测试结果

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。

说明：在输入框内写入 8bit 数据，选择“二进制”单选按钮后输入任意 10bit 密钥，选中“加密”或“解密”单选框后，点击“立即执行”便得到相应结果。

图 1 加密二进制交互图示

图 2 解密二进制交互图示

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。

说明：以下是 A 组同学的实验数据，我们使用“1010101010”作为相同密钥，对该密文进行解密操作，得到输出与 A 组明文一致，验证成功。

图 1 A 组同学实验结果

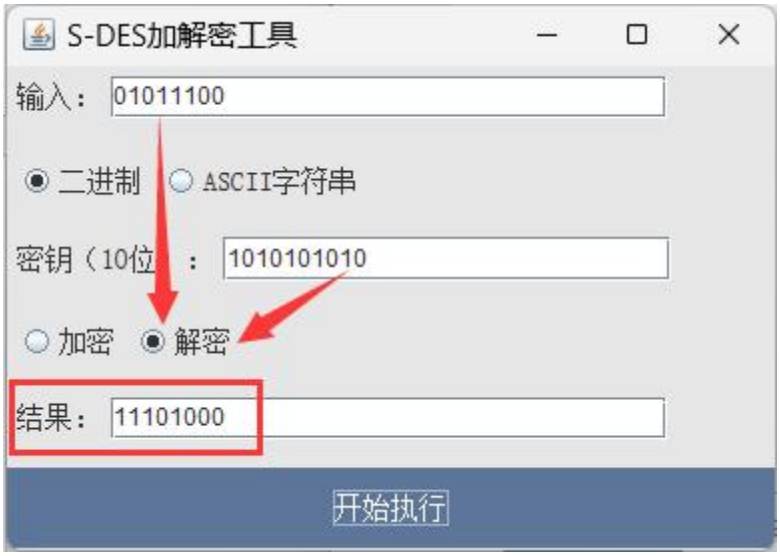

图 2 解密 A 组密文输出明文结果

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)。

说明:在输入框内写入 ASII 编码字符串,选择“ASII 字符串”单选按钮后输入任意 10bit 密钥，选中“加密”或“解密”单选框后，点击“立即执行”便得到相应结果。

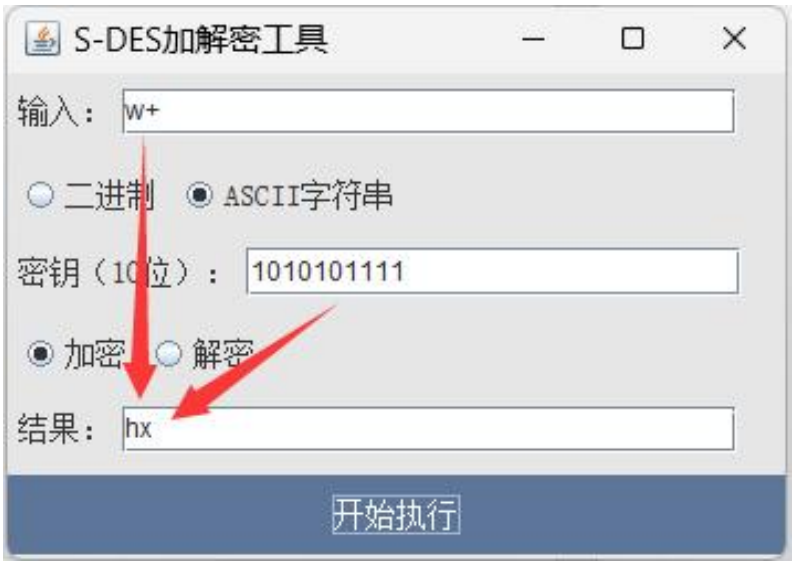

图 1 加密字符串交互图示

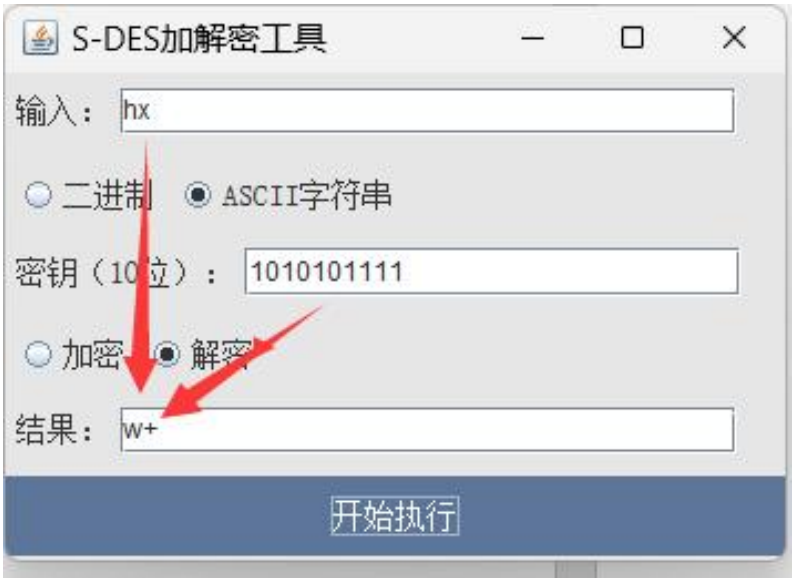

图 2 解密字符串交互图示

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。

说明：选择复选框（使用相同密钥的明、密文对数目），填入对应明密文对，点击“查找密钥”，得到暴力破解时长和相应密钥。

图 1　交互图示

图 2 破解两对明密文所得密钥及时长

图 3 破解三对明密文所得密钥及时长

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，是否会出现选择不同的密钥 $K_i \neq K_j$ 加密得到相同密文 C_n 的情况？

说明：对于随机选择的一个明密文对（明文：00100101；密文：10110000），可以找到不止一个密钥 K。

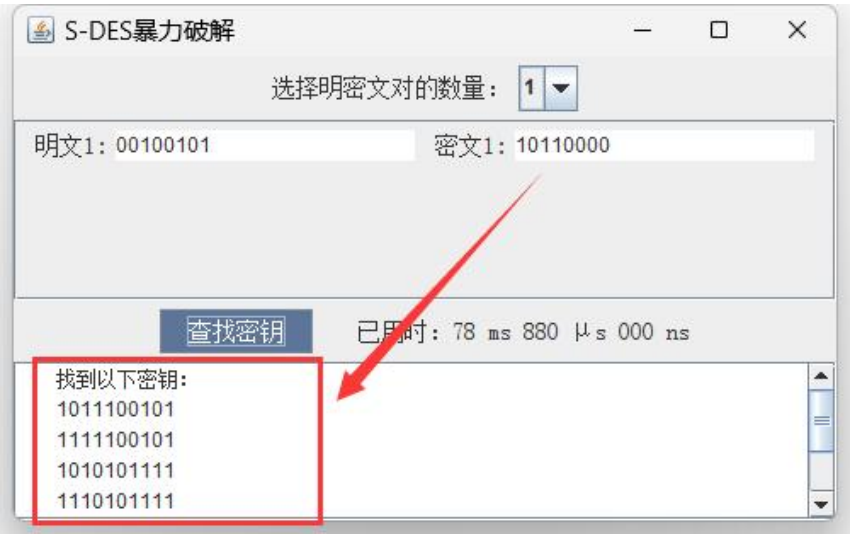

图 1 破解一对明密文所得密钥

说明：对于明文空间任意给定的明文分组 P_1, P_2, P_3（如图为明文 1，2，3），出现了选择不同的密钥 K_1，K_2（如图为密钥 0001000010，0101000010）加密得到相同密文 C_1, C_2, C_3（如图分别对应密文 1，2，3）的情况.

图 2 破解三对明密文所得密钥

结论：实验观察发现，密钥的第 2 位（从高位起）对明文的加密结果无影响。

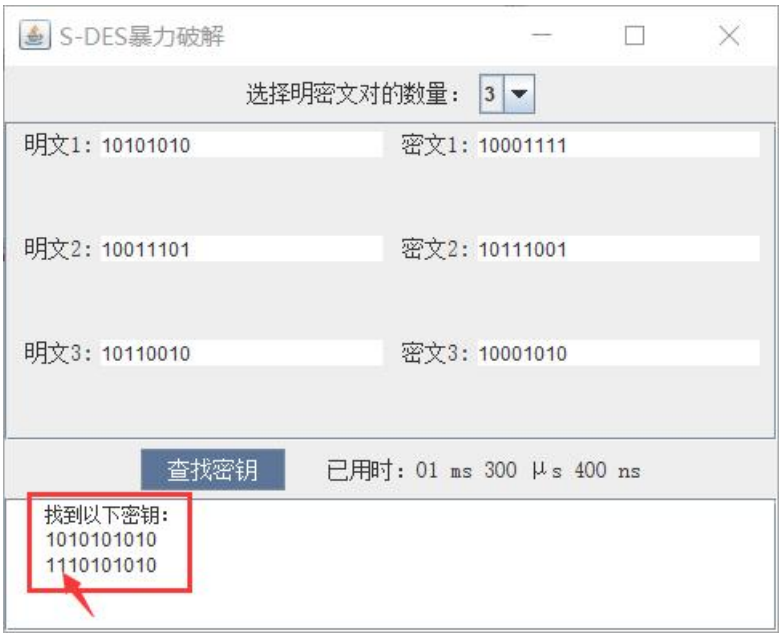

图 3 破解三对明密文对所得密钥仅第二位不同

图 4 破解四对明密文对所得密钥仅第二位不同