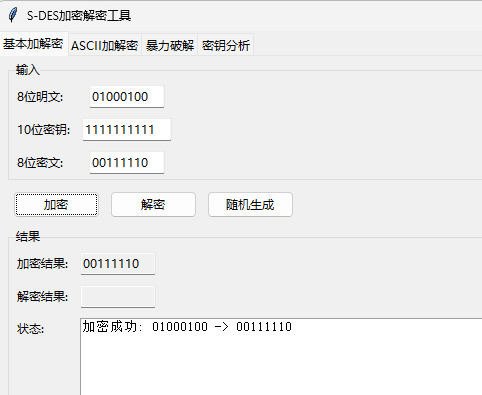
# 第一关

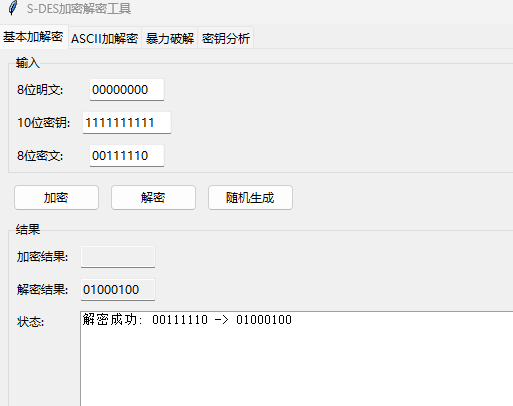
根据S-DES算法编写程序，提供GUI解密支持用户交互。输入8bit的数据和10bit的密钥，输出8bit的密文



# 第二关

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。

明文01000100，密钥1111111111，加密后的00111110密文成功解密为01000100

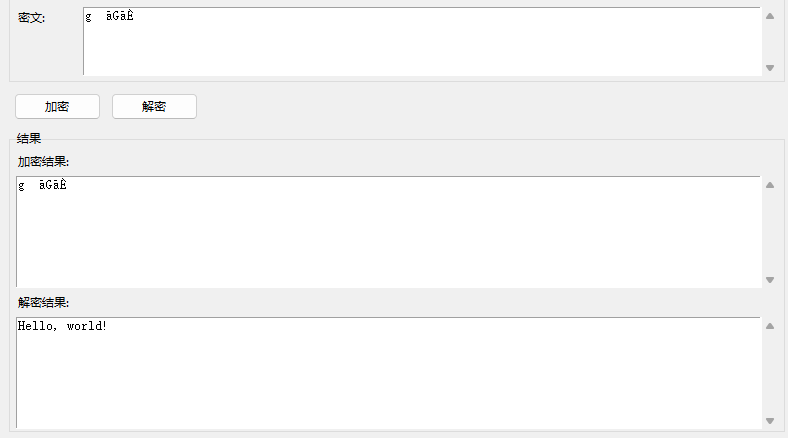


# 第三关

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)。

明文为“Hello，world！“，密钥为1111111111，加密与解密结果如下：

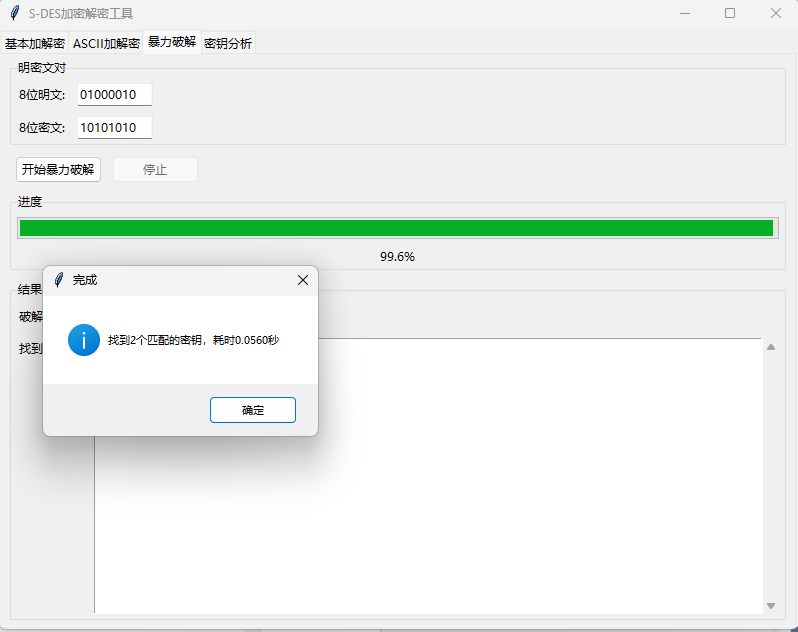


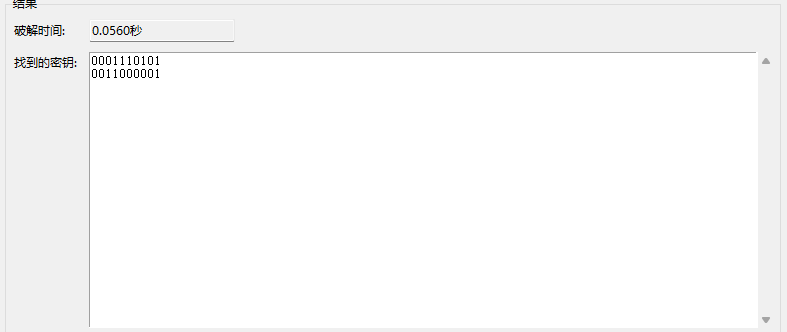


# 第四关

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。

明文为01000010，密文为10101010的情况下，找到两个匹配的密钥，用时0.056秒，因为一共只有1024个密钥，找到的密钥如下：





# 第五关

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}，是否会出现选择不同的密钥K\_{i}\ne K\_{j}加密得到相同密文C\_n的情况？

根据实验结果可知随机选择的明密文对下，可能存在多个密钥key，对于任意明文分组，可能出现不同密钥加密得到同一密文的情况。

