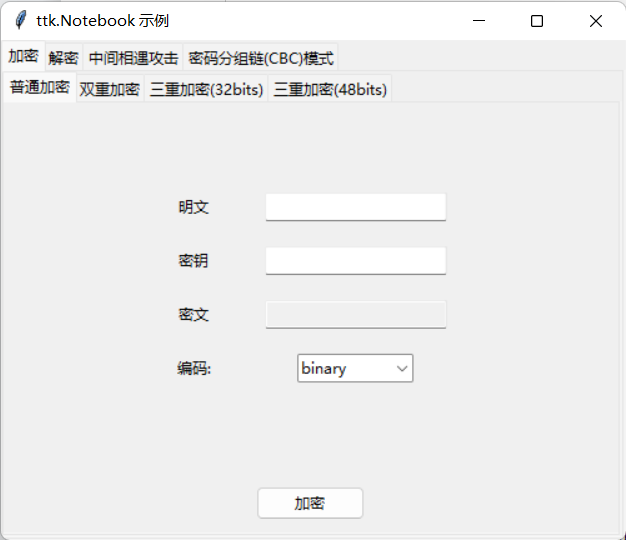
# S-AES用户指南

#### 基本操作

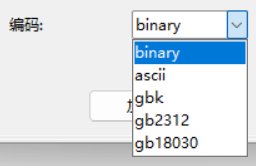
从main文件夹中的S-AES.exe启动界面。



选择解密、加密、中间相遇攻击、密码分组链(CBC)模式4个功能。



在加密和解密功能中，可通过下拉框选择binary，ascii，gbk，gb2312，gb18030五种编码。在中间相遇攻击和密码分组链(CBC)模式中，仅支持二进制编码(binary)。



在明文或密文中按对应的编码格式输入。

binary编码，输入十六进制字符，字符串长度限制为4的倍数。



ascii，gbk，gb2312，gb18030编码，输入任意长度字符串，要求对应编码支持该字符。ascii支持ASCII字符，gb2312支持通用汉字字符，gbk支持绝大多数汉字字符，gb18030支持少数民族字符。ᠠᠡᠢᠣ ᠤᠥ ᠦᠧ



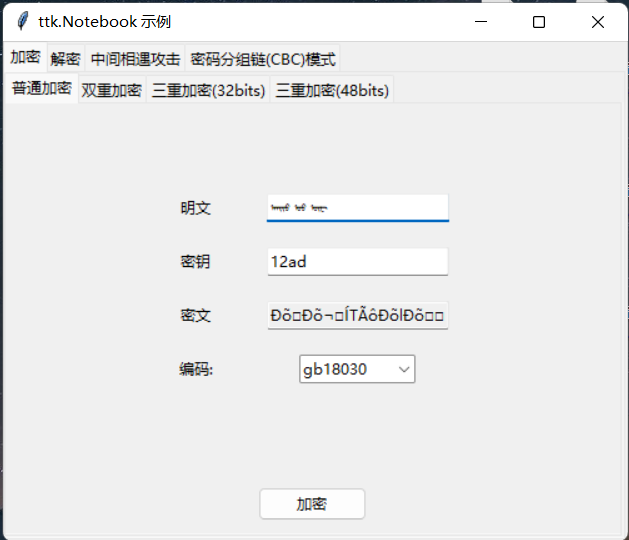
在密钥或初始向量中输入4位十六进制字符。



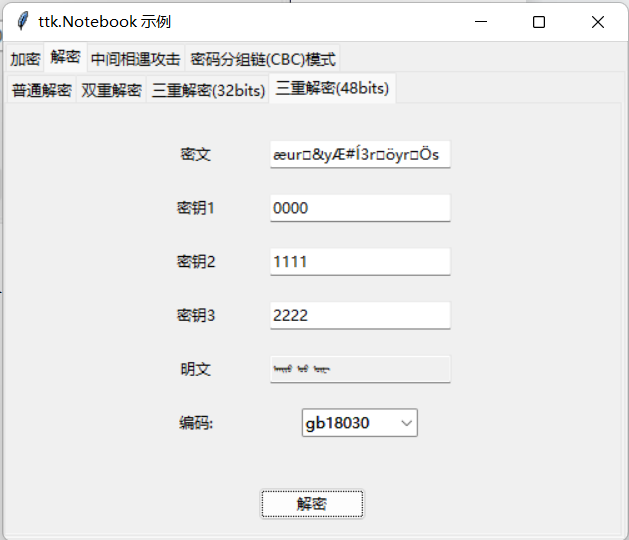
每项功能只需输入可编辑的输入框，点击按钮，在不可编辑的输入框显示结果。

#### 功能

1.加密将明文通过密钥加密成密文，可以选择普通加密，双重加密，三重加密(32bits)，三重加密(48bits)四种模式。

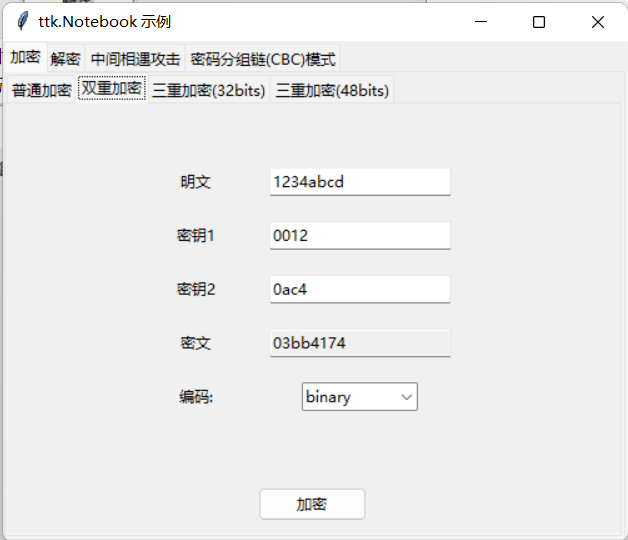


2.解密将密文通过密钥解密成明文，可以选择普通解密，双重解密，三重解密(32bits)，三重解密(48bits)四种模式。

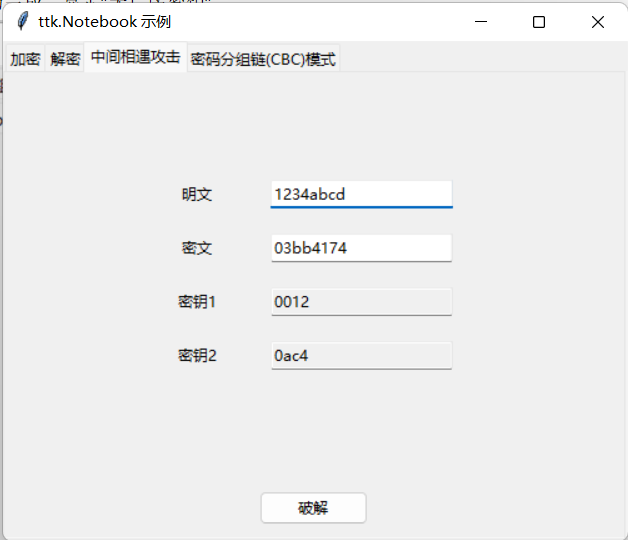


3.中间相遇攻击通过明密文对来破解双重加密，来获取两个密钥，每次点击破解返回一个结果，在显示所有结果后则遍历完成，显示”无后序密钥”，运行可能较慢。

双重加密

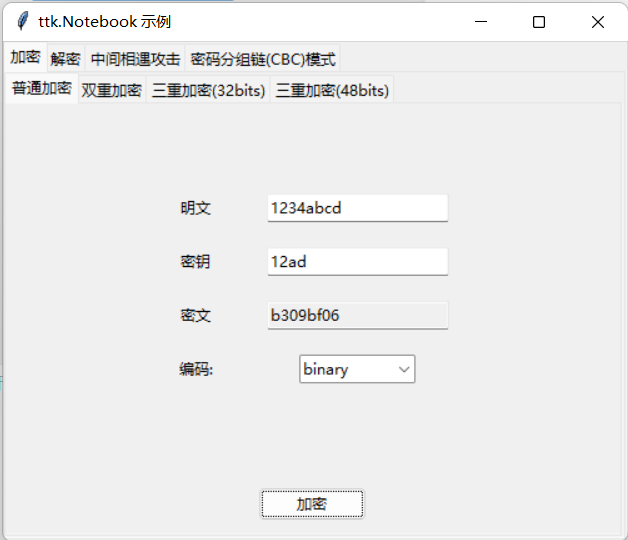


中间相遇攻击



4.密码分组链(CBC)模式相较于普通加密解密，添加了初始向量，对明密文对进行了混淆。

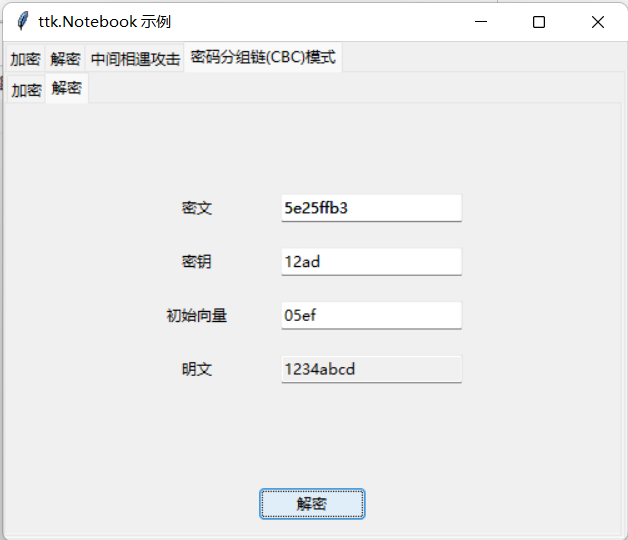
普通加密



CBC加密

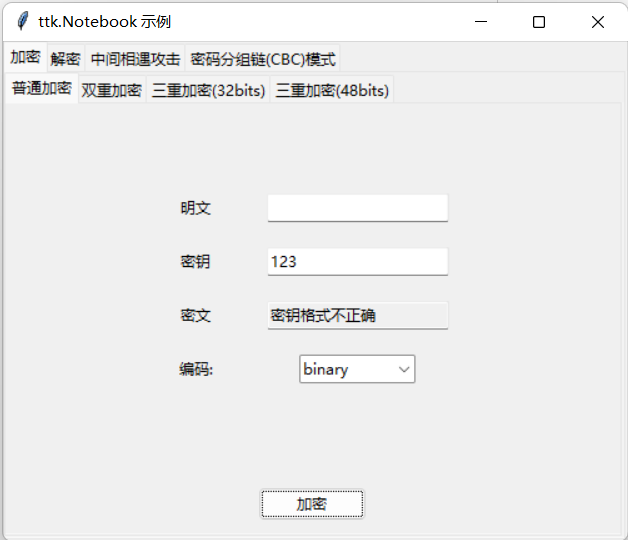


CBC解密

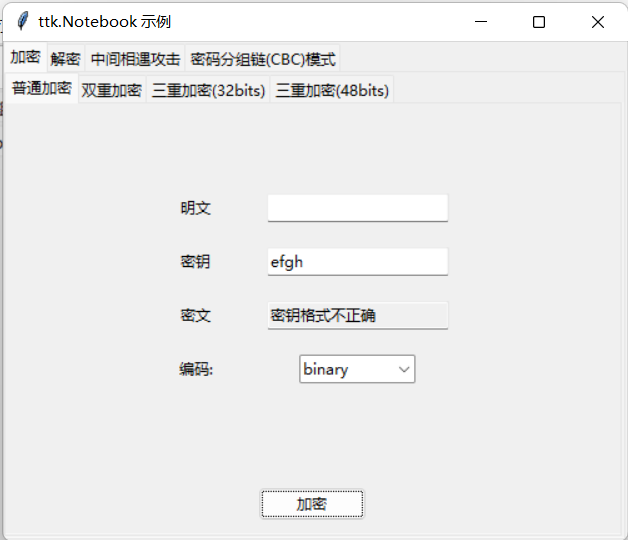


#### 报错

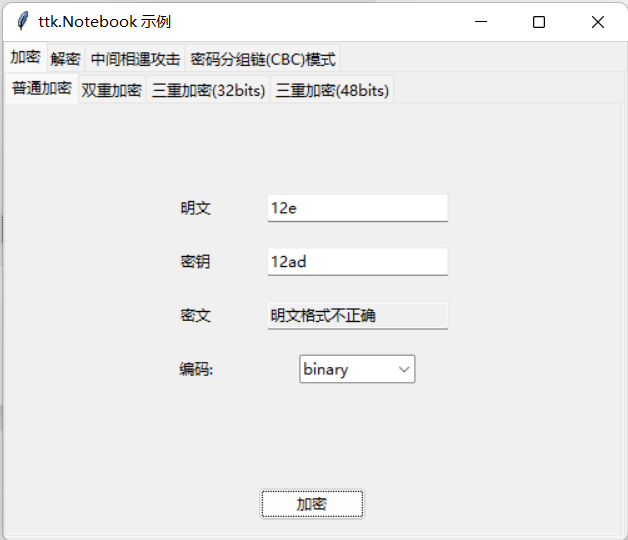
密钥和初始向量位数必须为4位



密钥和初始向量必须为十六进制字符



binary编码明密文位数必须为4及4的倍数位



明密文必须为对应编码支持的字符

