第 1 关：基本测试

1. 要求根据 S-AES 算法编写和调试程序，提供了 GUI 解密支持用户交互。输入可以是 16bit 的数据和 16bit 的密钥，输出是 16bit 的密文。

2.运行加密窗口文件，在明文框中输入 16bit 二进制明文，选择 1 轮加密、二进制输入后点击加密按钮即可，得到随机生成的 16bit 密钥和密文

图 1-1 一轮二进制加密

3. 运行解密窗口文件，在密文框及密钥框输入图 1-1 中的值，再点击解密按钮得到明文，明文与图 1-1 输入一致

图 1-2 一轮二进制解密

第 2 关：交叉测试

1. 与许哲凯小组进行交叉测试，许哲凯小组输入明文和密钥后得到密文，利用本小组算法得到相同的明文，与预期结果一致

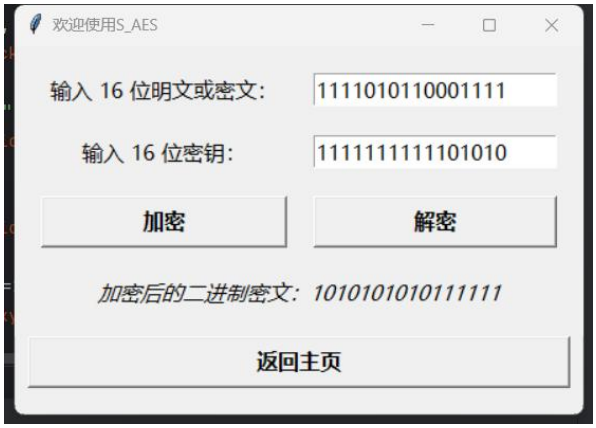

图 2-1 许哲凯小组加密结果

图 2-2 本算法解密结果

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 2 Bytes)，对应地输出也可以是 ACII 字符串(很可能是乱码)。

1. 输入 ASCII 值进行加密时选择 ASCII 输入/输出即可，解密结果与加密输入保持一致，如图 3-1 和图 3-2

图 3-1 一轮 ASCII 加密

图 3-2 一轮 ASCII 解密

第 4 关：多重加密

1.双重加密

（1）二进制双重加密：选择 2 轮加密后输入明文得到密文，同理选择 2 轮解密得到明文与输入保持一致

图 4-1-1 二进制双重加密

图 4-1-2 二进制双重解密

（2）输入 ASCII 时采取同样的操作得到结果与预期一致

图 4-1-3 ASCII 双重加密

图 4-1-4 ASCII 双重解密

2.中间相遇攻击

找到使用相同密钥的明、密文对，使用中间相遇攻击的方法找到正确的密钥 Key(K1+K2)。

```
正在处理明密文对1
正在处理明密文对2
正在查找匹配密钥
找到相同的数组: [1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0]
找到相同的数组: [0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0]
已与地址为 ''127.0.0.1:54769', 传输: '套接字'' 的目标虚拟机断开连接
```

图 4-2 相遇攻击结果

3.将 S-AES 算法通过三重加密进行扩展，按照 32 bits 密钥 Key(K1+K2)的模式进行三重加密解密，解密结果与预期结果均一致

（1）二进制三重加密：

图 3-1-1 二进制三重加密

图 3-1-2 二进制三重解密

（2）ASCII 三重加密：

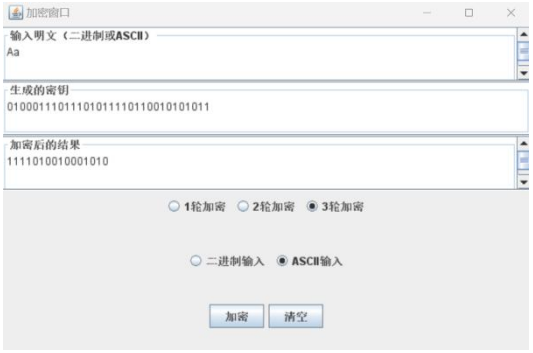

图 3-2-1 ASCII 三重加密

图 3-2-2 ASCII 三重解密

第 5 关：工作模式

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。

（1）CBC 模式进行加密

```
已连接到地址为 ''127.0.0.1:54790', 传输: '套接字'' 的目标虚拟机
密文 =
01010111010100100001000101010010010101111111100000111010111000011
密钥 =
0010010001000000
IV =
0010110101101111
明文 = yyhyyds
```

（2）CBC 模式下进行解密与预期一致

图 5-2 CBC 模式解密

（3）对密文分组进行替换或修改，然后进行解密，得到结果发现只有中间一部分被篡改

图 5-3 替换明文后解密