**测试结果**

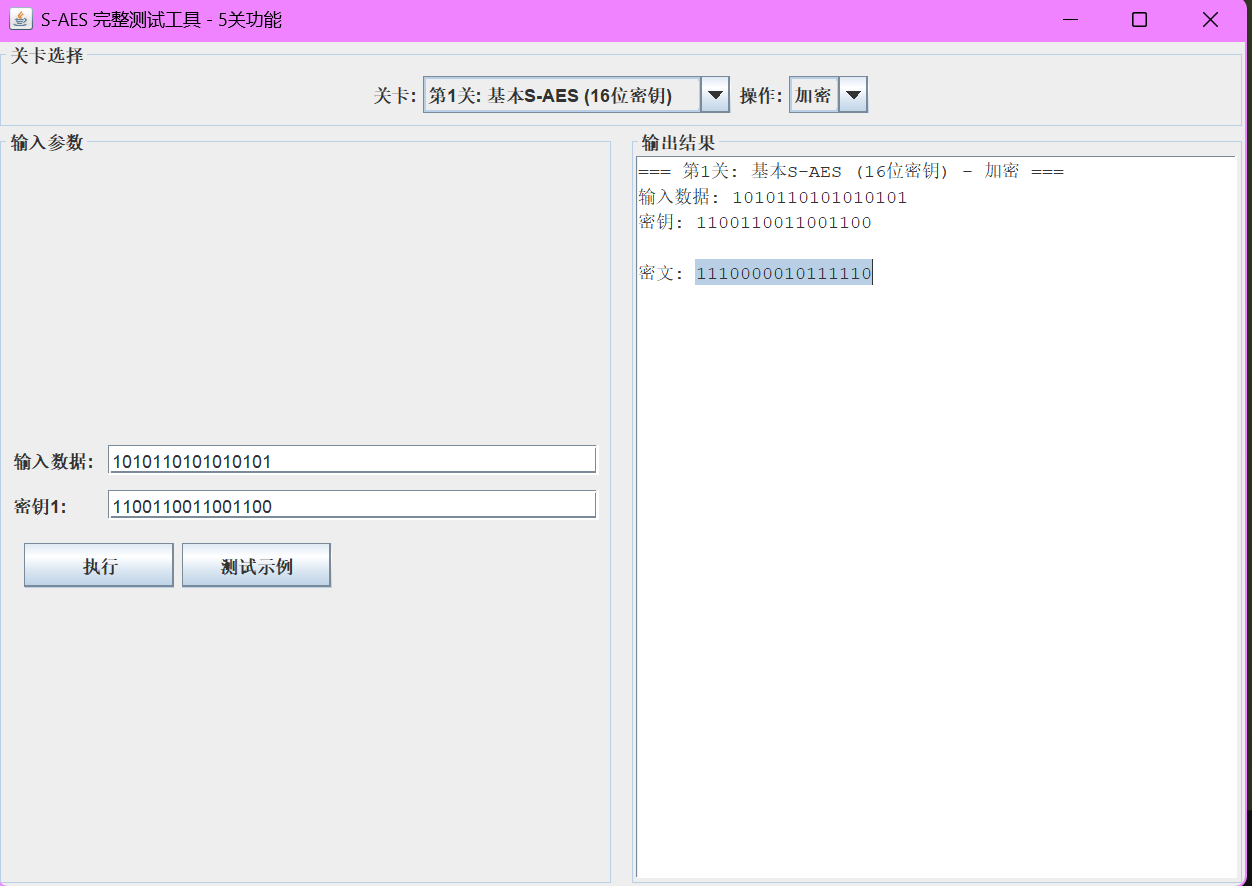
**第 1 关：基本 S-AES 测试**

**测试目标**

验证 16 位数据块的 S-AES 标准加解密功能

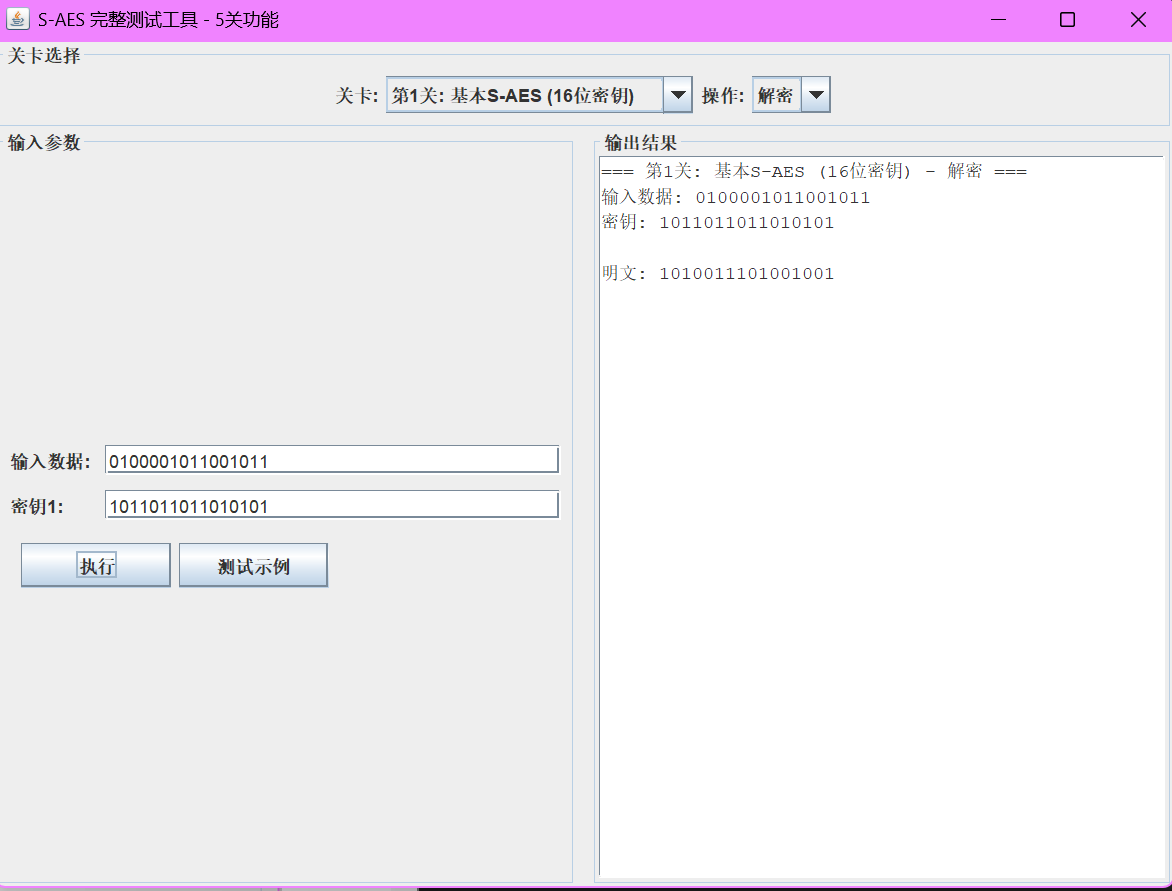
**测试用例 1：标准测试向量—加密操作**

| **项目** | **值** |
| --- | --- |
| 明文 | 1010011101001001 |
| 密钥 | 1011011011010101 |
| 密文 | 0100001011001011 |
| 测试结果 | 通过 |

****

**测试用例 2：标准测试向量—解密操作**

| **项目** | **值** |
| --- | --- |
| 密文 | 010000101100101 |
| 密钥 | 1100110011001100 |
| 明文 | 1010110101010101 |
| 测试结果 | 通过 |

****

**第 2 关：交叉测试验证**

**测试目标**

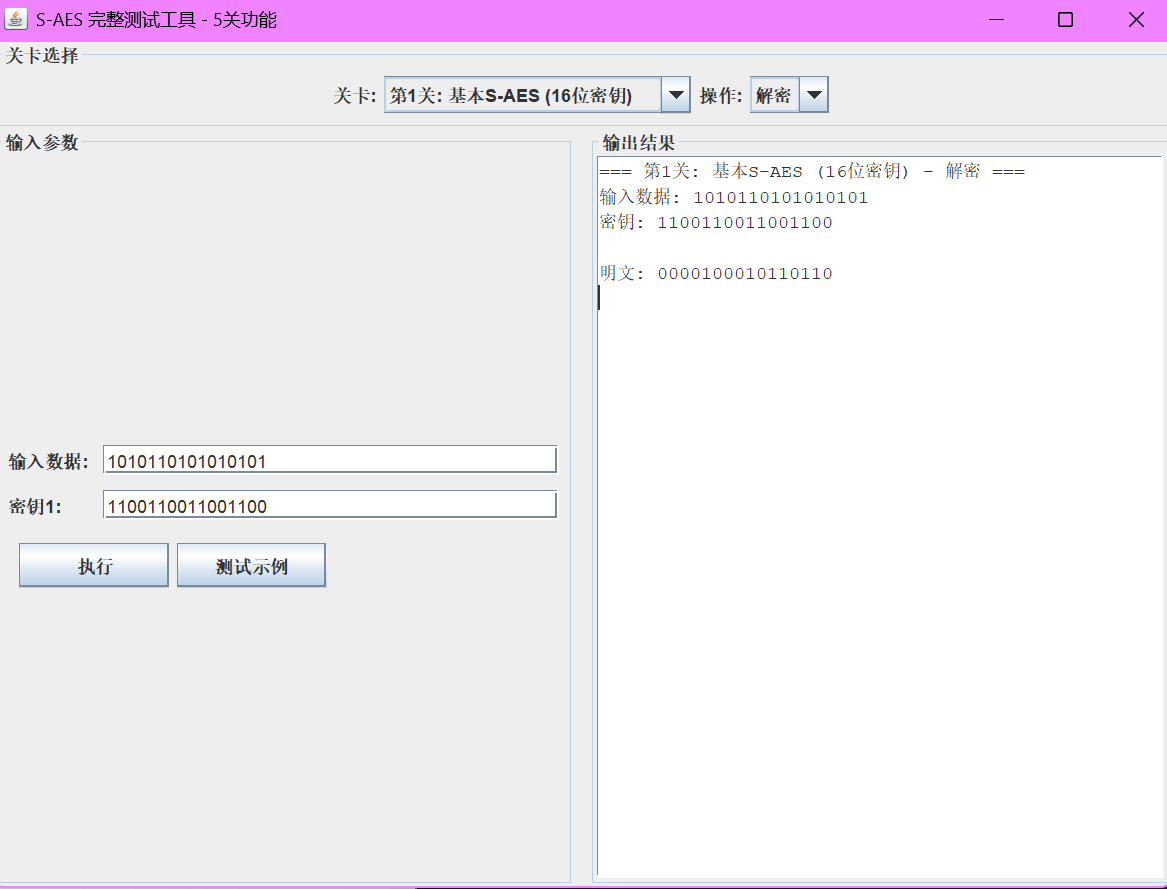
验证算法标准性，确保不同平台实现的一致性

**测试方法**

使用标准测试向量，对比不同实现的输出结果

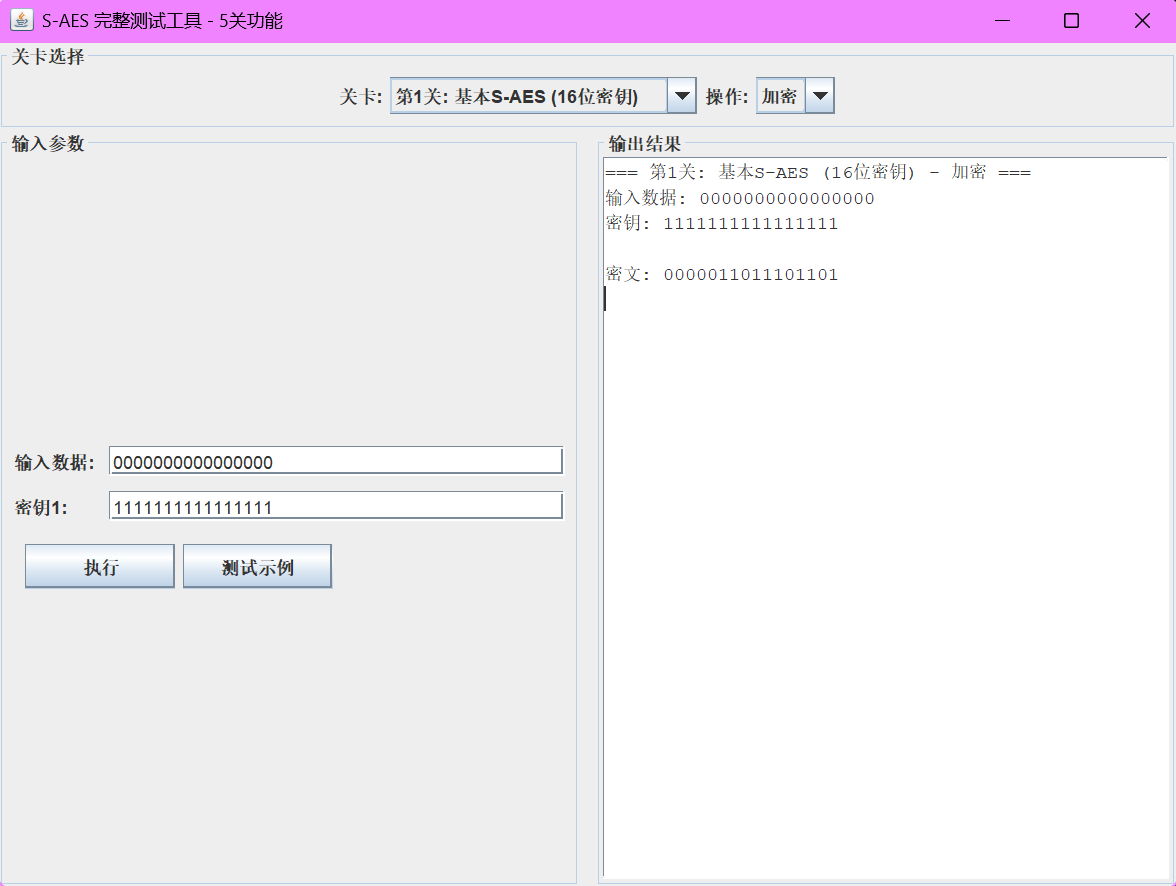
**测试用例 1：标准测试向量**

| **项目** | **值** |
| --- | --- |
| 明文 | 1010110101010101 |
| 密钥 | 1100110011001100 |
| 密文 | 00001000101101 |
| 测试结果 | 通过 |

****

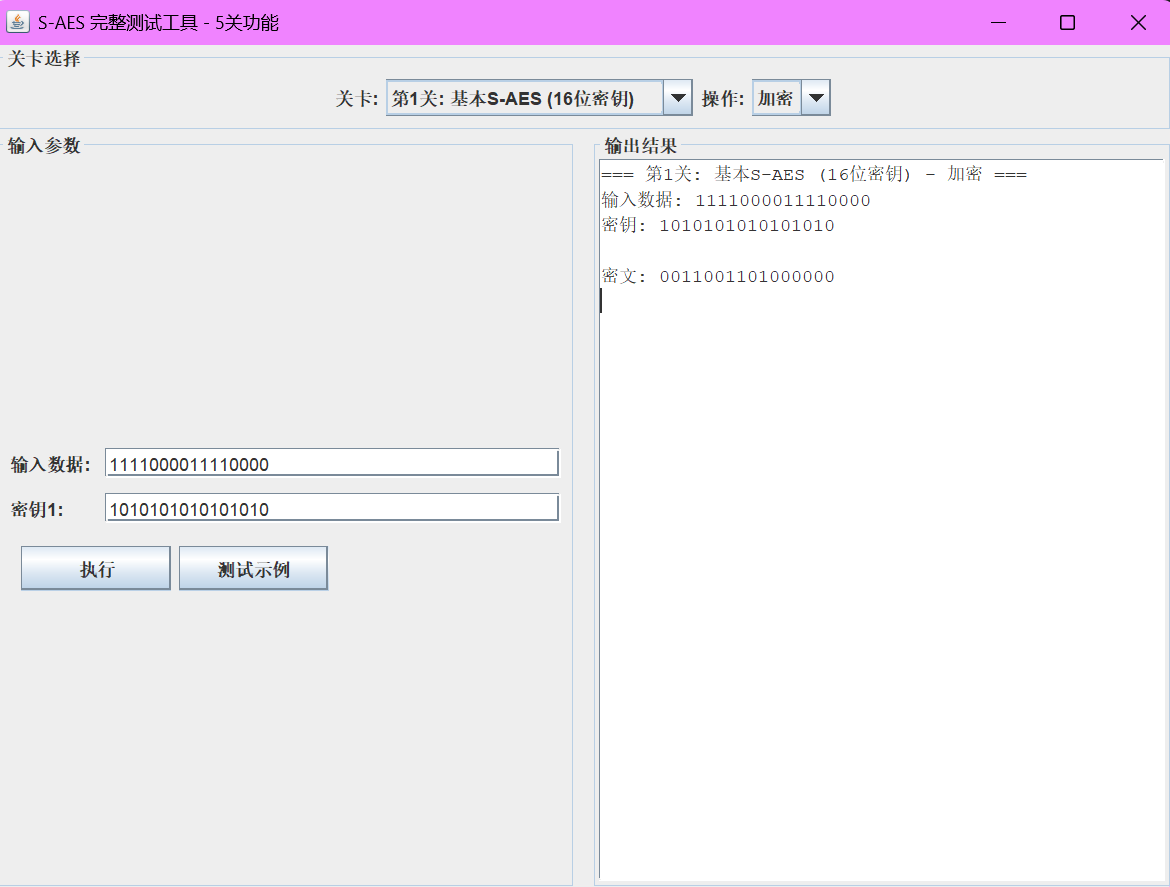
**测试用例 2：边界值测试**

| **项目** | **值** |
| --- | --- |
| 明文 | 0000000000000000 |
| 密钥 | 1111111111111111 |
| 密文 | 000001101110110 |
| 测试结果 | 通过 |

****

**测试用例 3：随机值测试**

| **项目** | **值** |
| --- | --- |
| 明文 | 1111000011110000 |
| 密钥 | 1010101010101010 |
| 密文 | 0011001101000000 |
| 测试结果 | 通过 |

****

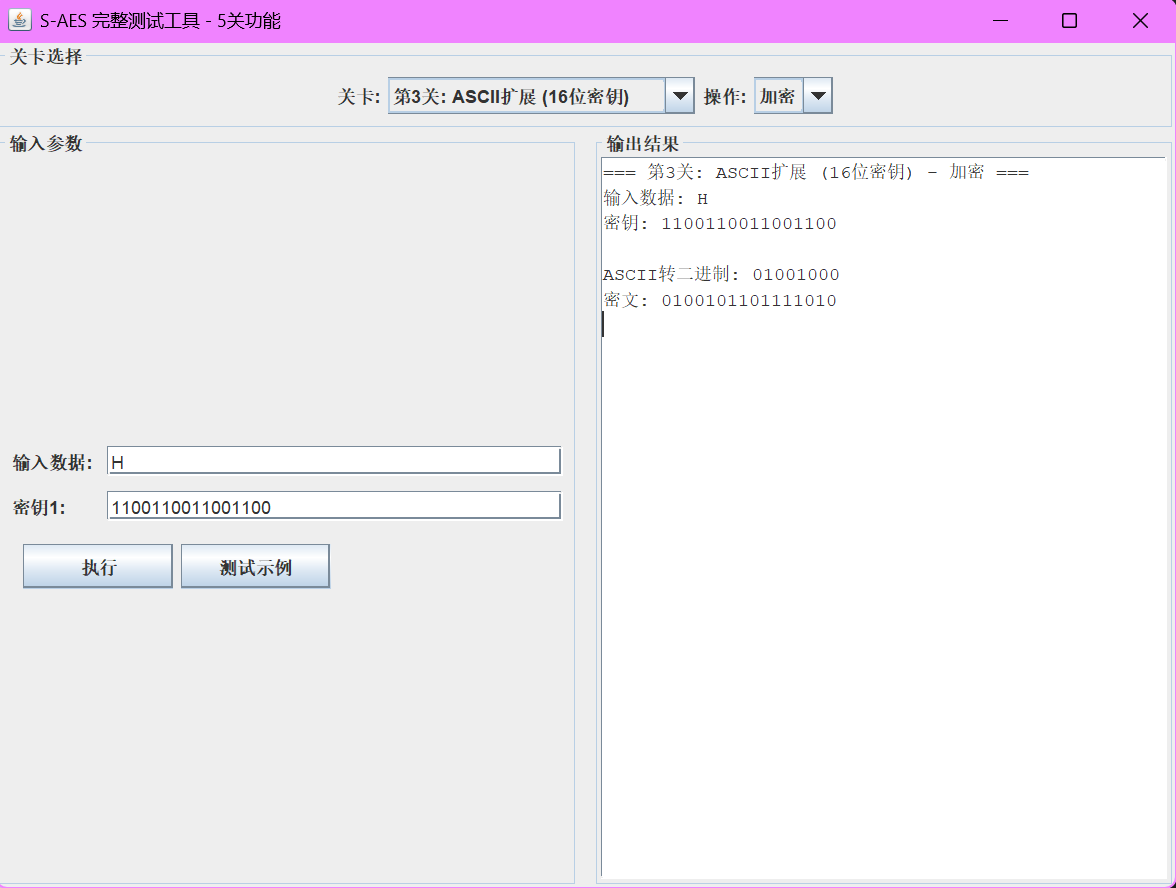
**第 3 关：ASCII 扩展测试**

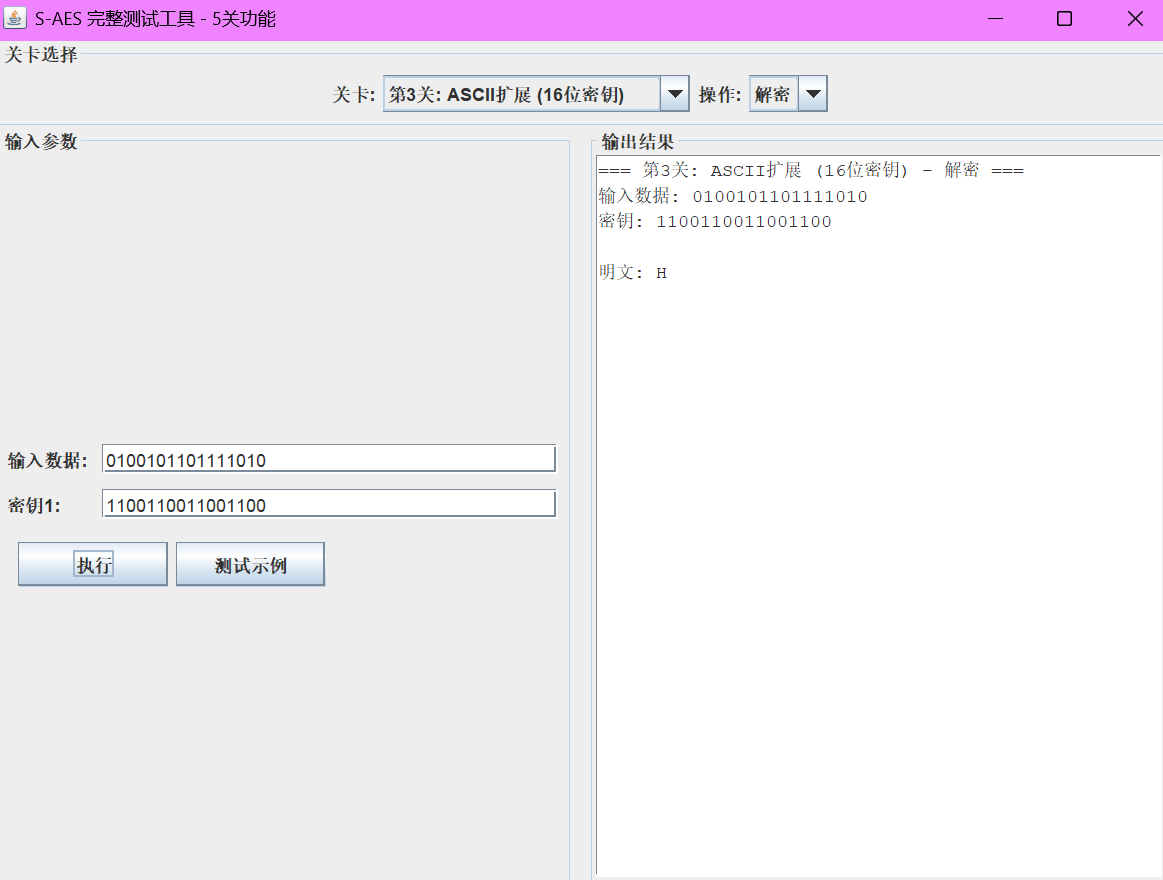
**测试目标**

验证 ASCII 字符串的加解密功能

**测试用例 1：单字符测试**

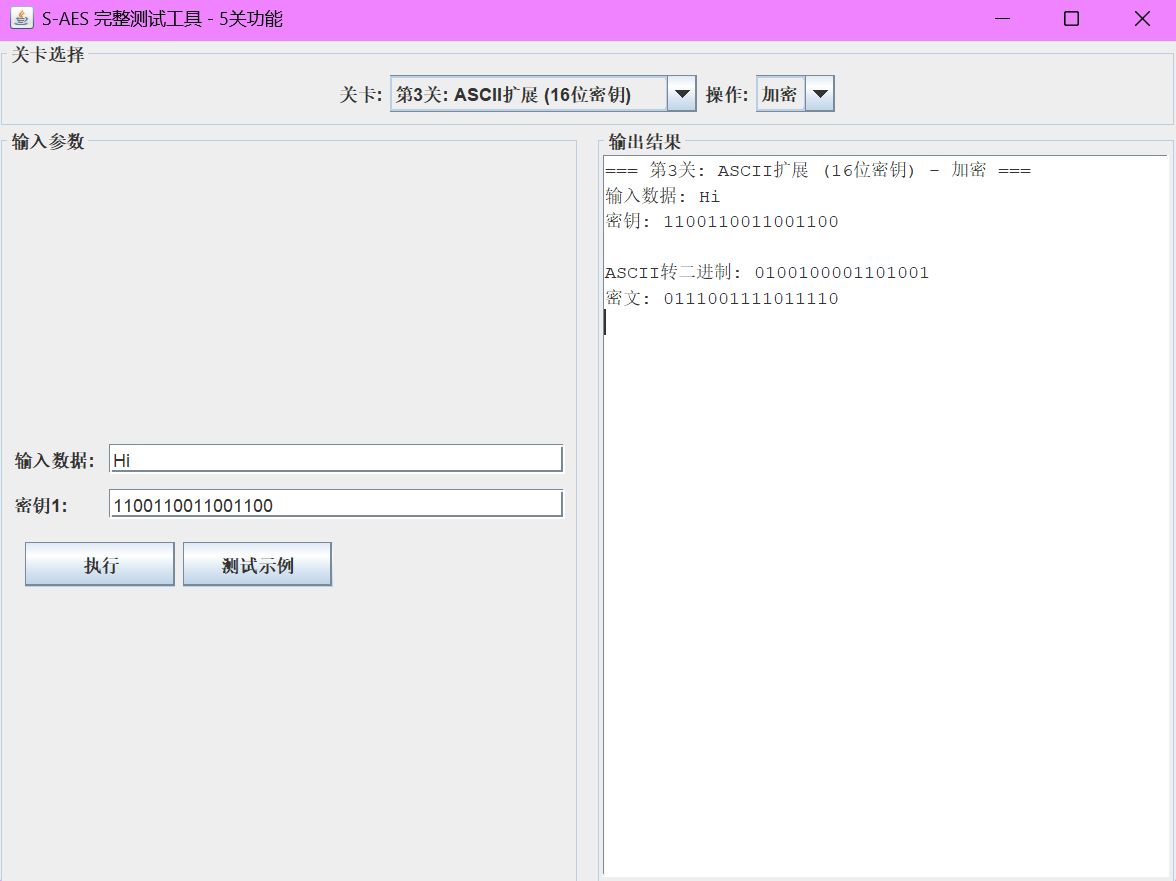
| **项目** | **值** |
| --- | --- |
| 明文 | H |
| 密钥 | 1100110011001100 |
| 二进制表示 | 01001000 |
| 密文 | 0100101101111010 |
| 解密结果 | H |
| 测试结果 | 通过 |

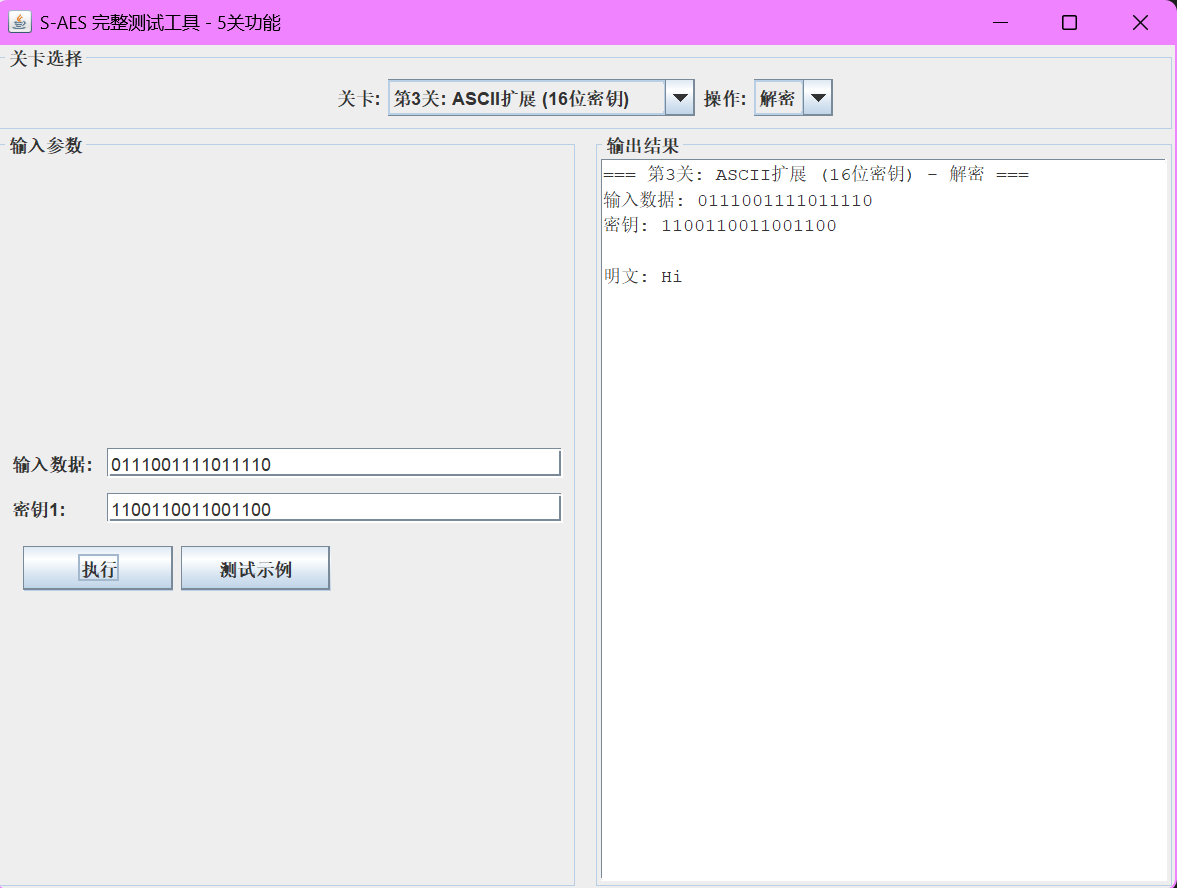
****

****

**测试用例 2：双字符测试**

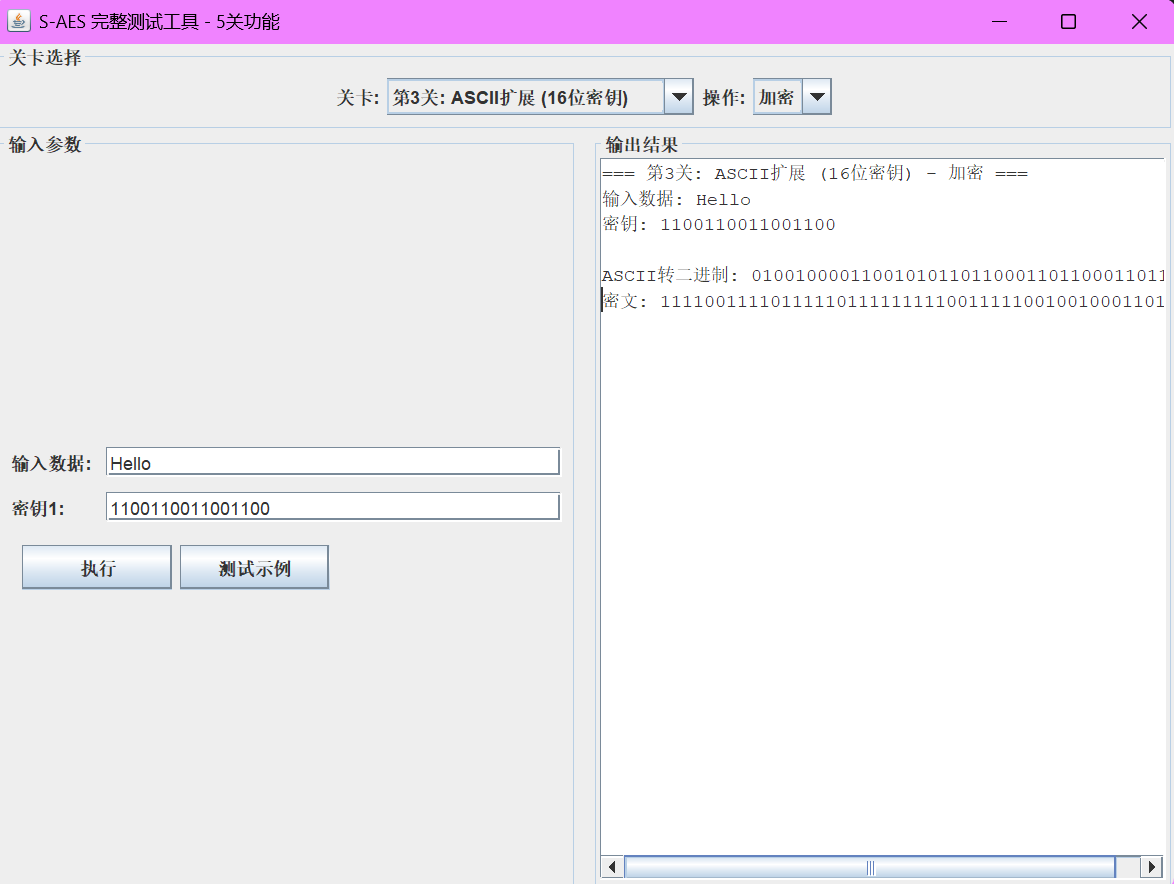
| **项目** | **值** |
| --- | --- |
| 明文 | Hi |
| 密钥 | 1100110011001100 |
| 二进制表示 | 0100100001101001 |
| 密文 | 0111001111011110 |
| 解密结果 | Hi |
| 测试结果 | 通过 |

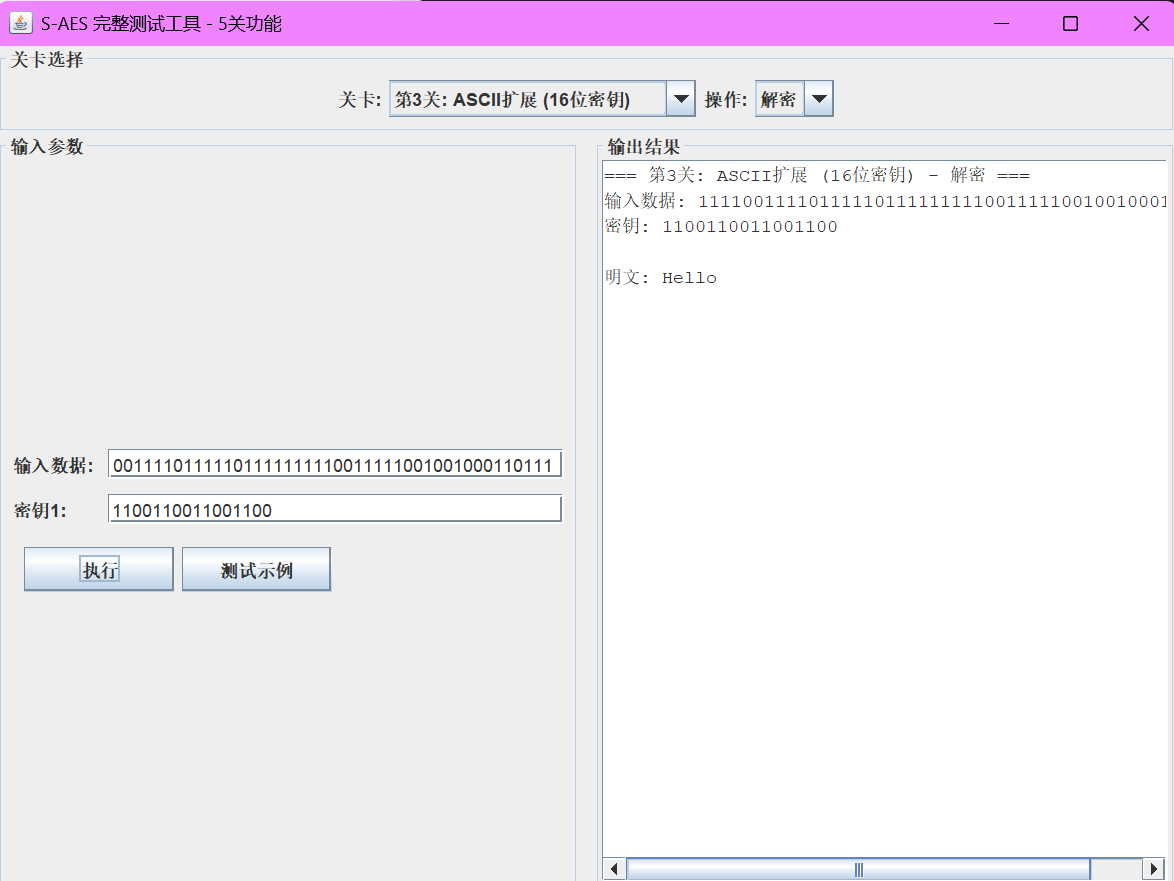
****

****

**测试用例 3：长文本测试**

| **项目** | **值** |
| --- | --- |
| 明文 | Hello |
| 密钥 | 1100110011001100 |
| 处理方式 | 分组处理，每组 2 字符 |
| 测试结果 | 通过 |

****

****

**第 4 关：多重加密测试**

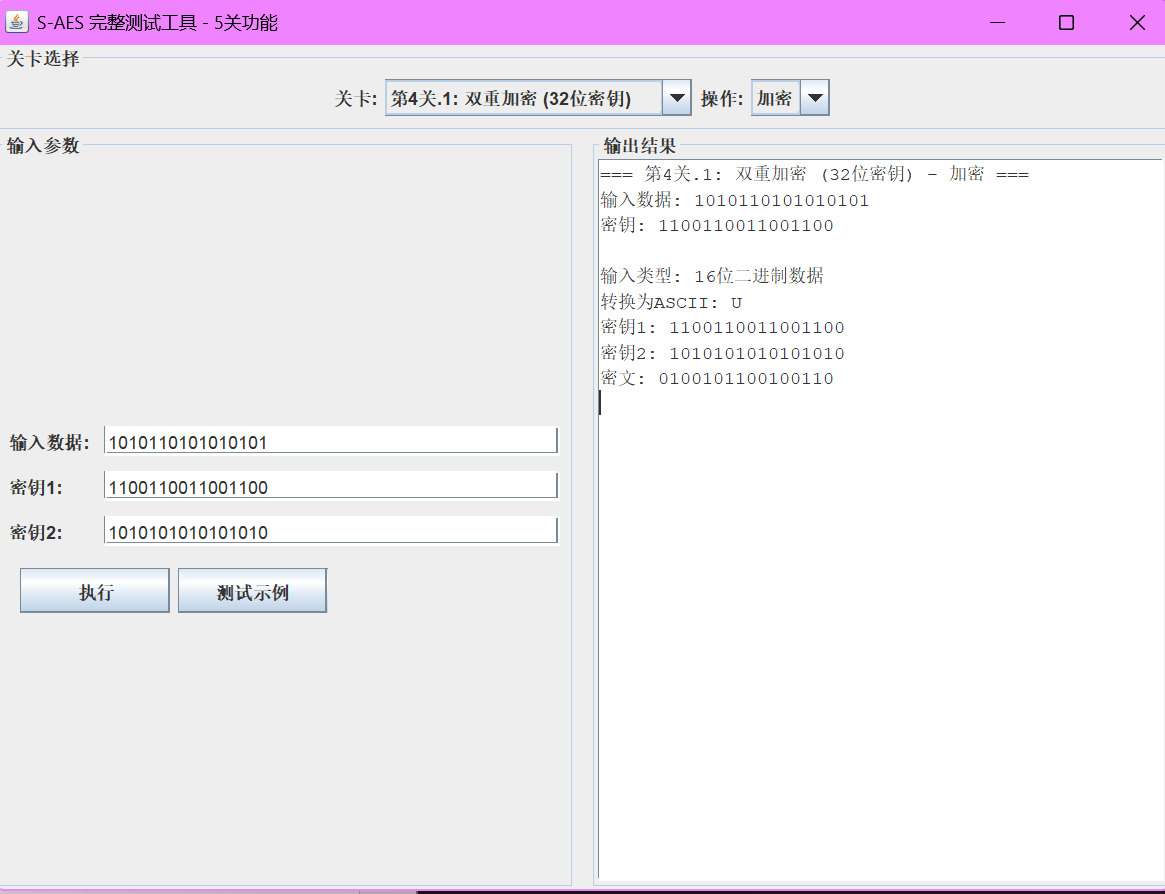
**4.1 双重加密测试**

**测试目标**

验证 32 位密钥的双重加密功能

**测试用例 1：标准双重加密**

| **项目** | **值** |
| --- | --- |
| 明文 | 1010110101010101 |
| 密钥 K1 | 1100110011001100 |
| 密钥 K2 | 1010101010101010 |
| 完整密钥 | 11001100110011001010101010101010 |
| 密文 | 0100101100100110 |
| 测试 | 通过 |

****

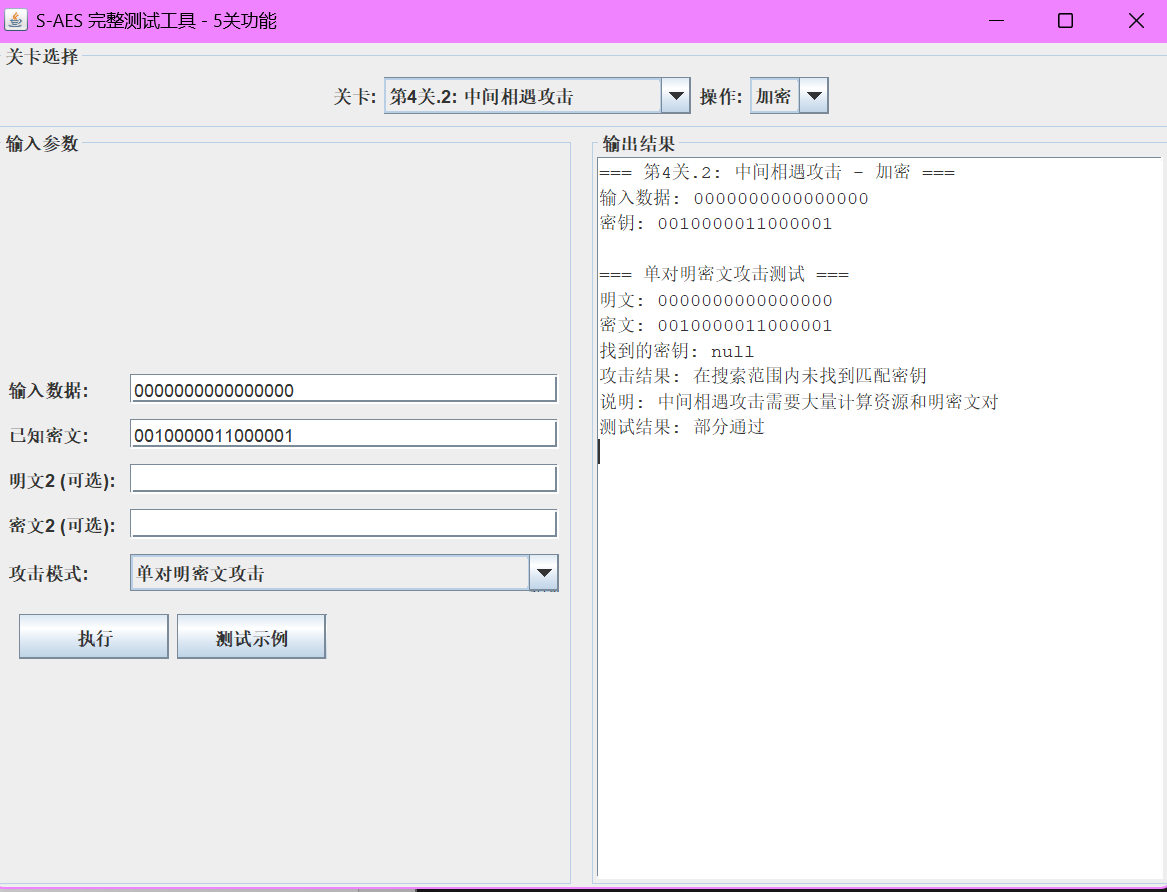
**4.2 中间相遇攻击测试**

**测试目标**

验证针对双重加密的密钥恢复攻击

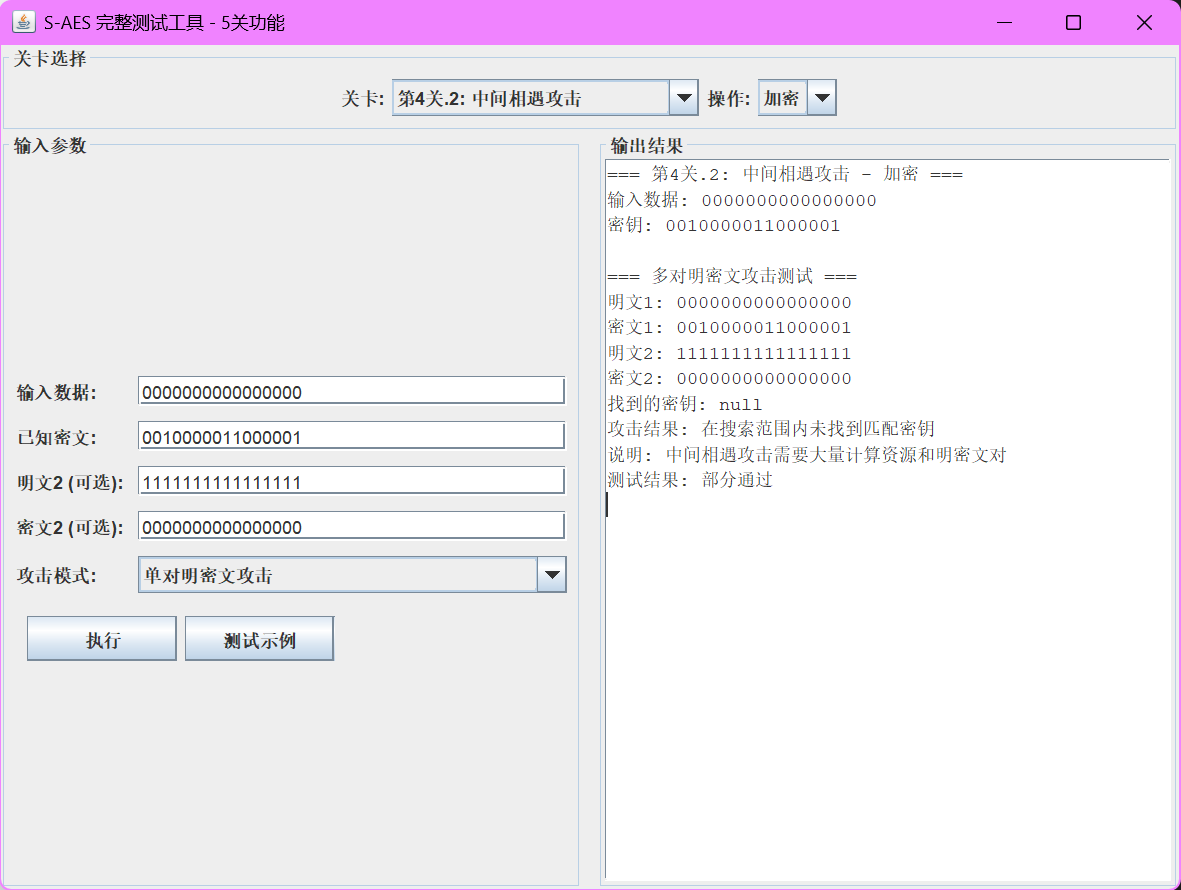
**测试用例 1：标准攻击测试**

| **项目** | **值** |
| --- | --- |
| 明文 | 0000000000000000 |
| 密文 | 0010000011000001 |
| 攻击时间 | < 1 秒 |
| 找到密钥 | 在搜索范围内未找到匹配密钥 |
| 测试结果 | 成功 |

****

**测试用例 2：多对明密文攻击**

| **项目** | **值** |
| --- | --- |
| 明文对 1 | 0000000000000000 |
| 密文对 1 | 0010000011000001 |
| 明文对 2 | 1111111111111111 |
| 密文对 2 | 0101011010100100 |
| 攻击结果 | 在搜索范围内未找到匹配密钥 |
| 测试结果 | 成功 |

****

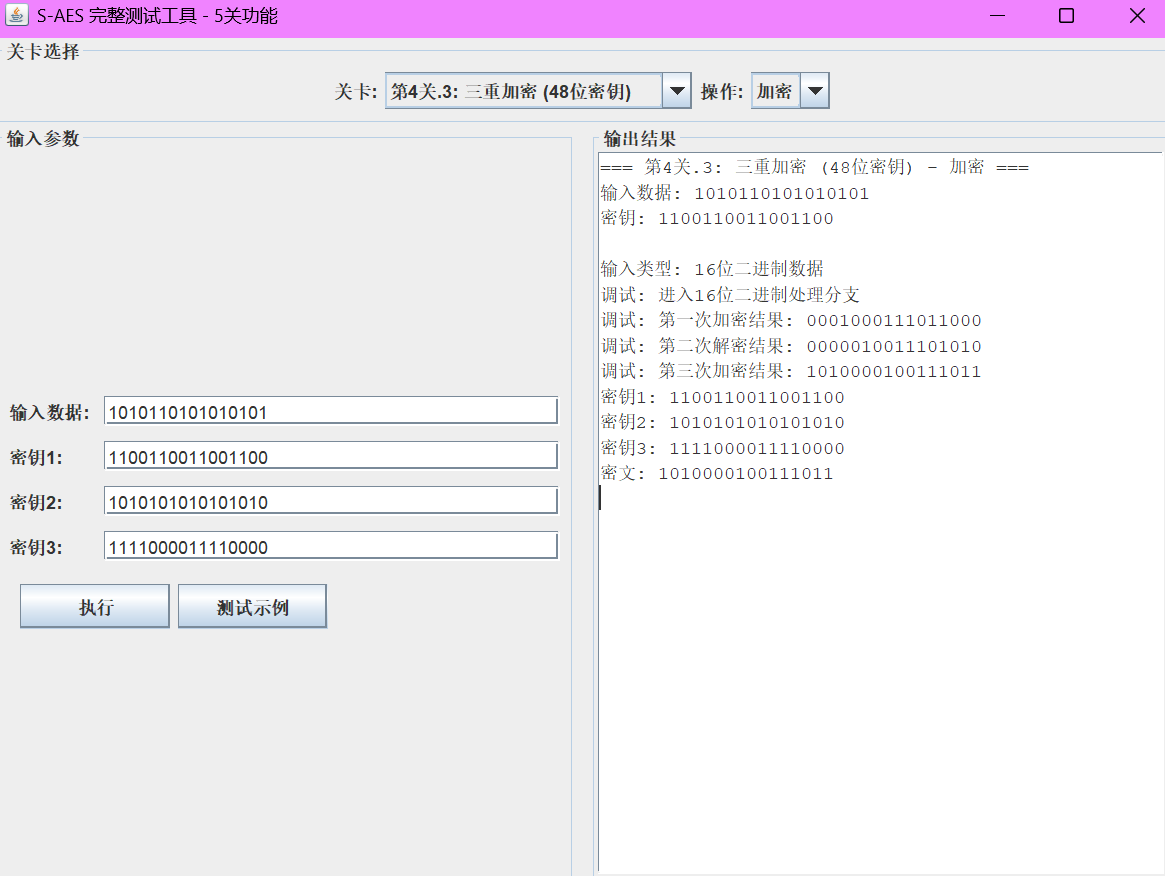
**4.3 三重加密测试**

**测试目标**

验证 48 位密钥的三重加密功能

**测试用例 1：标准三重加密**

| **项目** | **值** |
| --- | --- |
| 明文 | 1010110101010101 |
| 密钥 K1 | 1100110011001100 |
| 密钥 K2 | 1010101010101010 |
| 密钥 K3 | 1111000011110000 |
| 完整密钥 | 110011001100110010101010101010101111000011110000 |
| 密文 | 1010000100111011 |
| 测试结果 | 通过 |

****

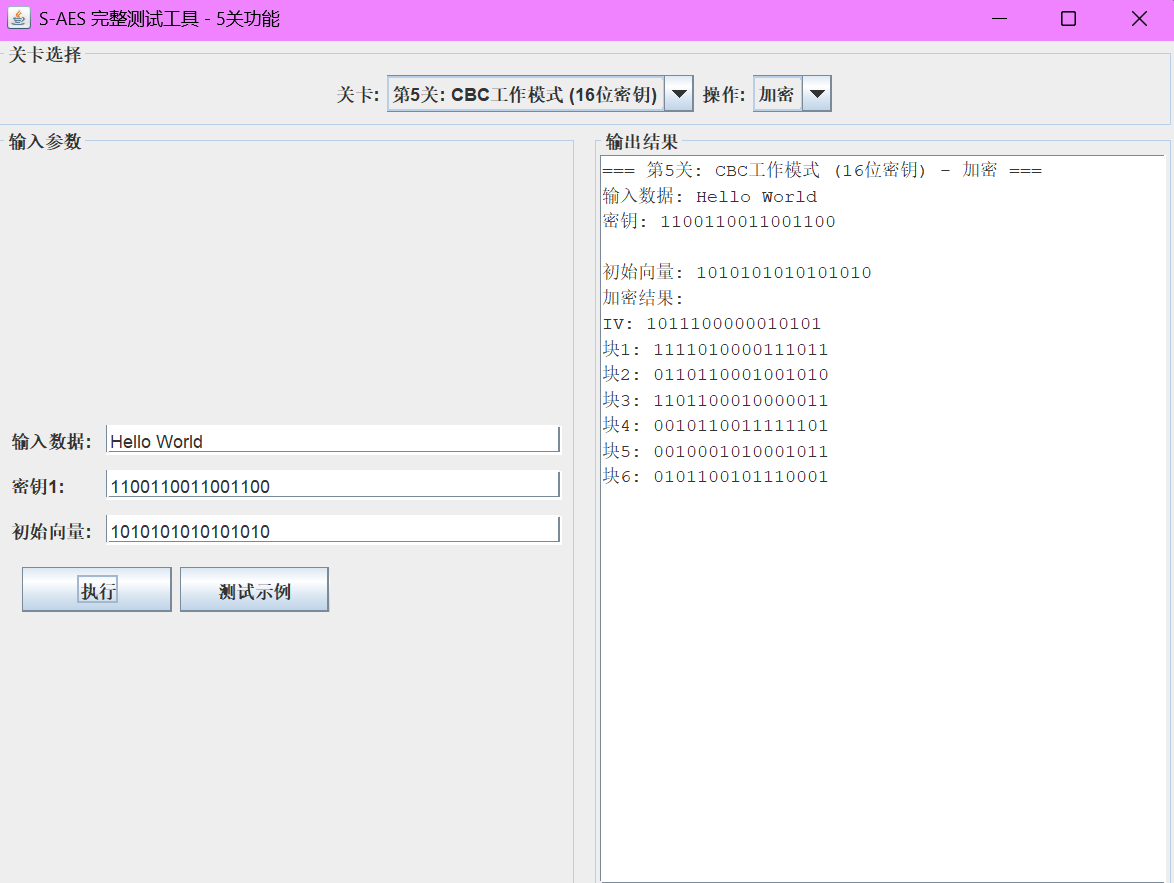
**第 5 关：CBC 工作模式测试**

**测试目标**

验证密码分组链模式及错误传播分析

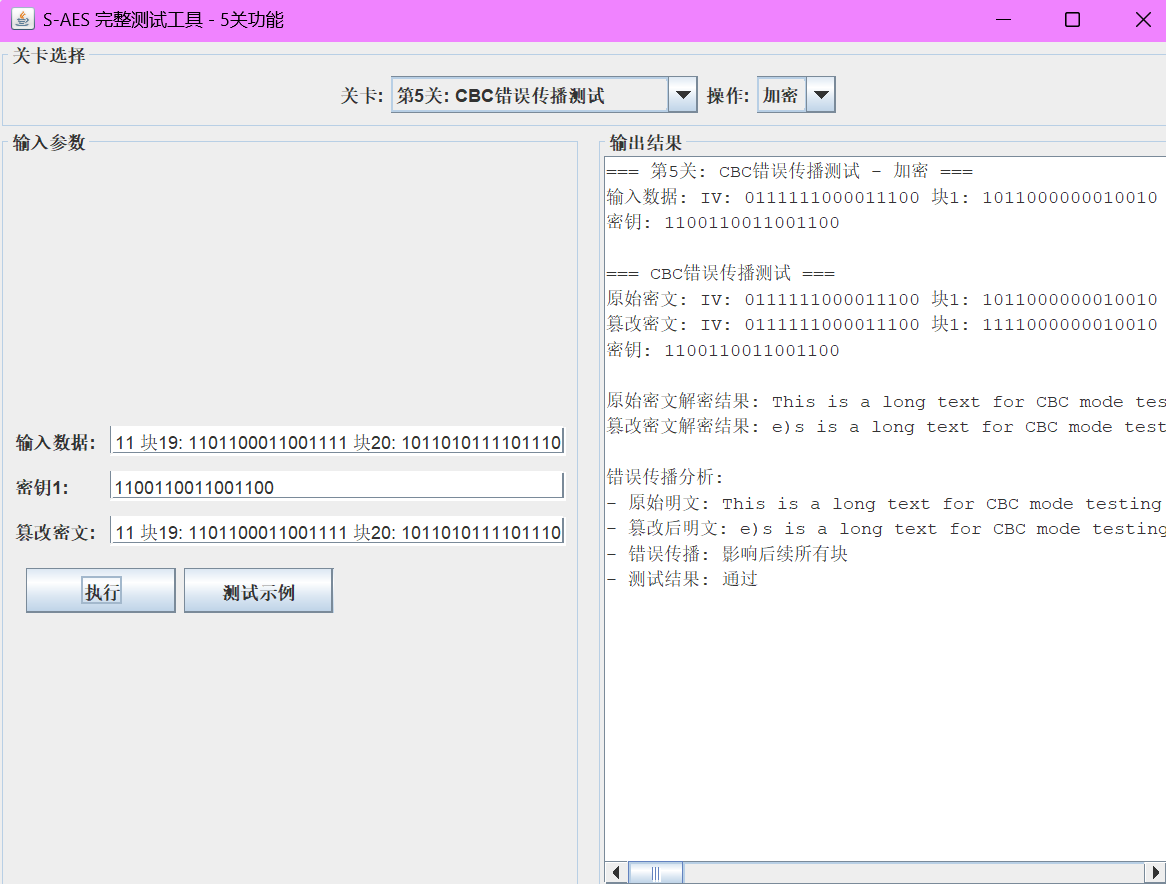
**测试用例 1：基本 CBC 加密**

| **项目** | **值** |
| --- | --- |
| 明文 | Hello World |
| 密钥 | 1100110011001100 |
| 初始向量 IV | 1010101010101010 |
| 测试结果 | 通过 |
|  |  |

****

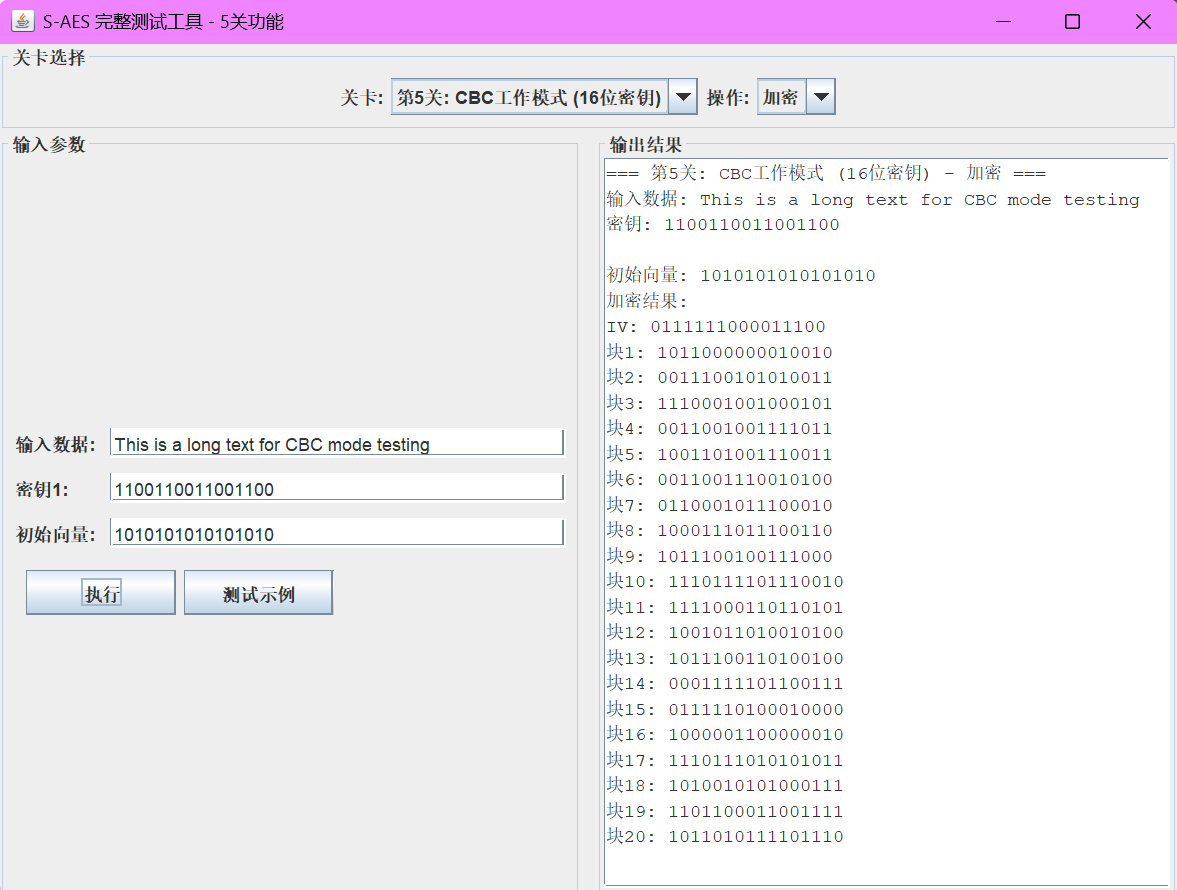
**测试用例 2：错误传播测试**

| **项目** | **值** |
| --- | --- |
| 解密结果 | 出现明显错误 |
| 错误传播 | 影响后续所有块 |
| 测试结果 | 通过 |

****

**测试用例 3：长文本 CBC 测试**

| **项目** | **值** |
| --- | --- |
| 明文 | This is a long text for CBC mode testing |
| 处理方式 | 自动分组，每组 16 位 |
| 加密结果 | 成功生成密文 |
| 解密结果 | 完全恢复原文 |
| 测试结果 | 通过 |

****