用户指南

1. 程序运行

运行 UI.py 文件，弹出程序界面；

运行 main.py 文件，实现程序的主要功能，包括二进制加密、解密功能；

运行 extend.py 文件，实现 ascll 码加密、解密功能；

运行 multiple_encryption.py 文件，实现多重加解密和中间相遇攻击；

运行 CBC.py 文件，实现了基于 CBC 模式明文加密、密文解密、密文篡改及结果显示。

2. 界面介绍

UI.py

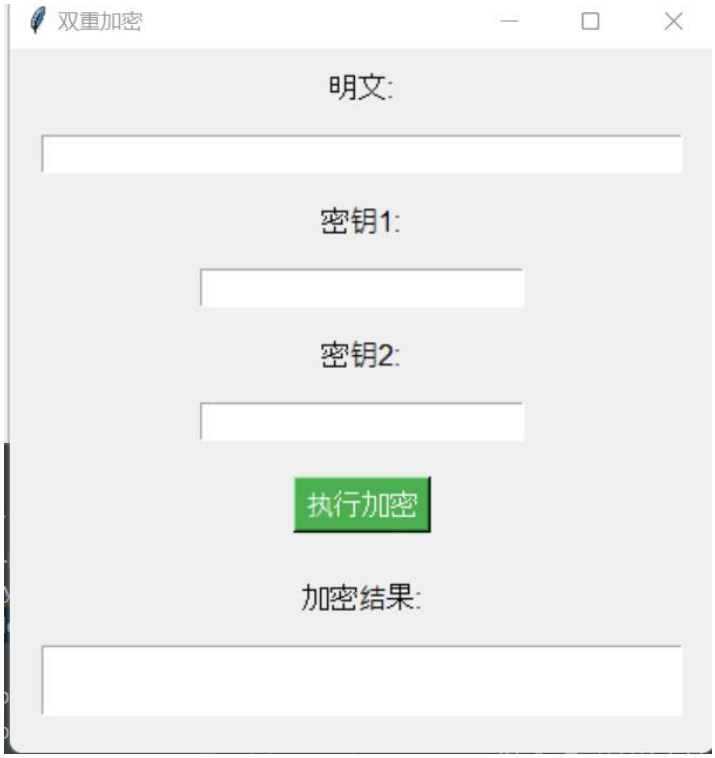
界面包含两个输入框，在明文（or 密文）输入框输入 16bit 二进制明文或者密文，在密钥输入框输入 16bit 密钥，点击加密或解密按钮，可在“输出”框得到加密后的密文或解密后的明文。

明文或密文可选择二进制输入或字符输入，输入明文密文为二进制时，输出的结果也是二进制；输入明文密文为字符串时，输出的结果也是 ascll 字符串。

multiple_encryption.py

主界面可选择双重加密，中间相遇攻击，三重加密三个功能。

双重加密：

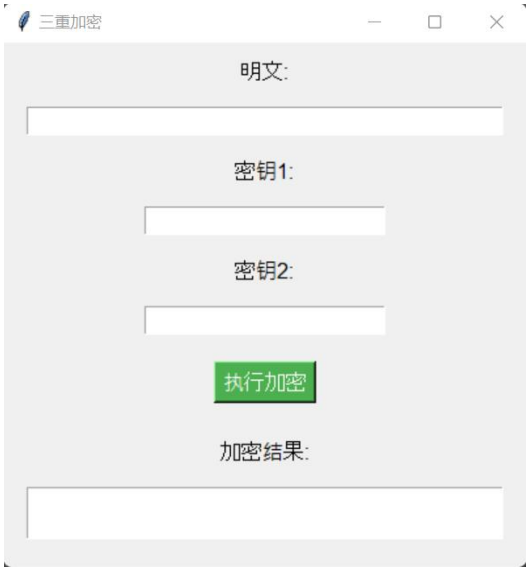


界面包括三个输入框，一个按钮和一个输出框。在明文输入框输入 16bits 二进制的明文，把 32bits 的密钥（分为 16+16）分别输入在密钥 1 输入框和密钥 2 输入框.点击执行加密，在加密结果输出框显示双层加密后的加密结果。

中间相遇攻击：

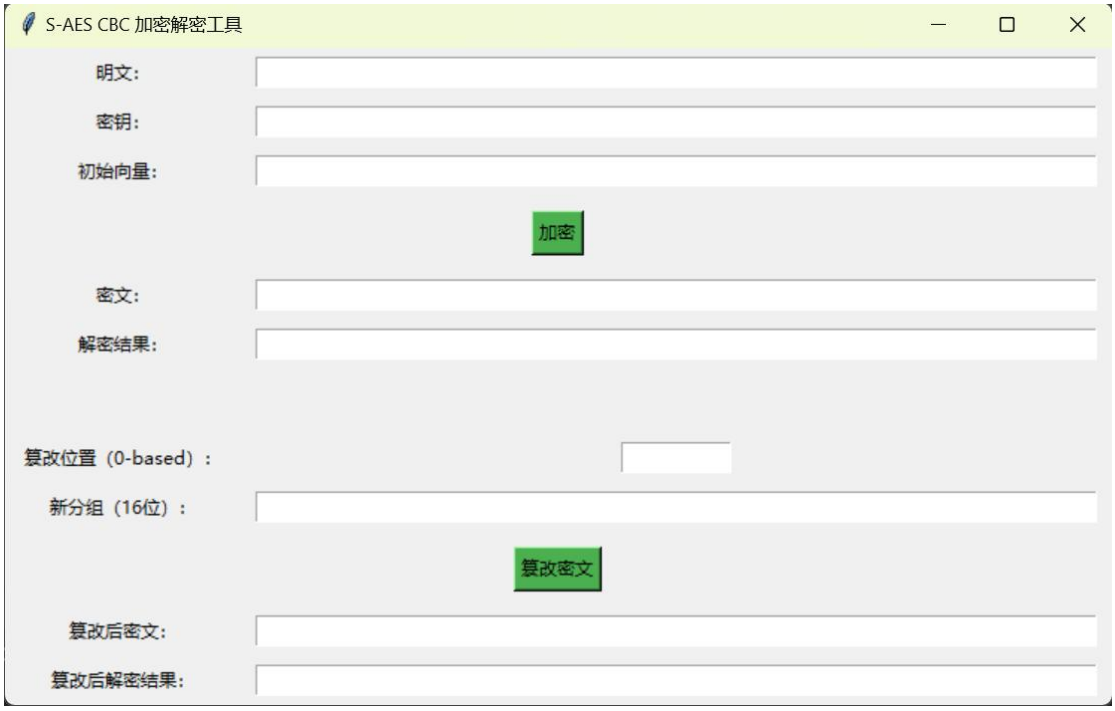
界面包括两个输入框，一个按钮和一个输出框。在已知明文输入框输入明文列表，以逗号分割，每个明文为 16bits 的二进制，在已知密文输入框输入密文列表，以逗号分割，每个密文为 16bits 的二进制。点击执行攻击，在攻击结果输出框破解出的密钥。

三重加密：



界面包括三个输入框，一个按钮和一个输出框。在明文输入框输入 16bits 二进制的明文，把 32bits 的密钥（分为 16+16）分别输入在密钥 1 输入框和密钥 2 输入框，点击执行加密，在加密结果输出框显示双层加密后的加密结果。

CBC.py



界面包括五个输入框，两个按钮和四个输出框。

在明文输入框输入待加密的明文列表，每个明文为 16 位 2 进制，多个明文之间用逗号分隔。在密钥输入框输入 16 位 2 进制密钥。在初始向量输入框输入 16 位 2 进制初始向量。点击加密按钮，程序将对输入的明文列表进行加密，并显示加密后的密文列表和解密后的明文列表，同时判断加密解密是否成功（成功则显示“密码分组链模式加密解密成功”，失败则显示“密码分组链模式加密解密失败”）。

在篡改位置（0-based）输入框输入要篡改的密文分组的位置（从 0 开始计数），在新分组（16 位）输入框输入新的 16 位 2 进制密文分组。点击篡改密文按钮后，程序将替换指定位置的密文分组，并显示篡改后的密文列表和解密后的明文列表。