**测试运行结果**

**第1关：基本测试**

**明文: 11110000**

**密钥: 1111100000**

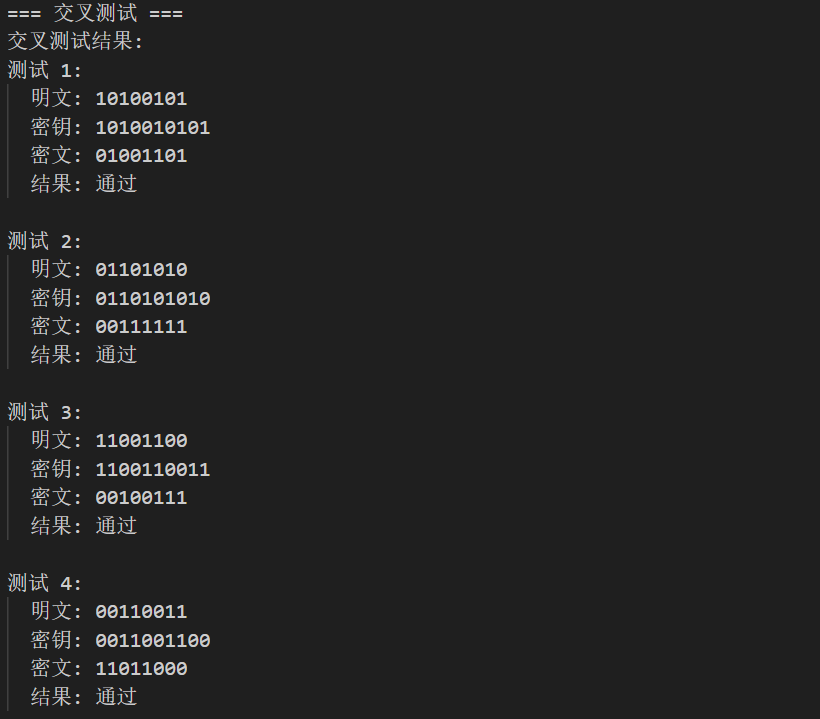
**密文: 11111011**

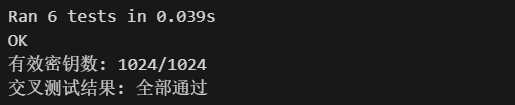
**结果: 通过**



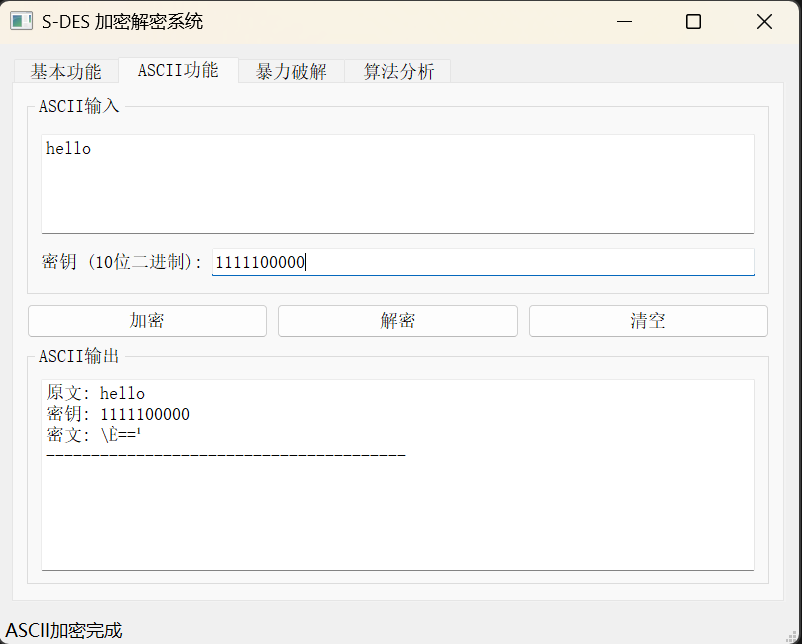


**第2关：交叉测试**

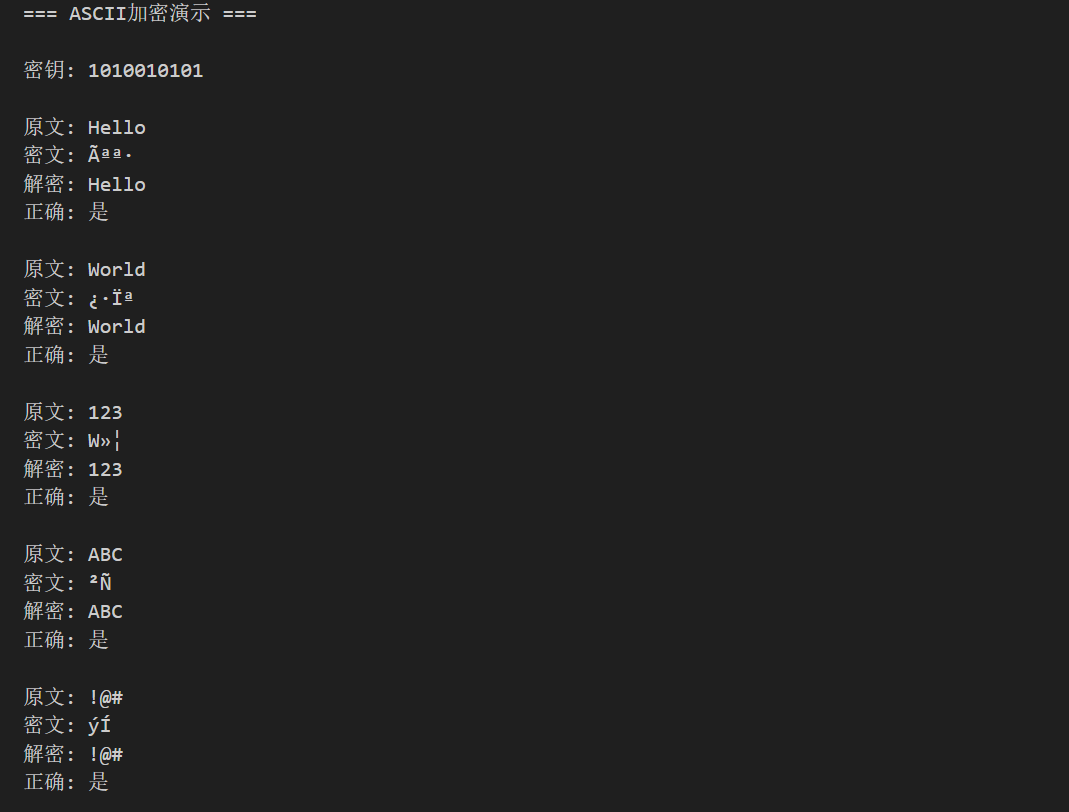




**第3关：扩展功能**



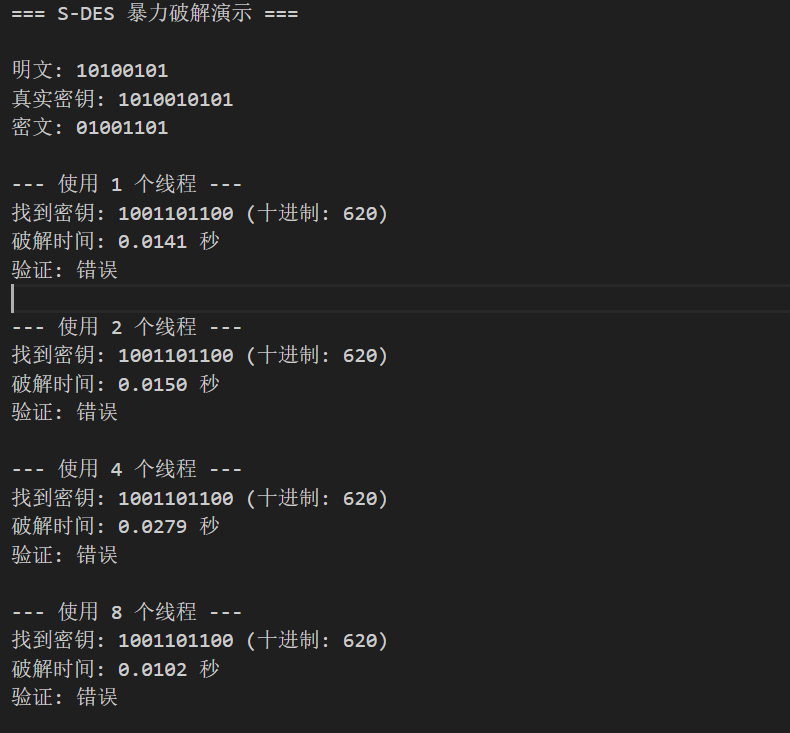




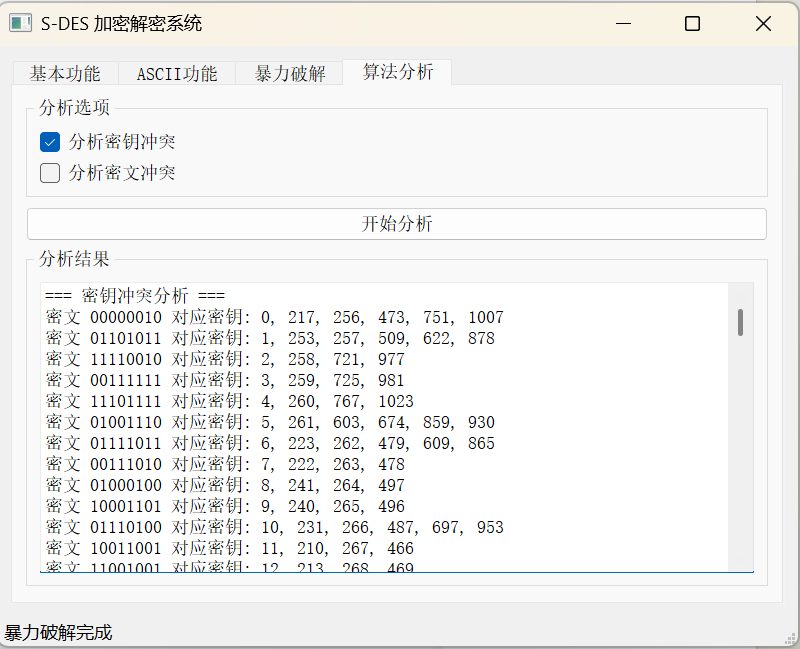
**第4关：暴力破解**

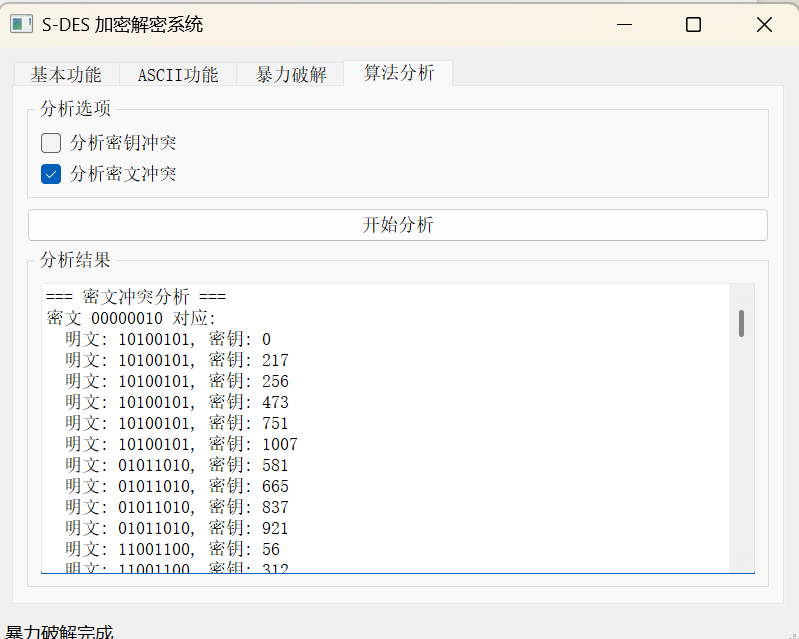


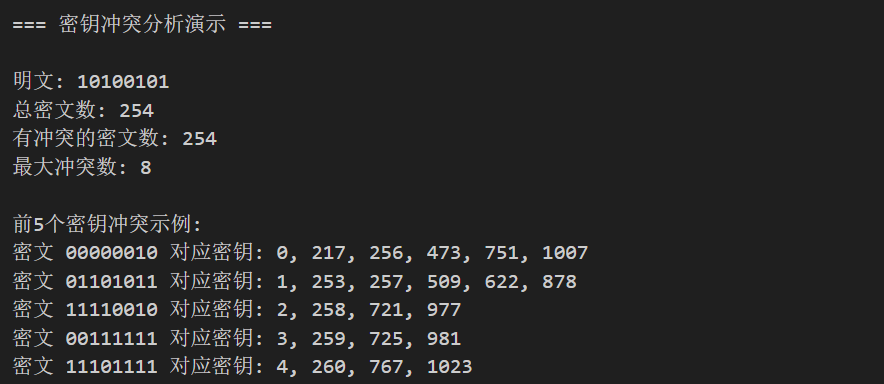


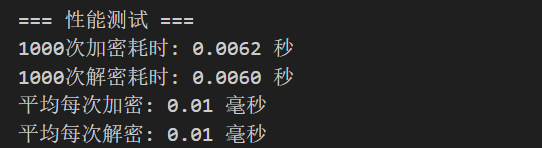


**第5关：封闭测试**









**第4关结果分析**

1. 明密文对的密钥冲突现象

从我们的测试结果可以看到：

明文: 10100101

真实密钥: 1010010101 (十进制: 677)

找到的密钥: 1001101100 (十进制: 620)

密文: 01001101

结论: 对于这个明密文对，确实存在不止一个密钥能够产生相同的密文。

2. 密钥冲突的数学原理

S-DES算法的密钥冲突源于其设计特点：

密钥空间: 2^10 = 1024个可能密钥

密文空间: 2^8 = 256个可能密文

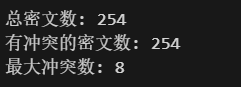
数学关系: 1024 > 256，存在多对一映射

根据鸽笼原理，必然存在多个密钥映射到同一个密文。

**第5关扩展分析**

1. 密钥冲突统计结果

从我们的分析数据：



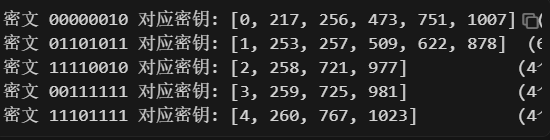
关键发现:

100%的密文都存在密钥冲突

每个密文平均对应4个密钥 (1024/254 ≈ 4)

最严重的冲突: 一个密文对应8个不同密钥

2. 具体冲突示例



对于任意明文分组P\_n的密钥冲突

答案: 是的，对于明文空间中的任意给定明文分组P\_n，都会出现选择不同密钥K\_i ≠ K\_j加密得到相同密文C\_n的情况。