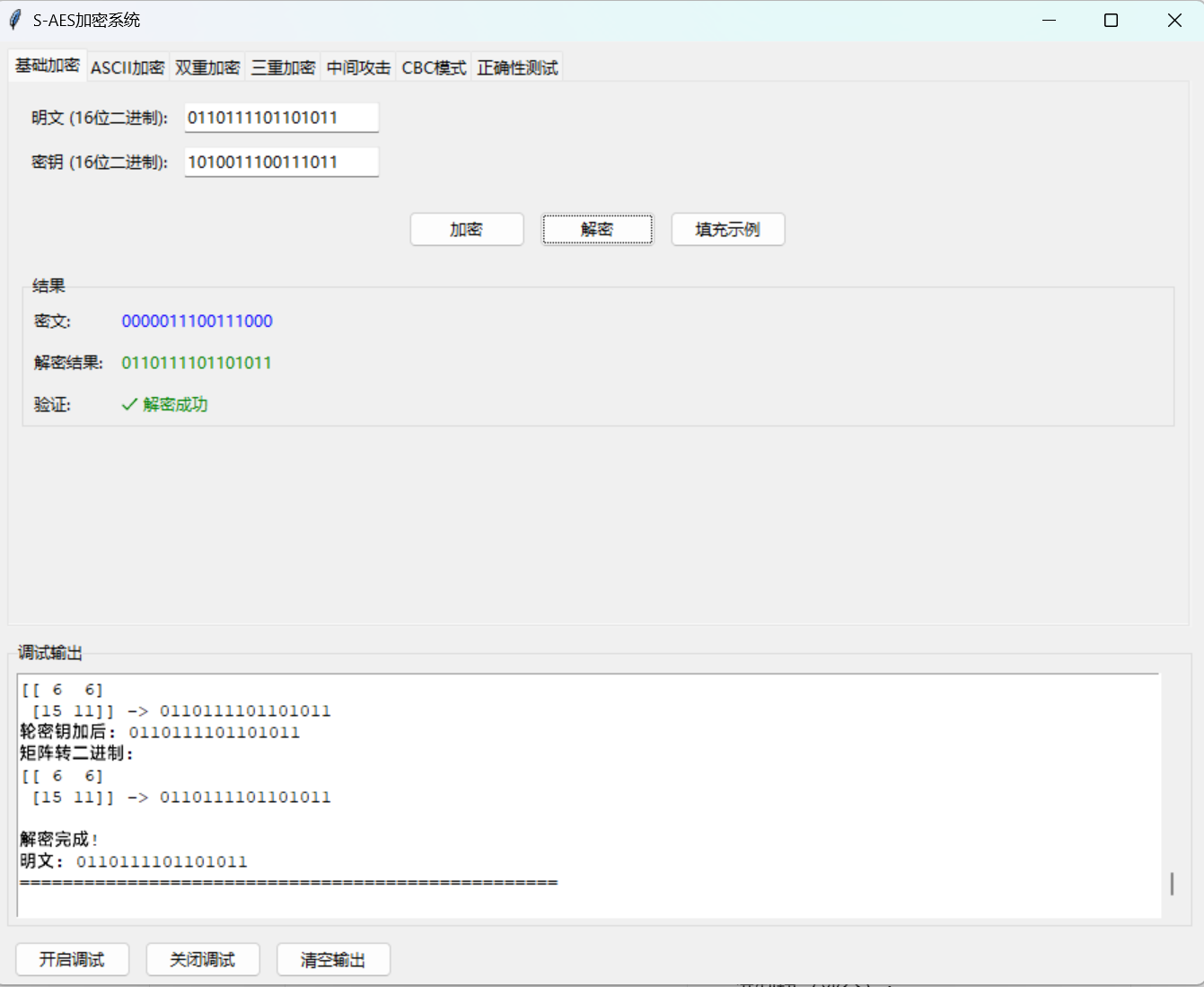
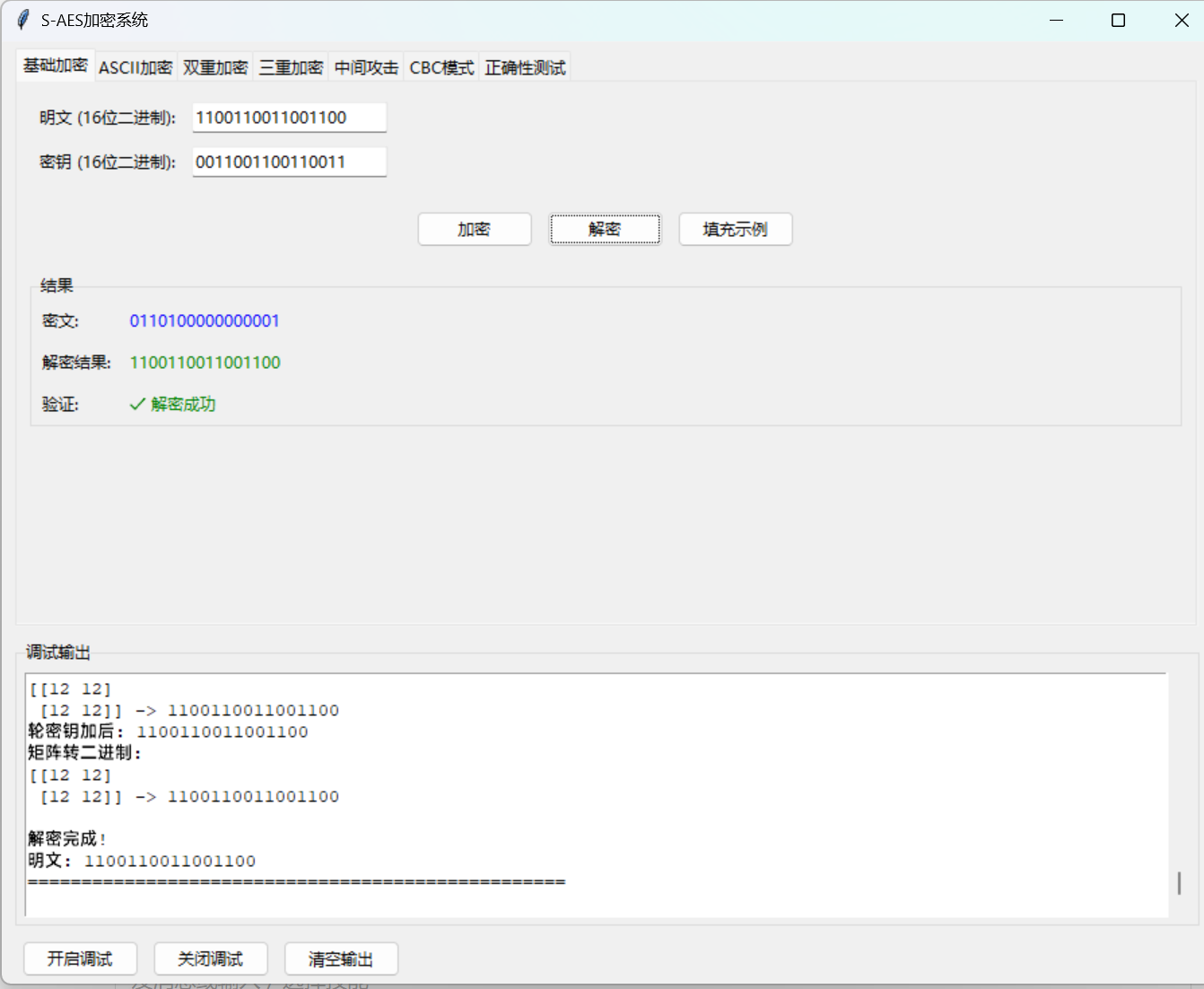
第一关：基本测试



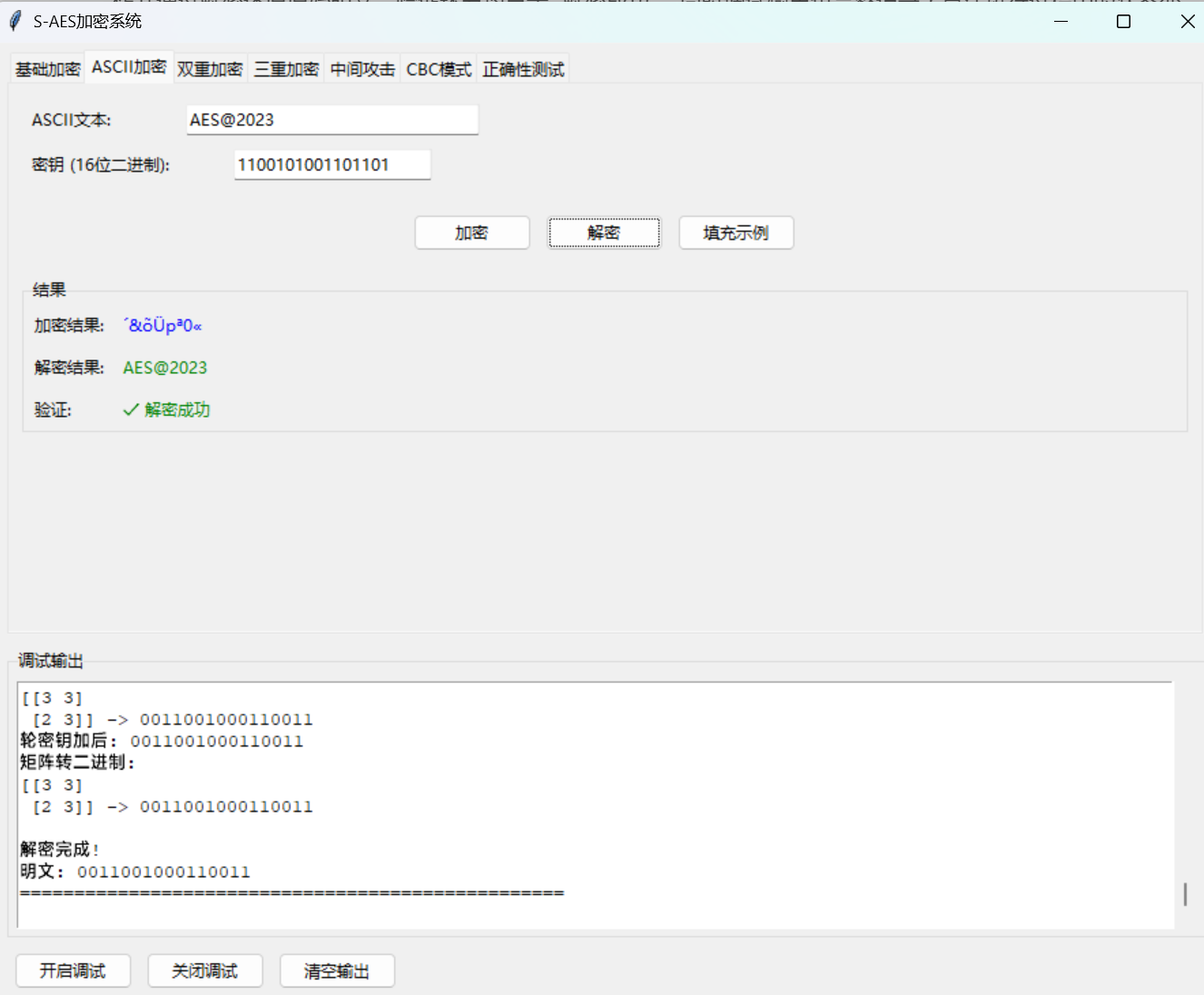
实验结果表明，S-AES 加密解密系统及其中间相遇攻击、CBC 模式等功能均运行正常。基础加密解密通过预设明文和密钥验证，结果一致；ASCII 字符串加密解密能准确还原原始文本；双重和三重加密在 32 位、48 位密钥模式下均实现正确加解密；中间相遇攻击成功找到目标密钥对；CBC 模式加密解密结果准确，且篡改测试验证了其分组依赖特性。正确性测试中，标准用例、S 盒、列混淆及交叉测试均通过，证明系统实现符合 S-AES 算法规范。

第二关：交叉测试



对这两张图片的 S-AES 加密解密结果进行交叉测试可知，在不同明文和密钥的组合下，系统均能准确完成加密操作并通过解密还原原始明文，验证环节均显示 “解密成功”，同时调试输出也完整记录了算法执行过程中的状态变换，充分表明该 S-AES 加密解密系统的加解密功能稳定可靠，算法逻辑符合规范，可在多种输入场景下实现正确的加密解密循环。

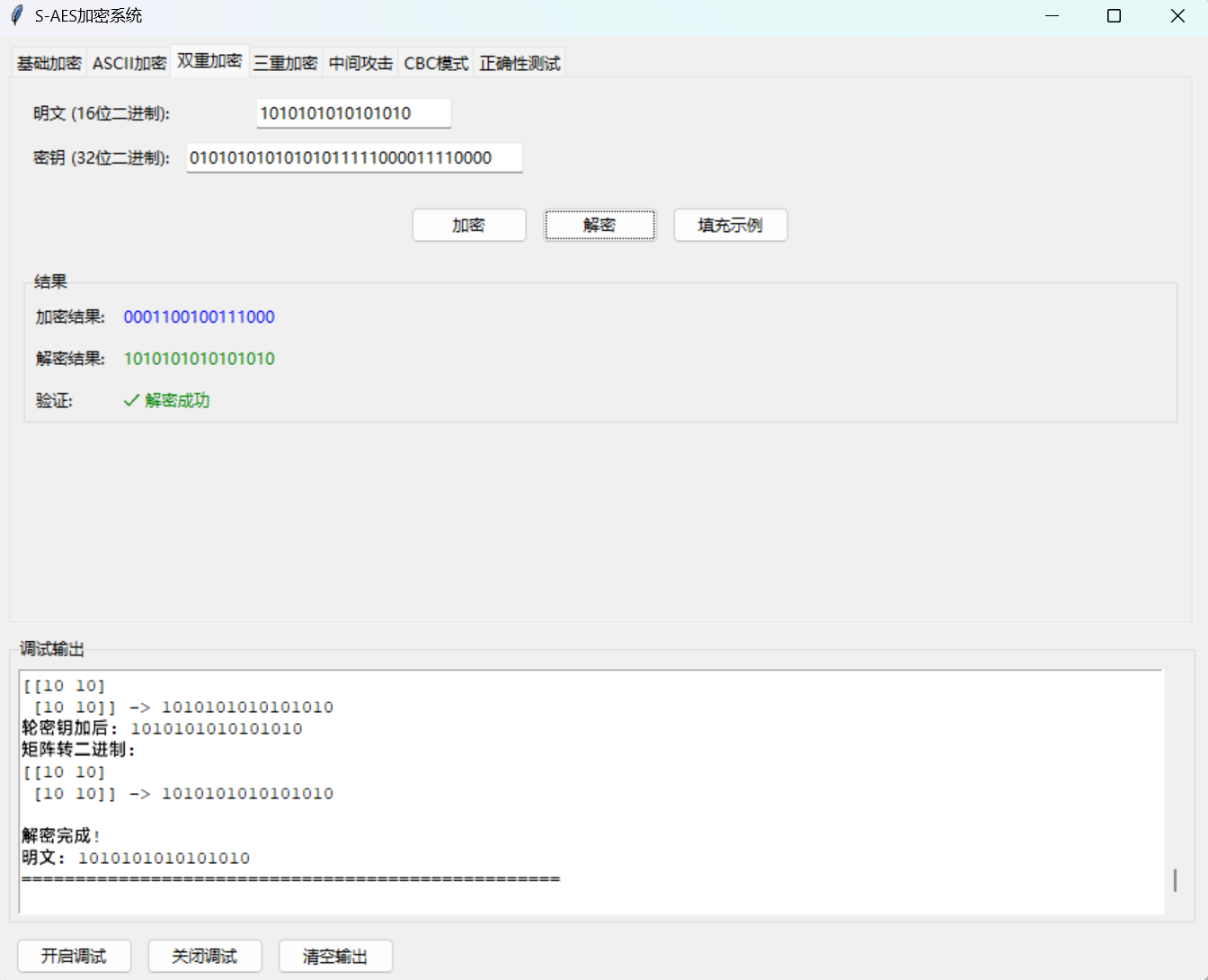
**第3关：扩展功能**



该S-AES加密系统在ASCII加密功能测试中，对ASCII文本“AES@2023”使用密钥“1100101001101101”进行加密，得到对应乱码形式的加密结果，随后解密操作成功还原原始文本，验证显示“解密成功”，同时调试输出完整记录了算法执行过程中的状态变换，充分证明系统在ASCII字符串加解密场景下功能稳定、逻辑正确。

**第4关：多重加密**

3.4.1 双重加密



该S-AES加密系统在双重加密功能测试中，对明文“1010101010101010”使用32位密钥“01010101010101011111000011110000”进行加密，得到密文“0001100100111000”，随后解密操作成功还原原始明文，验证显示“解密成功”，调试输出也完整记录了算法执行过程中的状态变换，表明系统在双重加密模式下功能稳定、逻辑正确。

3.4.3 三重加密



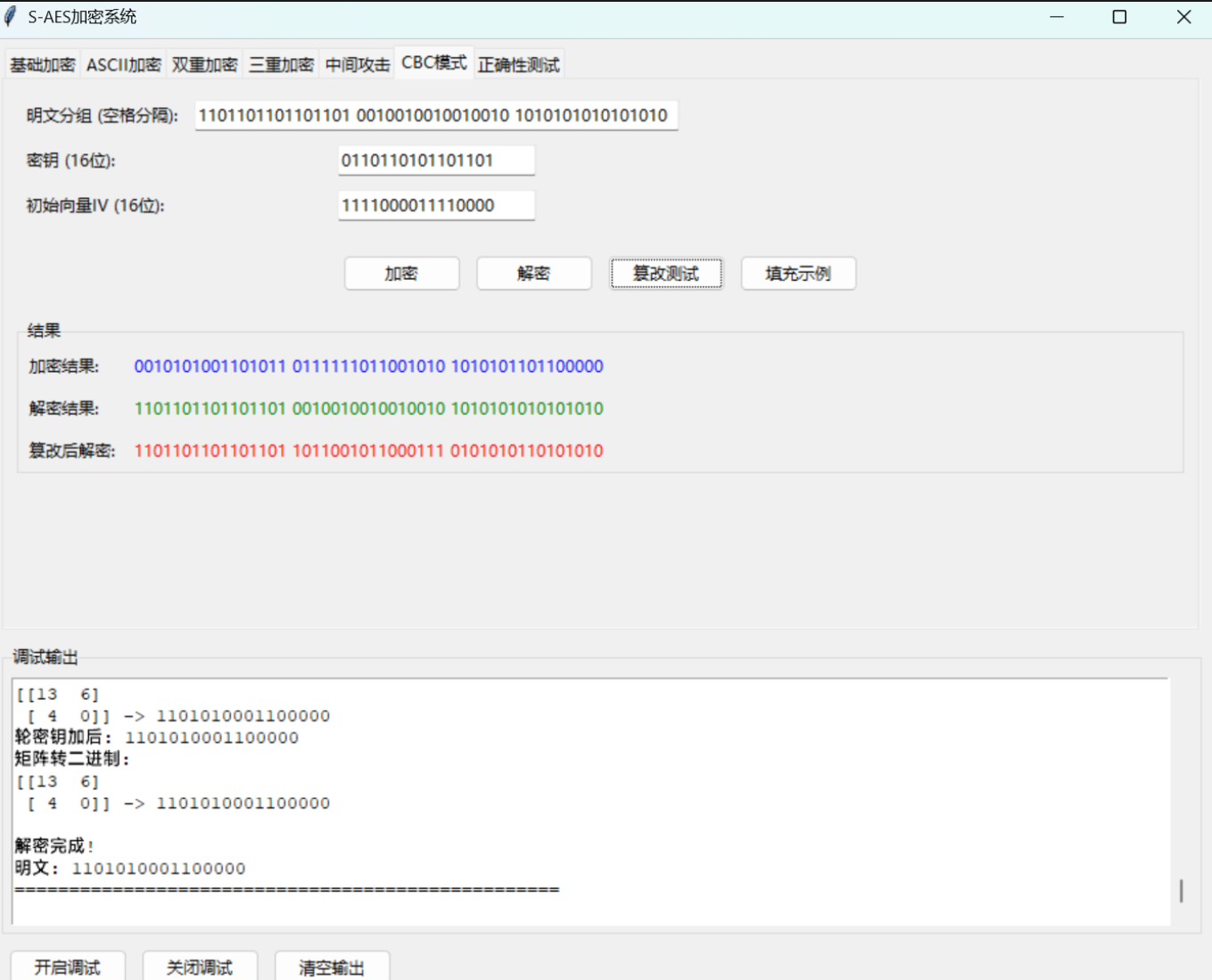
该S-AES加密系统在48位密钥的三重加密模式下，对明文“0011001100110011”使用密钥“100110011001100101100110011001101111000011110000”完成加密，得到密文“1000101100100110”，随后解密操作成功还原原始明文，验证显示“解密成功”，表明系统在三重加密模式下功能稳定、逻辑正确，可满足高安全级别的加密需求。

3.4.2 中间相遇攻击



该S-AES加密系统在中间相遇攻击测试中，基于已知明文“1110001110001110”和已知密文“0011010011010110”，测试1000组密钥对后，找到15个可能的密钥对，成功验证了中间相遇攻击在双重加密场景下的破解有效性，调试输出也完整记录了算法执行过程中的状态变换。

**第5关：工作模式**



该S-AES加密系统在CBC模式测试中，对明文分组“1101101101101101 0010010010010010 1010101010101010”使用密钥“0110110101101101”和初始向量“1111000011110000”完成加密，解密后成功还原原始明文，同时篡改测试中密文的修改导致对应及后续明文分组错乱，验证了CBC模式的加密正确性和分组依赖特性。