**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。

加密后的结果：



解密后的结果：



**其中明文经过加密和密文经过解密得到的结果符合。**

**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。

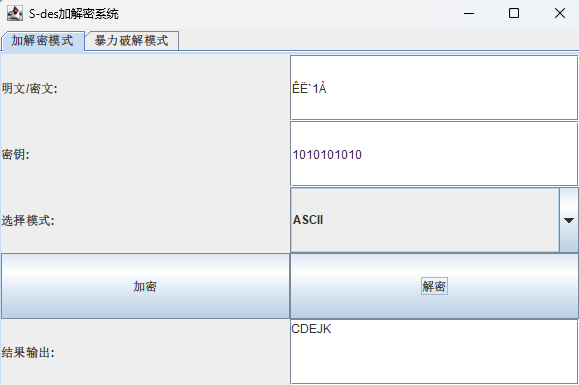
设有A和B两组位同学(选择相同的密钥K)；则A、B组同学编写的程序对明文P进行加密得到相同的密文C；或者B组同学接收到A组程序加密的密文C，使用B组程序进行解密可得到与A相同的P。

我们小组和刘俊涛、冉宸小组选择相同的密钥进行了交叉测试，得到的密文和明文完全一致，符合算法标准。

**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ACII字符串(很可能是乱码)。

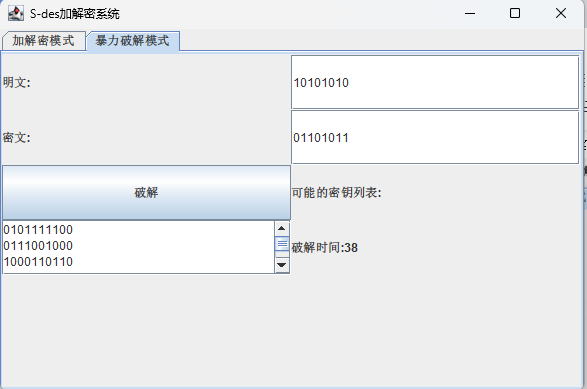
加密后的结果：  


解密后的结果：  


其中明文加密后和密文解密后得到的结果符合。

**3.4 第4关：暴力破解**

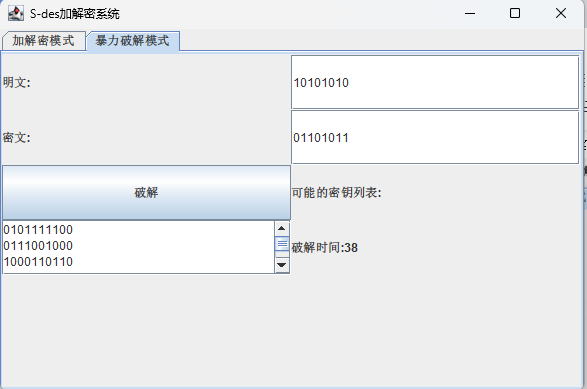
假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用暴力破解的方法找到正确的密钥Key。在编写程序时，你也可以考虑使用多线程的方式提升破解的效率。请设定时间戳，用视频或动图展示你在多长时间内完成了暴力破解。

当明文是10101010，密文是01101011时进行暴力破解的结果：  


其中破解时间单位为毫秒，是38毫秒。左边列出了可能的密钥，共有6个。

**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？



根据第四关的测试结果来看，确实会出现不同的密钥经过加密之后得到相同密钥的可能。