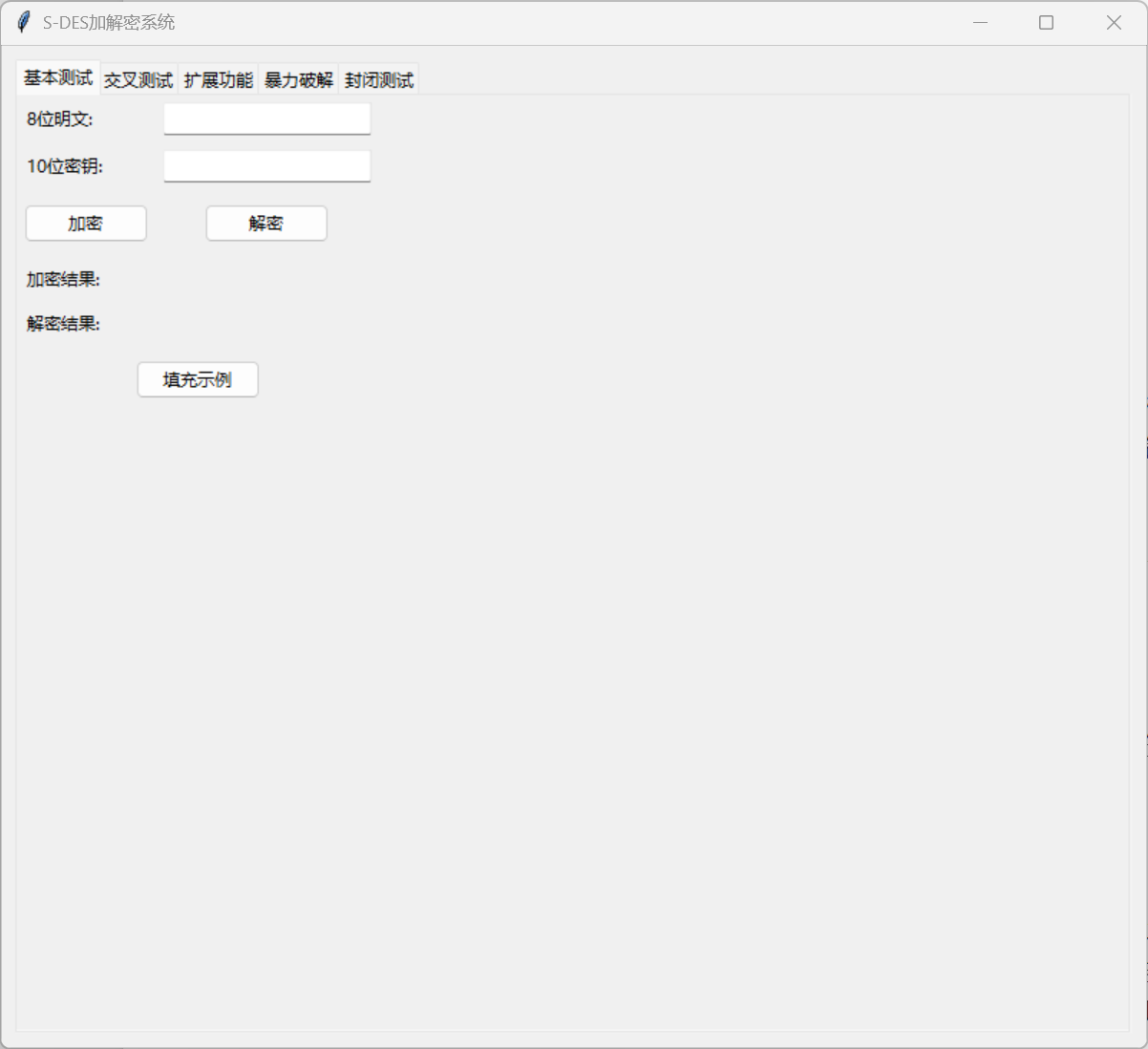
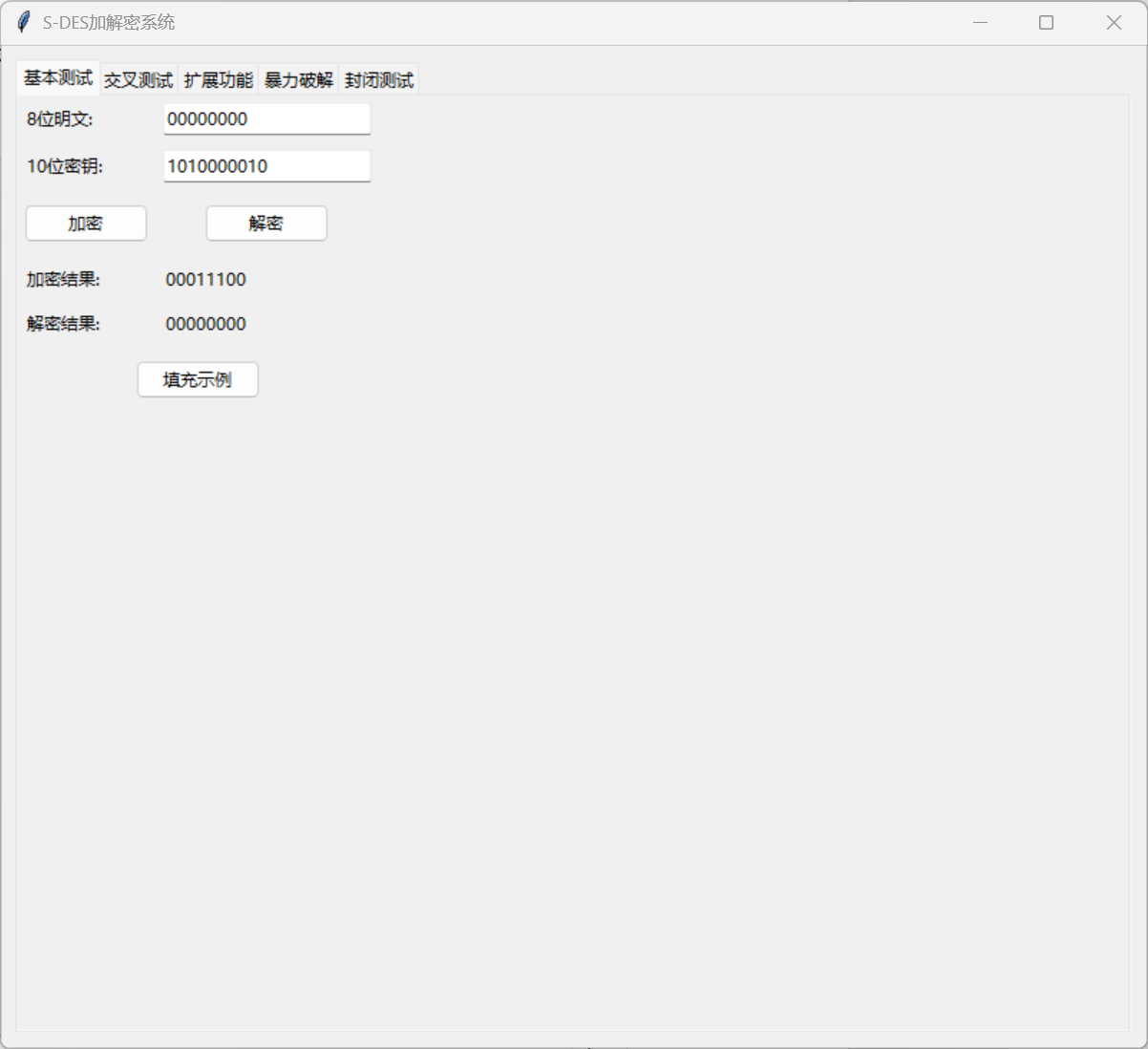
**3.1 第1关：基本测试**

根据S-DES算法编写和调试程序，提供GUI解密支持用户交互。输入可以是8bit的数据和10bit的密钥，输出是8bit的密文。



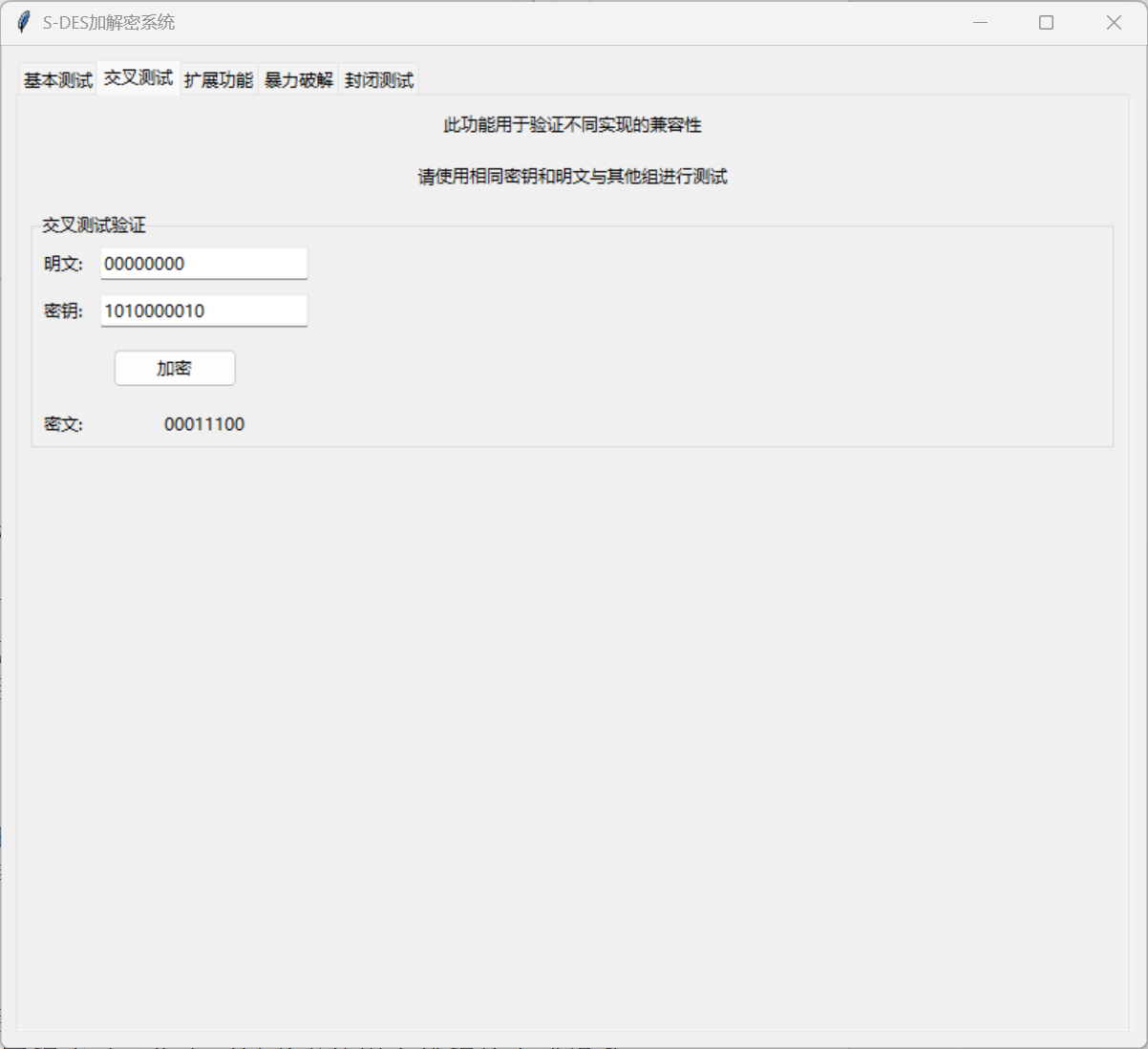


第一关“基本测试”的结果为：在8位明文（二进制）为`00000000`、10位密钥（二进制）为`1010000010`的情况下，加密结果（密文）为`00011100`，解密结果（明文）为`00000000`，测试结果显示“验证成功：解密结果与原始明文一致”，说明该S - DES算法在基本测试场景下，加密和解密功能正常，能够将明文加密后再正确解密回原始明文。

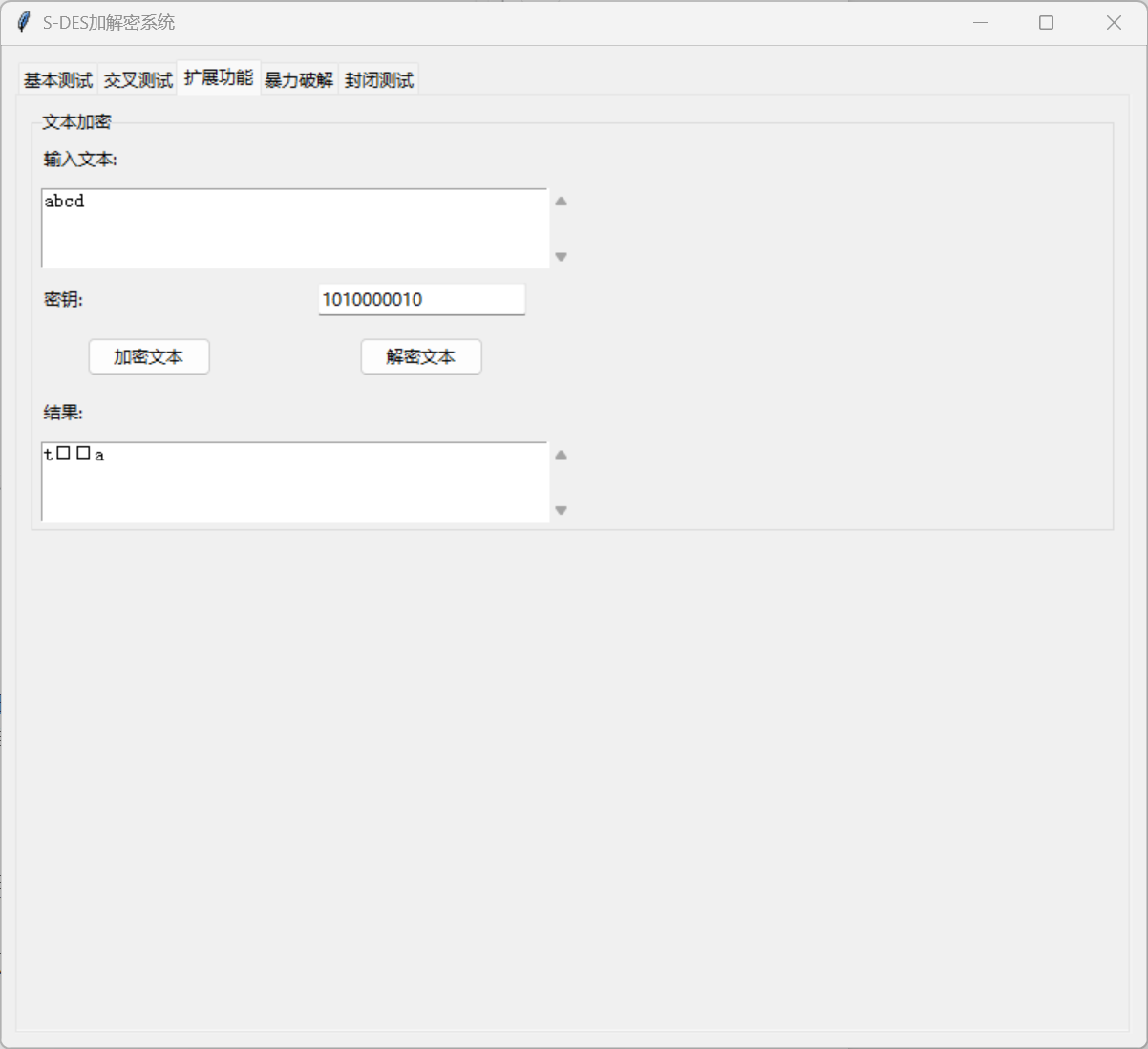
**3.2 第2关：交叉测试**

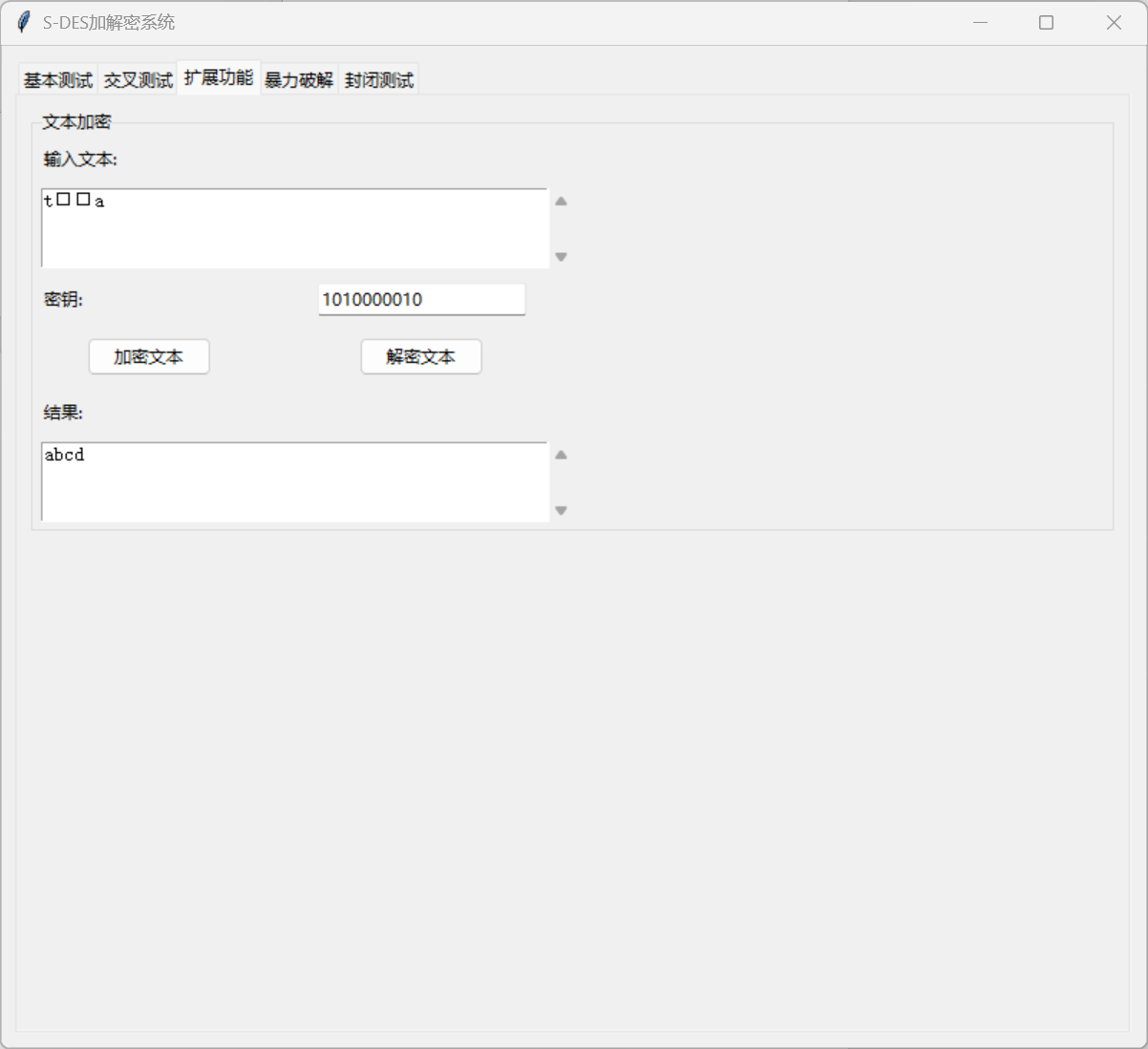
考虑到是**算法标准**，所有人在编写程序的时候需要使用相同算法流程和转换单元(P-Box、S-Box等)，以保证算法和程序在异构的系统或平台上都可以正常运行。

设有A和B两组位同学(选择相同的密钥K)；则A、B组同学编写的程序对明文P进行加密得到相同的密文C；或者B组同学接收到A组程序加密的密文C，使用B组程序进行解密可得到与A相同的P。



**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1 Byte)，对应地输出也可以是ASCII字符串(很可能是乱码)。



第3关“ASCII字符串加密：对文本进行加密解密”的测试结果为：明文（ASCII字符串）为“abcd”，10位密钥（二进制）为“1010000010”时，经过加密操作得到了对应的密文（二进制和ASCII形式），再经过解密操作后，解密结果为“abcd”，与原始明文一致，说明该S - DES算法能够对ASCII字符串进行有效的加密和解密，加密解密流程正常。

**3.4 第4关：暴力破解**

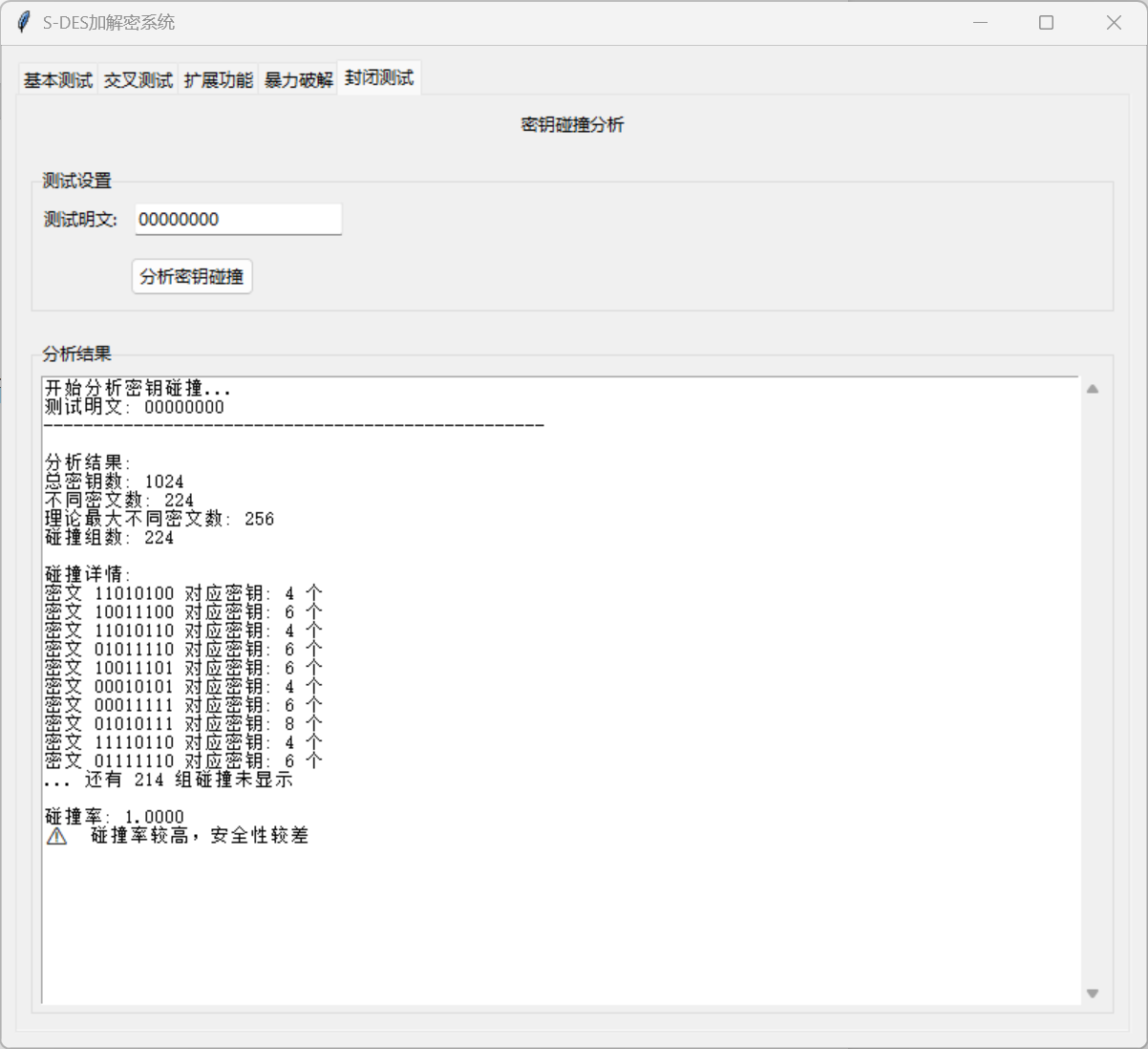
假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用暴力破解的方法找到正确的密钥Key。在编写程序时，你也可以考虑使用多线程的方式提升破解的效率。请设定时间戳，用视频或动图展示你在多长时间内完成了暴力破解。



第4关“暴力破解：通过明文和密文寻找密钥”的测试结果为：在8位明文（二进制）为`00000000`、8位密文（二进制）为`00011100`的情况下，经过暴力破解操作，成功找到6个匹配的密钥，为` 0000110101，0110000000， 0110100100，1010000010，1010100110， 1100110111`，这表明该S - DES算法的暴力破解功能正常，能够根据给定的明文和密文，找出对应的加密密钥。

**3.5 第5关：封闭测试**

根据第4关的结果，进一步分析，对于你随机选择的一个明密文对，是不是有不止一个密钥Key？进一步扩展，对应明文空间任意给定的明文分组[P\_{n}](" \l ")，是否会出现选择不同的密钥[K\_{i}\ne K\_{j}](" \l ")加密得到相同密文[C\_n](" \l ")的情况？



第5关“密钥碰撞分析：寻找产生相同密文的不同密钥”的测试结果为：在8位测试明文（二进制）为`00000000`的情况下，经过分析，共发224组密钥碰撞。例如，第1组密文`11010100 `包含4个不同的密钥，第2组密文`10011100`也存在对应的多个不同密钥，这表明该S - DES算法存在密钥碰撞现象，即不同的密钥对相同的明文进行加密，可能会得到相同的密文。