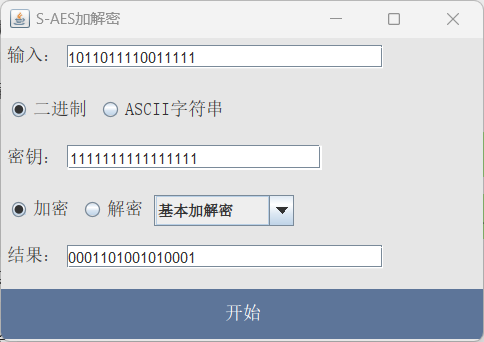
**测试结果**

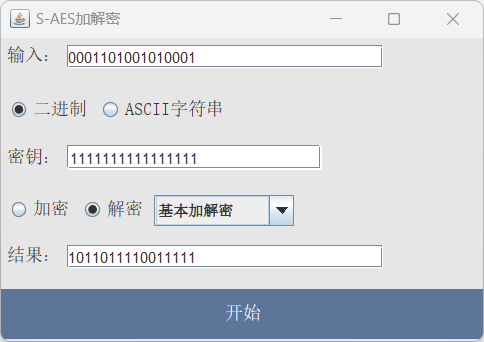
**第1关：基本测试**

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

例如对以下数据对进行加解密基本测试，所得结果符合预期。

|  |  |  |
| --- | --- | --- |
| 明文 | 密钥 | 密文 |
| 1011011110011111 | 1111111111111111 | 0001101001010001 |





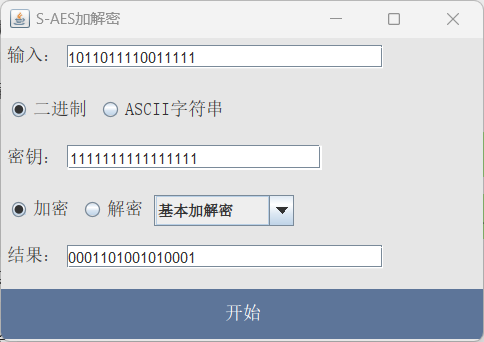
**第2关：交叉测试**

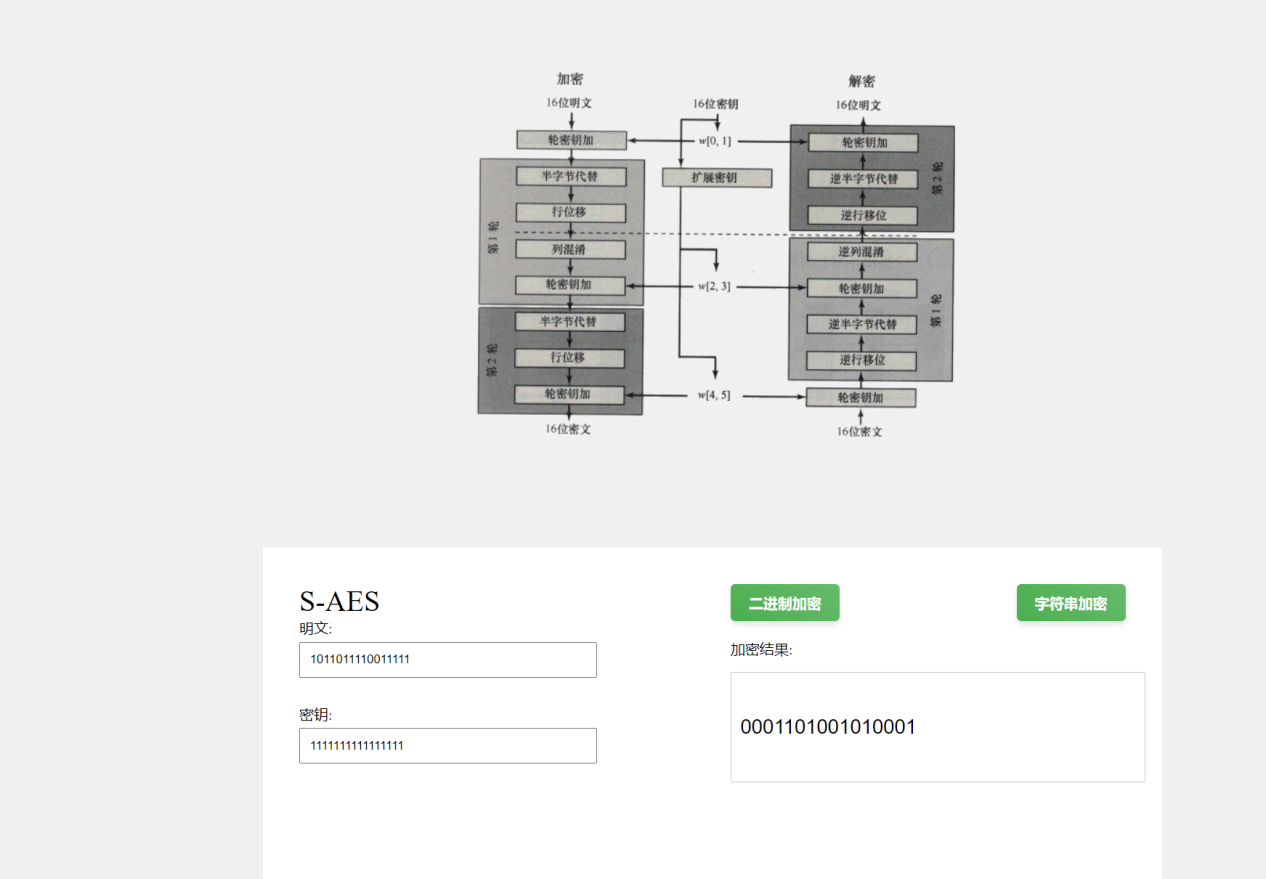
考虑到是"**算法标准"**，所有人在编写程序的时候需要使用相同算法流程和转换单元(替换盒、列混淆矩阵等)，以保证算法和程序在异构的系统或平台上都可以正常运行。

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。

选择如下明文和密钥进行交叉测试：

|  |  |
| --- | --- |
| 明文 | 密钥 |
| 1011011110011111 | 1111111111111111 |





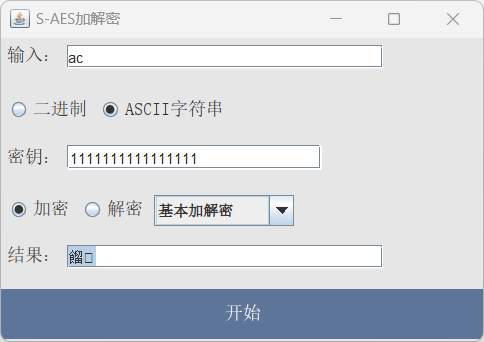
两组程序生成的密文相同，均为0001101001010001，交叉测试通过。

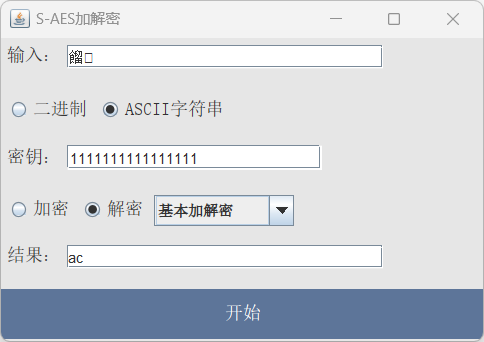
**第3关：扩展功能**

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)。

例如对以下数据对进行ASCII加解密测试。

|  |  |  |
| --- | --- | --- |
| 明文 | 密钥 | 密文 |
| ac | 1111111111111111 | 餾줻 |





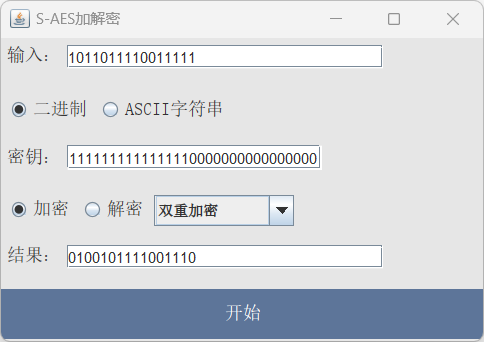
**第4关：多重加密**

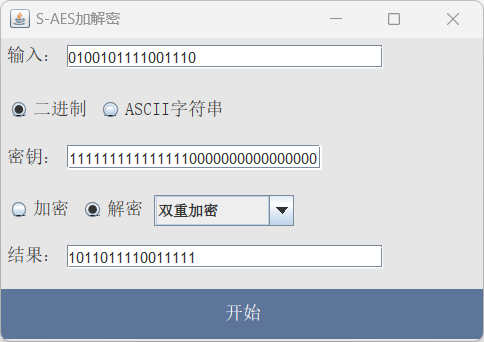
**4.1双重加密**

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。

例如对以下数据对进行双重加解密基本测试，所得结果符合预期。

|  |  |  |
| --- | --- | --- |
| 明文 | 密钥 | 密文 |
| 1011011110011111 | 11111111111111110000000000000000 | 0100101111001110 |





**4.2 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)。

例如明密文对为1个：

|  |  |
| --- | --- |
| 明文 | 密文 |
| 1011011110011111 | 0100101111001110 |

查找到：

|  |  |
| --- | --- |
| key1 | key2 |
| 1001011111111111 | 0110001111010010 |
| 0110101111111111 | 1001000101001101 |
| 1001101111111111 | 0111010100001010 |
| 1001101111111111 | 1000111101111011 |



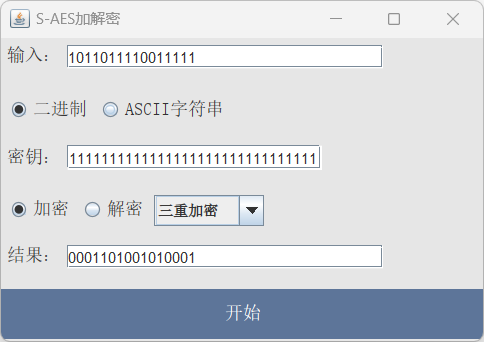
**4.3 三重加密**

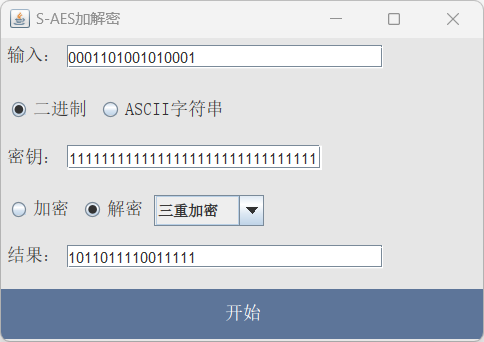
将S-AES算法通过三重加密进行扩展.

选择(2)使用48bits(K1+K2+K3)的模式进行三重加解密。

例如对以下数据对进行三重加解密基本测试，所得结果符合预期。

|  |  |  |
| --- | --- | --- |
| 明文 | 密钥 | 密文 |
| 1011011110011111 | 11111111111111111111111111111111  1111111111111111 | 0001101001010001 |





**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。注意初始向量(16 bits) 的生成，并需要加解密双方共享。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，请对比篡改密文前后的解密结果。

例如对以下数据对进行CBC加解密基本测试,明文为16bit，初始向量为1110010010011001。

|  |  |  |
| --- | --- | --- |
| 明文 | 密钥 | 密文 |
| 1011011110011111 | 1111111111111111 | 0000001001111000 |





修改密文0000001001111000的前四位为1111：

|  |  |  |
| --- | --- | --- |
| 密文 | 密钥 | 明文 |
| 1111001001111000 | 1111111111111111 | 0000011110010011 |



解密得明文由1011011110011111变为0000011110010011