**3.1 第1关：基本测试**

验证 16 位数据块的 S-AES 标准加解密功能



**3.2 第2关：交叉测试**

标准测试



边界值测试



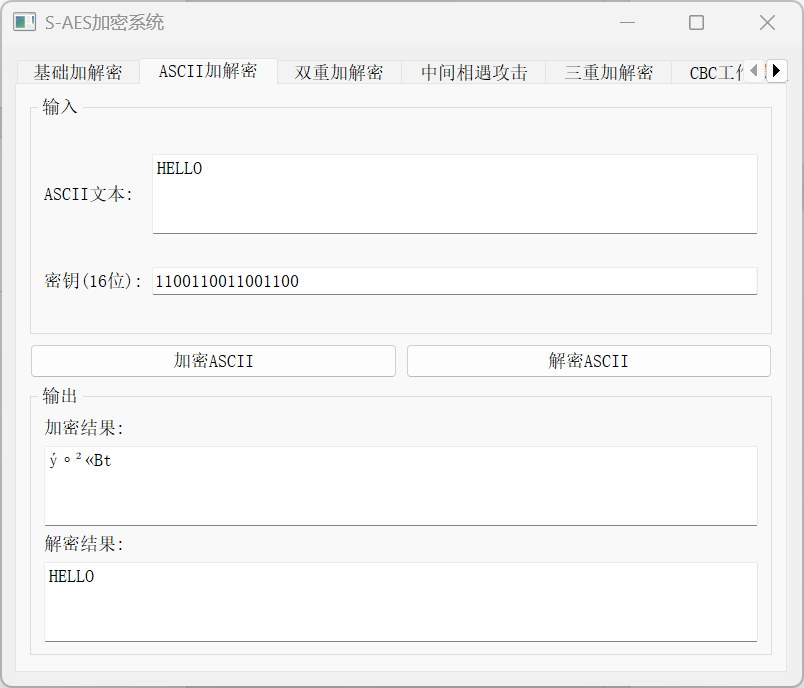
随机值测试



**3.3 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)。





**3.4 第4关：多重加密**

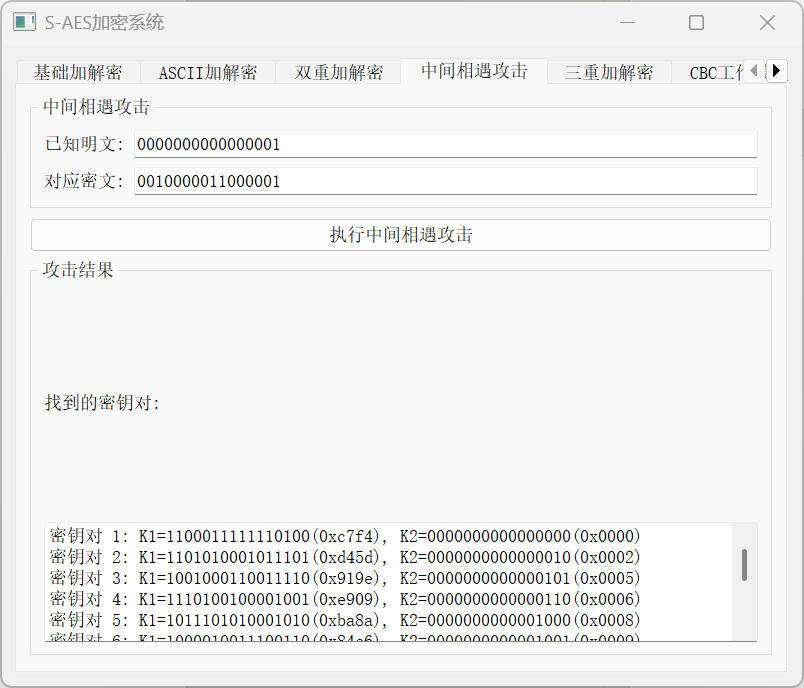
3.4.1 双重加密

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。



3.4.2 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)。



密钥对1符合3.4.1

3.4.3 三重加密

将S-AES算法通过三重加密进行扩展

使用48bits(K1+K2+K3)的模式进行三重加解密。



**3.5 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。

