S-DES 加解密、破解程序用户手册

一、 程序简介

S-DES 是 DES 加密算法的简化版本，本程序实现了使用 10bit 密钥对单组 8bit 明文的 DES 加密。同时根据 DES 加密的对称特性，本程序同时具有解密功能，对于给定密文和密钥能够进行解密。给定明密文对，本程序能够进行暴力破解，查找可能匹配的密钥。为优化用户体验，本程序设计有 GUI 界面，支持字符串输入，并返回加密后的字符串。

二、 功能简介

1. 加密功能

用户输入明文串，选择输入模式，程序根据输入模式返回对应的密文串。用户可以指定密钥生成密文，若不指定密钥，则程序随机生成密钥，返回密钥加密后的密文，并在输出框中提示密钥。

2. 解密功能

用户输入密文串，选择输入模式，程序根据输入模式返回对应的明文串。用户可以指定密钥进行解密，若不指定密钥，则程序默认使用之前进行加密的密钥进行解密。

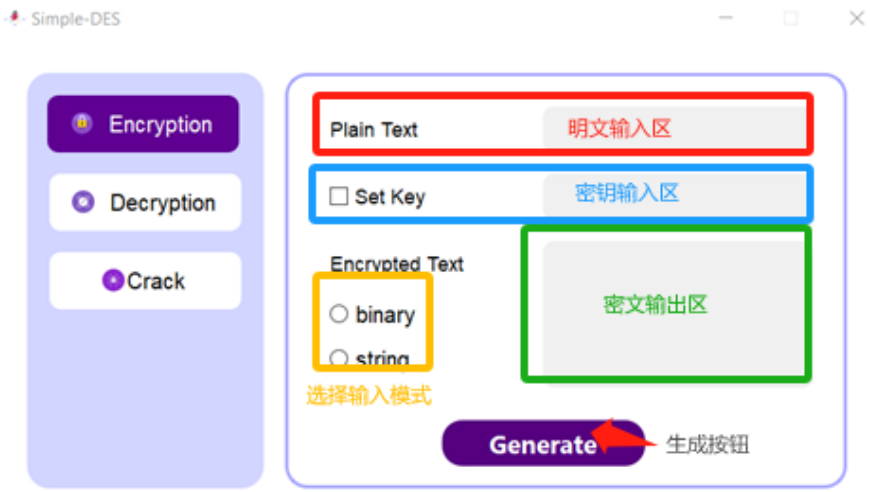
3. 破解功能

用户输入一对明密文，程序通过暴力破解的手段寻找可能的密钥，并将符合条件的密钥打印出来。

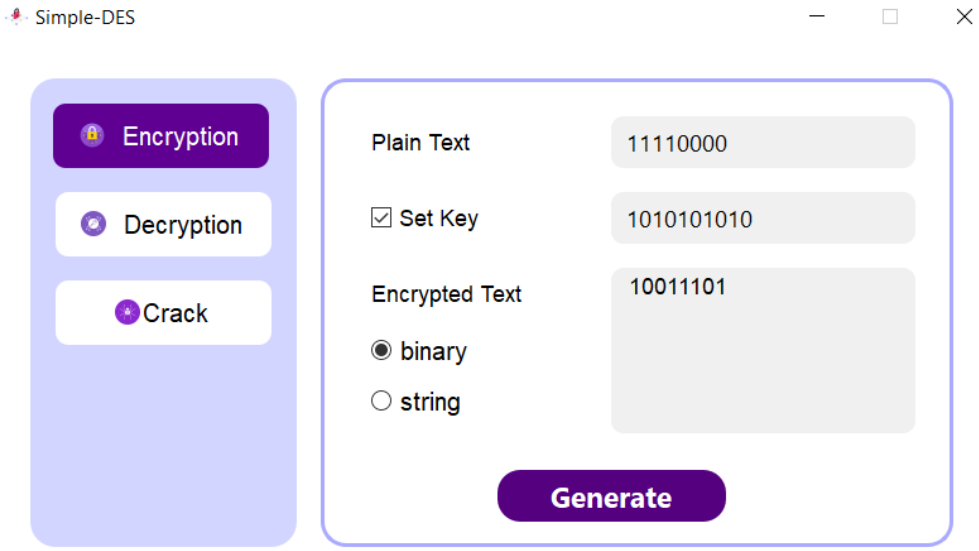
三、 使用说明

1. 加密功能

程序加密界面如下，左侧为功能选择区，右侧为输出区。

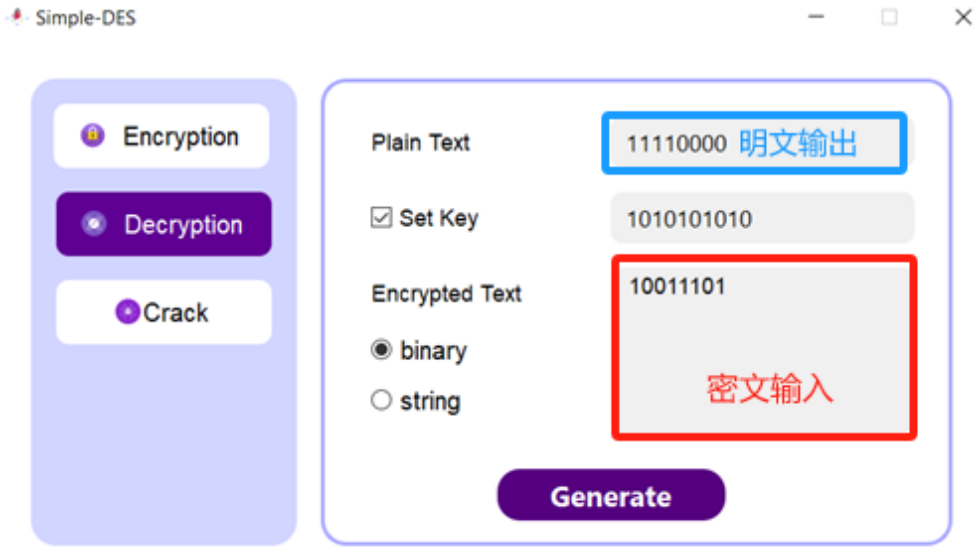


使用加密功能时需要在明文输入区输入明文二进制串或字符串，需选择对应 binary 或 string 选项，可选择 set key 选项，勾选后可输入密钥，不选择则系统随机生成密钥。点击 generate 生成密文，密文在下方密文区显示。使用示例如下：



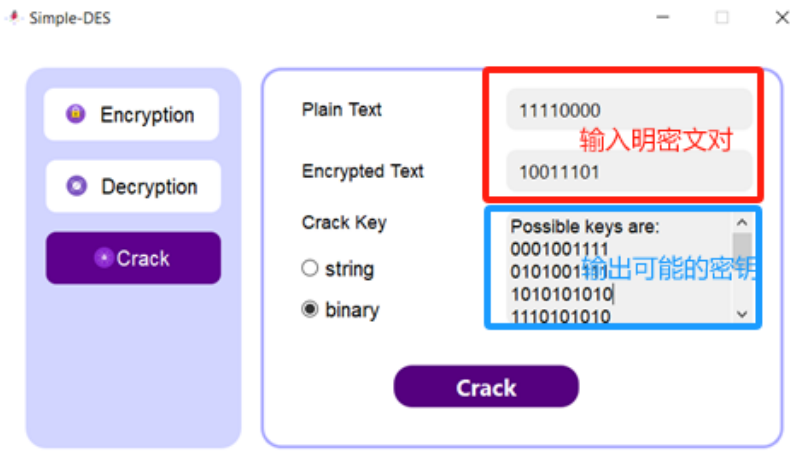
2. 解密功能

使用解密功能时，首先在功能区选择 Decryption，切换到解密界。在密文区输入密文，然后勾选设置密钥，输入密钥。支持密文字符串或密文二进制串输入，对应的明文根据密文的输入模式输出对应的形式。解密功能示例如下：

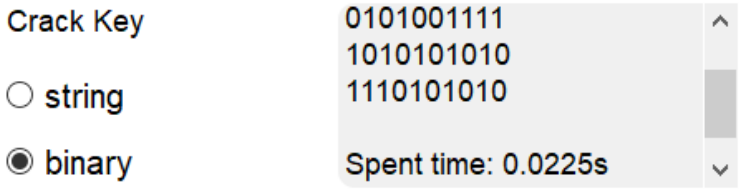


3. 破解功能

在功能区选择 Crack 选项，切换到破解界面，在明文区和密文区输入明密文对的明文和密文的二进制串，选择 binary 模式（暂未支持 string 模式），点击 Crack 按钮开始破解，在下方的密钥输出区将会返回可能的密钥结果。破解功能示例如下：

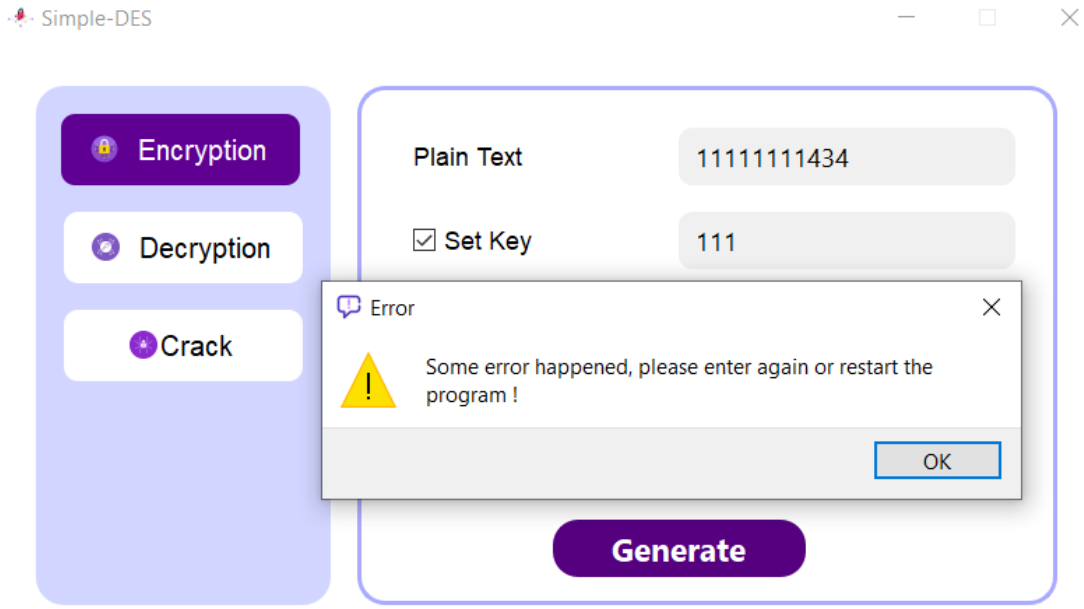


同时，在密钥输出底部会显示本次破解所花费的时间，如下图所示：



4. 程序出错提示

当输入不正确或程序出现内部错误的时候，程序会发出提示，需要进行重新输入，若多次输入都有错误，请尝试重启程序。



四、 注意事项

1. 本程序选用的密钥长度较短，不适宜加密重要信息
2. 本程序对字符串输入要求较为严格，虽然已使用正则表达式限制输入、进行输入检查，但仍存在错误格式的字符串输入的可能性，若程序崩溃，请重新进入本程序。