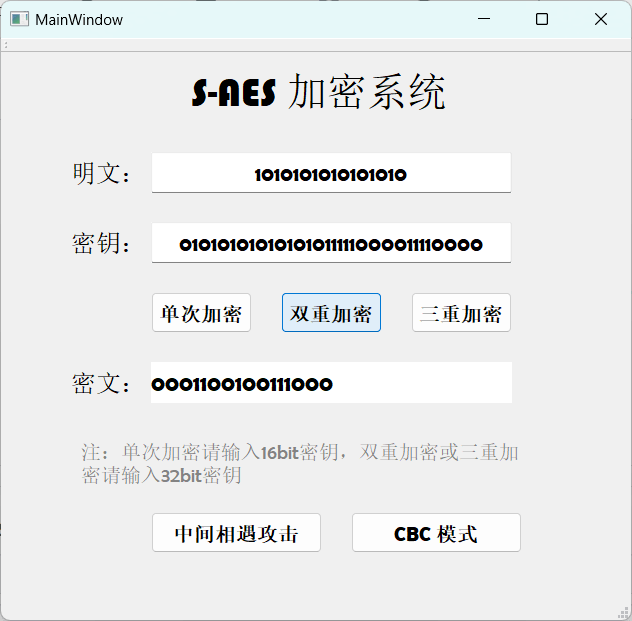
**2. 扩展功能：**

支持输入ASCII编码字符串，用户可以输入任意ASCII字符，程序将其转换为相应的二进制格式进行加解密。

****

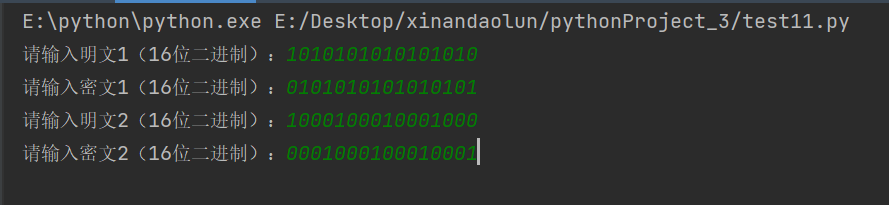
**3.****双重加密：**

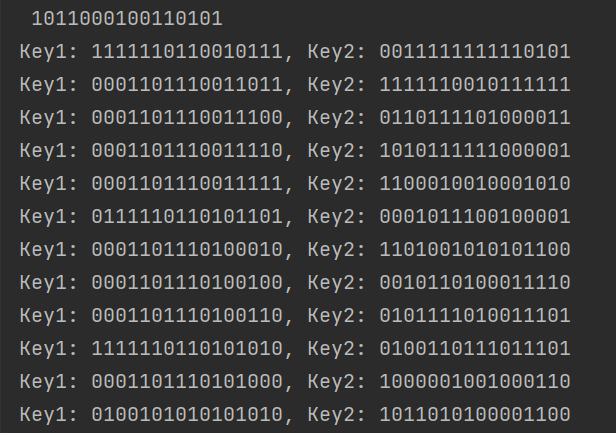
将S-AES算法通过双重加密进行扩展，分组长度仍然是16 bits，但密钥长度为32 bits

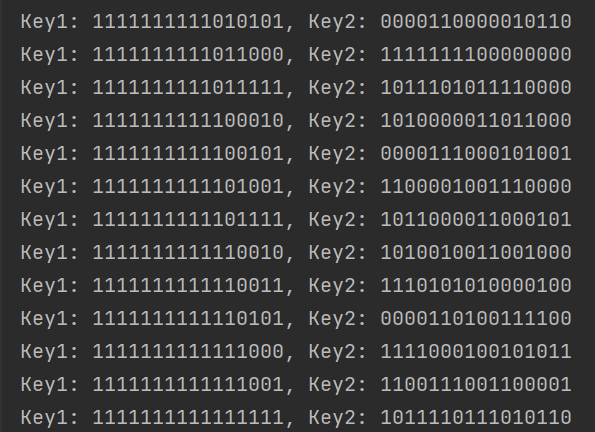


**4.中间相遇攻击：**

假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用中间相遇攻击的方法找到正确的密钥Key(K1+K2)

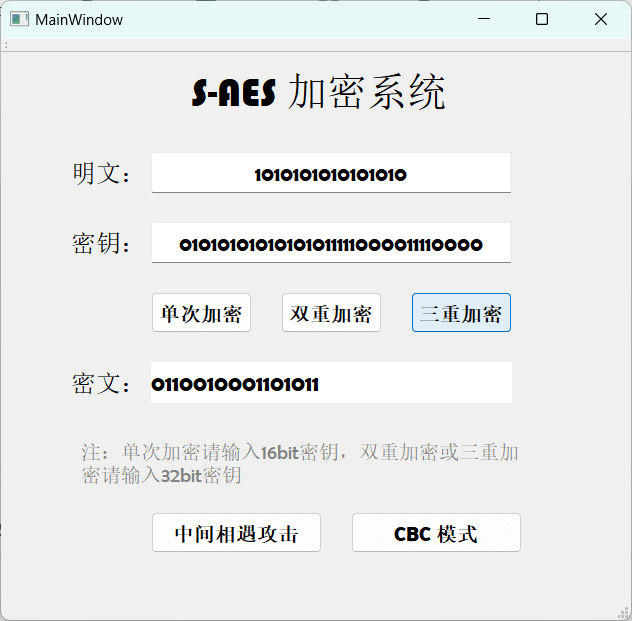






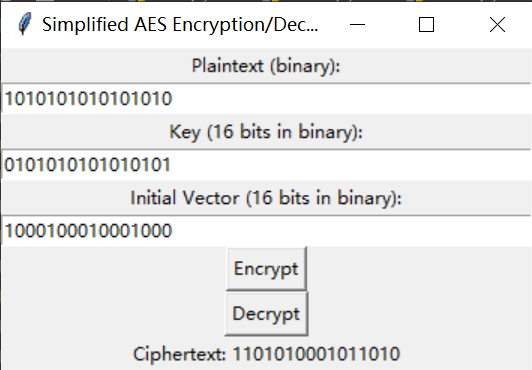
**5.三重加密：**

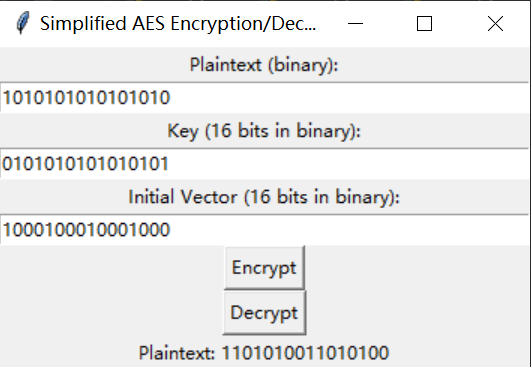
将S-AES算法通过三重加密进行扩展：(1)按照32 bits密钥Key(K1+K2)的模式进行三重加密解密，(2)使用48bits(K1+K2+K3)的模式进行三重加解密



**6.CBC模式：**

基于S-AES算法，使用密码分组链(CBC)模式对较长的明文消息进行加密。在CBC模式下进行加密，并尝试对密文分组进行替换或修改，然后进行解密。





#### **6. 联系方式**

****支持信息****：

电话：13977336796

QQ：2502717432