**用户指南**

**1.简介**

S-DES（简化数据加密标准）是一种教学用的对称加密算法，旨在帮助理解DES算法的基本原理。本工具提供了S-DES的加密、解密、ASCII字符串处理、暴力破解密钥以及密钥唯一性分析等功能，适用于学习和实验目的。

**2.系统要求**

操作系统：Windows、Linux 或 macOS

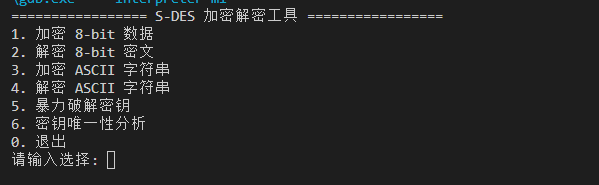
编译器：支持C++11或以上标准的编译器（如GCC、Clang、MSVC）

内存：至少 512MB RAM

处理器：支持多线程的处理器（建议用于暴力破解功能）

**3.使用方法**

启动程序后，将显示一个菜单界面，用户可以根据需要选择不同的功能。



用户可以输入相应的数字选择功能，输入 0 退出程序。

**4.功能详解**

加密 8-bit 数据

输入：8位二进制明文字符串（例如 10101010）和10位二进制密钥（例如 1010000010）。

输出：加密后的8位密文字符串。

解密 8-bit 密文

输入：8位二进制密文字符串和10位二进制密钥。

输出：解密后的8位明文字符串。

加密 ASCII 字符串

输入：任意长度的ASCII明文字符串和10位二进制密钥。

输出：加密后的ASCII密文字符串（可能显示为乱码）。

解密 ASCII 字符串

输入：加密后的ASCII密文字符串和10位二进制密钥。

输出：解密后的ASCII明文字符串。

暴力破解密钥

输入：已知的8位二进制明文和对应的8位二进制密文。

输出：找到的密钥（如果存在）以及破解所耗费的时间。

密钥唯一性分析

输入：8位二进制明文和对应的8位二进制密文。

输出：生成相同密文的所有密钥列表，并指示密钥是否唯一。

**5.常见问题与解决**

输入格式错误

确保输入的明文、密文和密钥为正确长度的二进制字符串（8位或10位），且仅包含字符 0 和 1。

加密/解密结果乱码

加密或解密ASCII字符串时，结果可能包含不可显示字符，这是由于二进制数据转换为ASCII字符时产生的。建议在处理二进制数据时使用8-bit数据选项。

暴力破解耗时较长

暴力破解功能已启用多线程加速，但仍可能耗费一定时间。确保系统具备足够的处理能力，并避免在资源受限的环境中使用。