第1关：基本测试

输入密钥是1010101010101010，明文是1010101010101010，

加密后密文是1010111110111000。

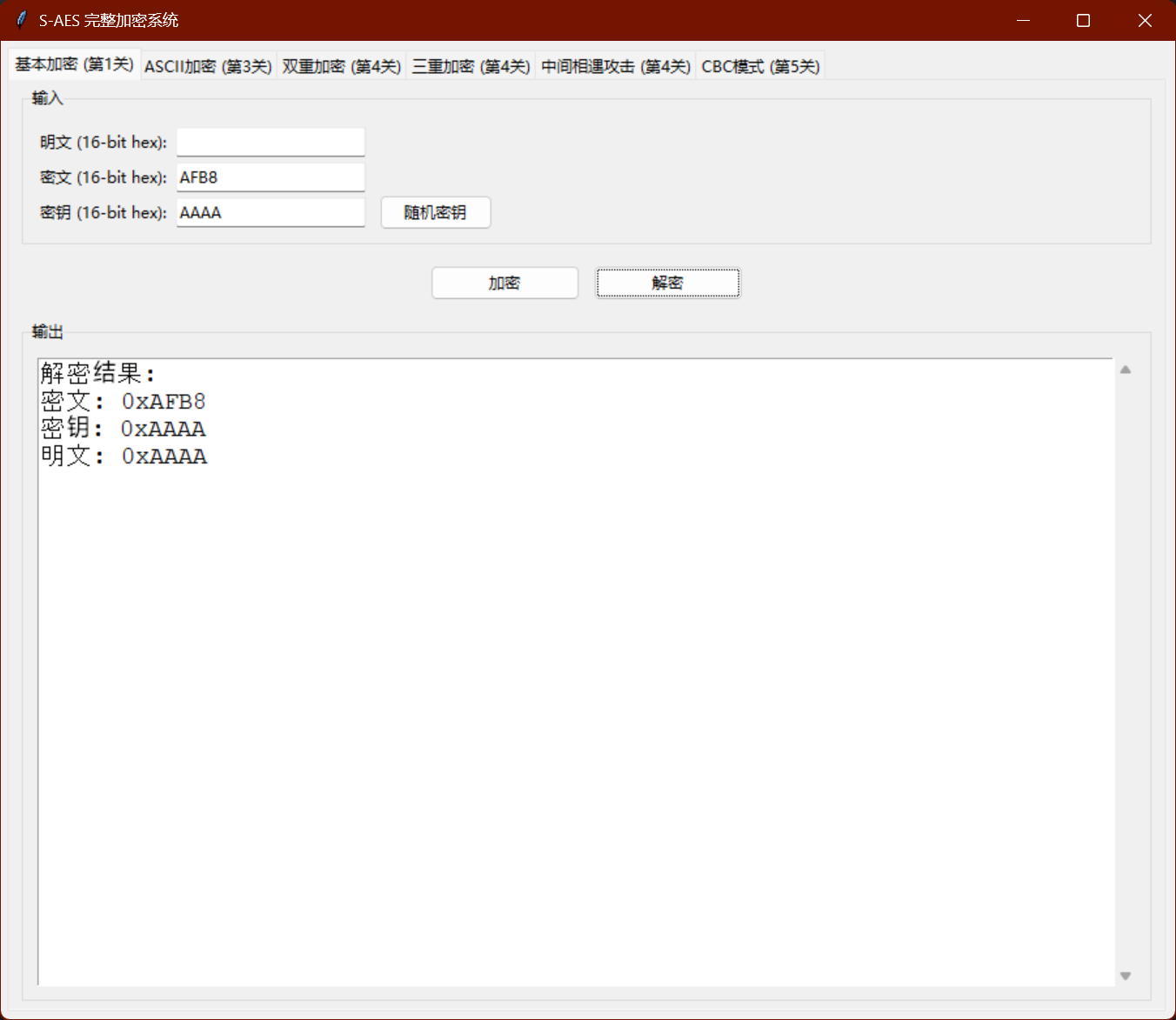






第2关：交叉测试

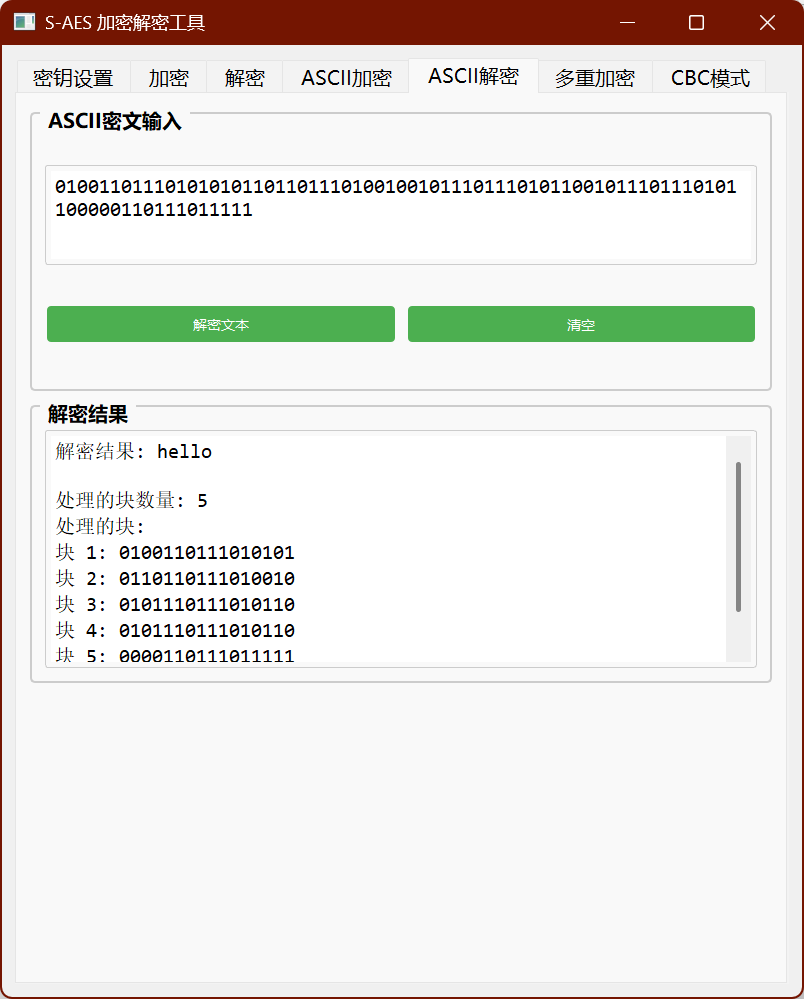
用其他小组的算法，输入第一关的密文和密钥，解密出的明文相同，十六进制表示为0xAAAA



第3关：扩展功能

明文是hello，加密后是五个16位的二进制密文块，解密后明文对应上了。





第4关：多重加密

多重加解密的效果如下。

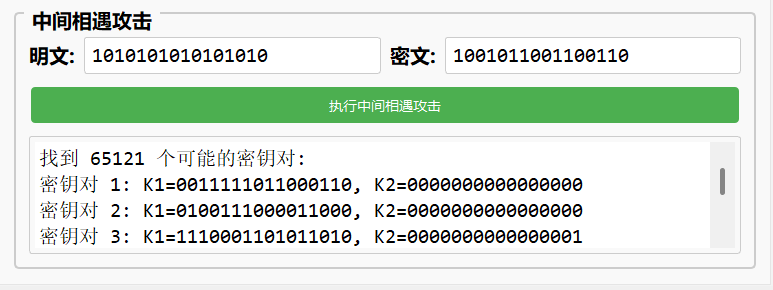
例如双重加密中，密钥是0xAAAAAAAA,明文是0xAAAA,密文是0x9666,

解密后能够对上。





使用中间相遇攻击对上面二重加密的明密文对进行破解，能够找到数万个可能的密钥对。



第5关：工作模式

使用CBC模式加解密，初始向量一致，密钥依旧是0xAAAA，明文是0xAAAAAAAAAAAA，针对每16位明文都生成16位密文块，解密结果也能对的上。

