用户指南

1. 介绍

1.1 什么是 S-DES 加密算法?

S-DES（Simplified Data Encryption Standard）是一种简化版的数据加密算法，旨在教育和理解加密算法的基本原理。它是对经典的数据加密标准（DES）的简化，具有较短的密钥长度和数据块长度，因此不适用于真正的安全应用。S-DES 通常用于教育、学术和基础加密概念的演示。

1.2 S-DES 的关键特点

（1）短密钥长度： S-DES 使用 10 位密钥，其中 2 位用于奇偶校验，因此实际有效密钥长度为 8 位。

（2）小数据块： S-DES 的数据块长度为 8 位二进制数。

（3）两轮加密： S-DES 通常包括两轮加密，每轮使用不同的子密钥。

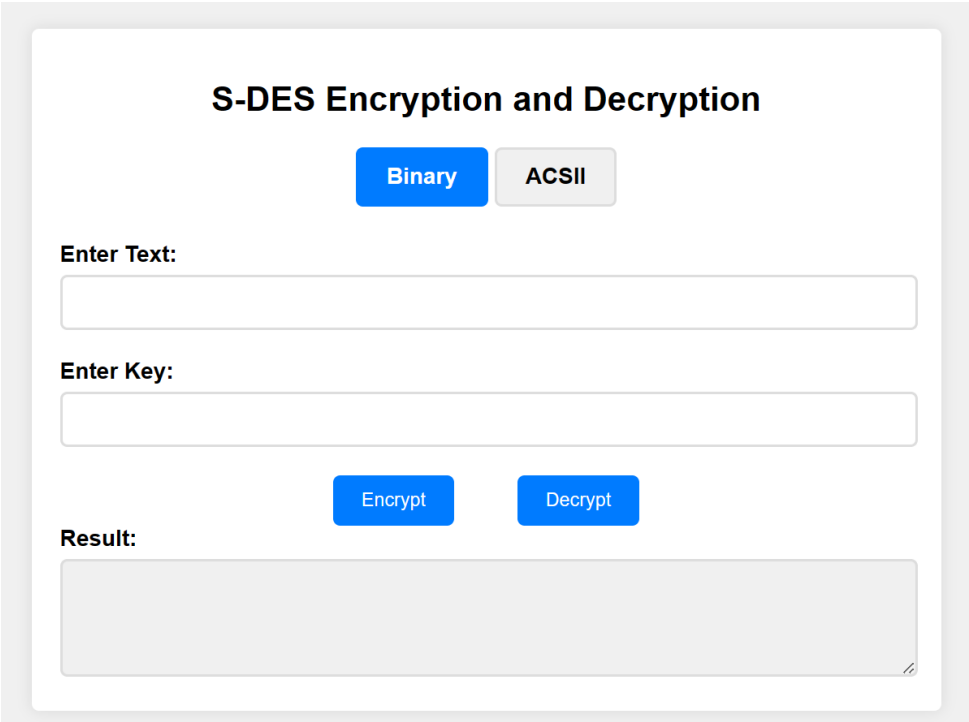
（4）置换和 S-盒： S-DES 使用置换表和 S-盒来混淆和替代数据。

（5）教育性质： S-DES 主要用于教育和理解加密算法的基本概念，而不是用于实际的数据安全。

1.3 用户指南概览

欢迎使用 S-DES 加密算法程序，此程序为 Simplified Data Encryption Standard (S-DES) 的一个简化版本，本用户指南旨在帮助教育和理解加密算法的基本原理，且由于 S-DES 的限制，该算法不适用于实际的安全应用。

1.4 用户界面



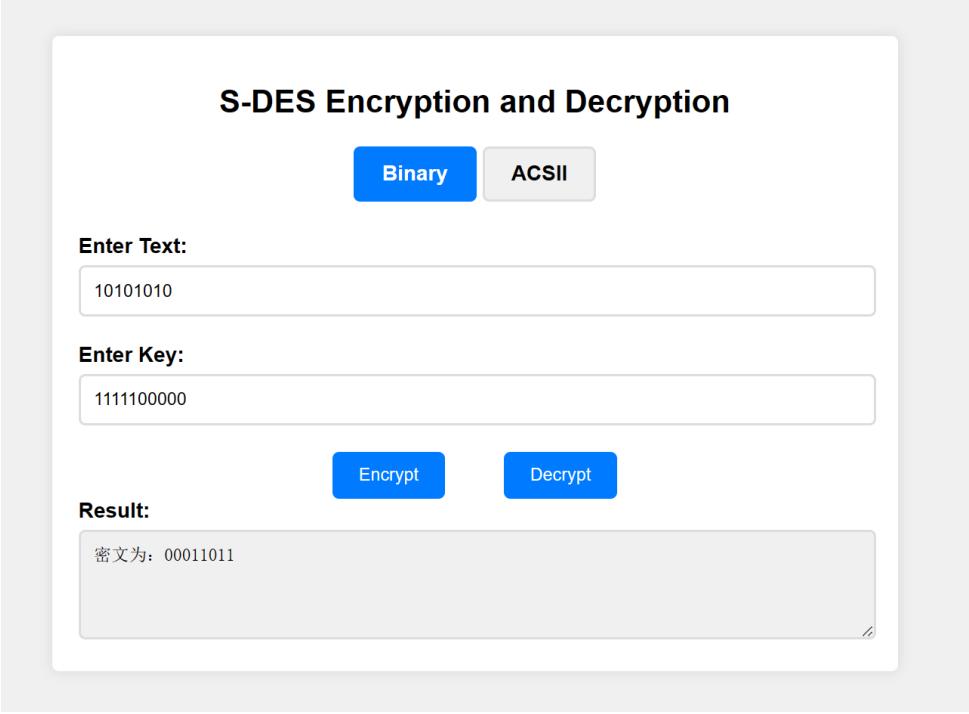
2. S-DES 算法流程

S-DES 算法包括以下主要步骤：
初始置换（Initial Permutation）
密钥生成（Key Generation）
轮函数（Round Function）
扩展置换（Expansion Permutation）
S-盒替代（S-Box Substitution）
P4 置换（Permutation P4）
两轮加密（Two Rounds of Encryption）
逆初始置换（Inverse Initial Permutation）

3. 使用说明

3.1 二进制加密

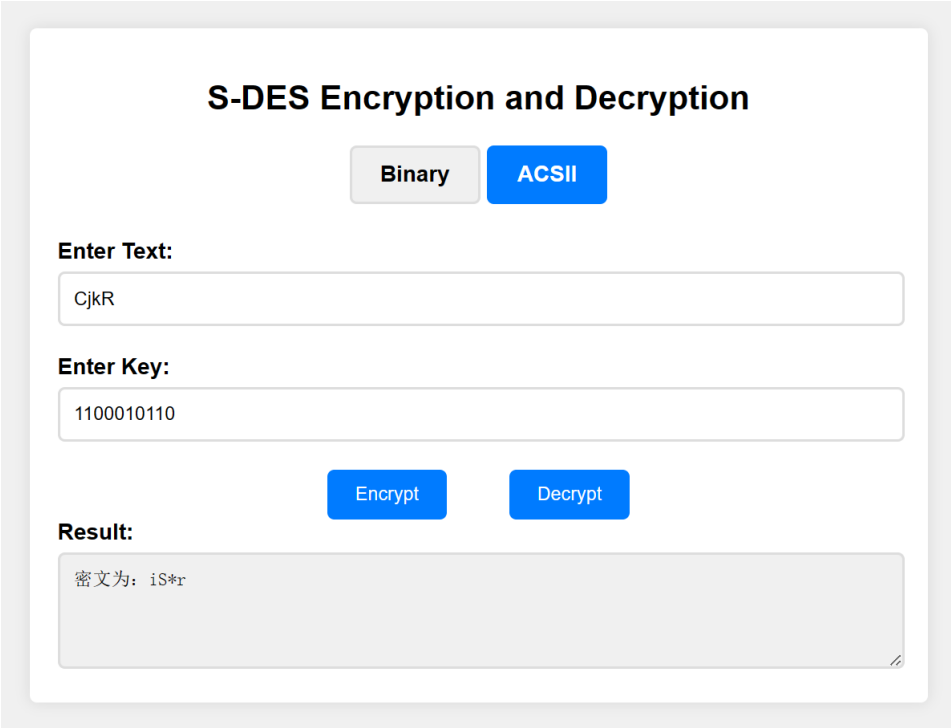
（1） 选择 Binary
（2） 输入二进制明文，长度为 8bit 位
（3） 输入密钥，长度为 10bit 位
（4） 点击“Encrypt”
（5） 在 Result 框中得到加密后的密文
示例：明文为 10101010
密钥为 1111100000
输出密文为 00011011



3.2 ACSII 字符串加密

（1） 选择 ACSII
（2） 输入 ACSII 字符串
（3） 输入密钥，长度为 10bit 位
（4） 点击“Encrypt”
（5） 在 Result 框中得到加密后的密文

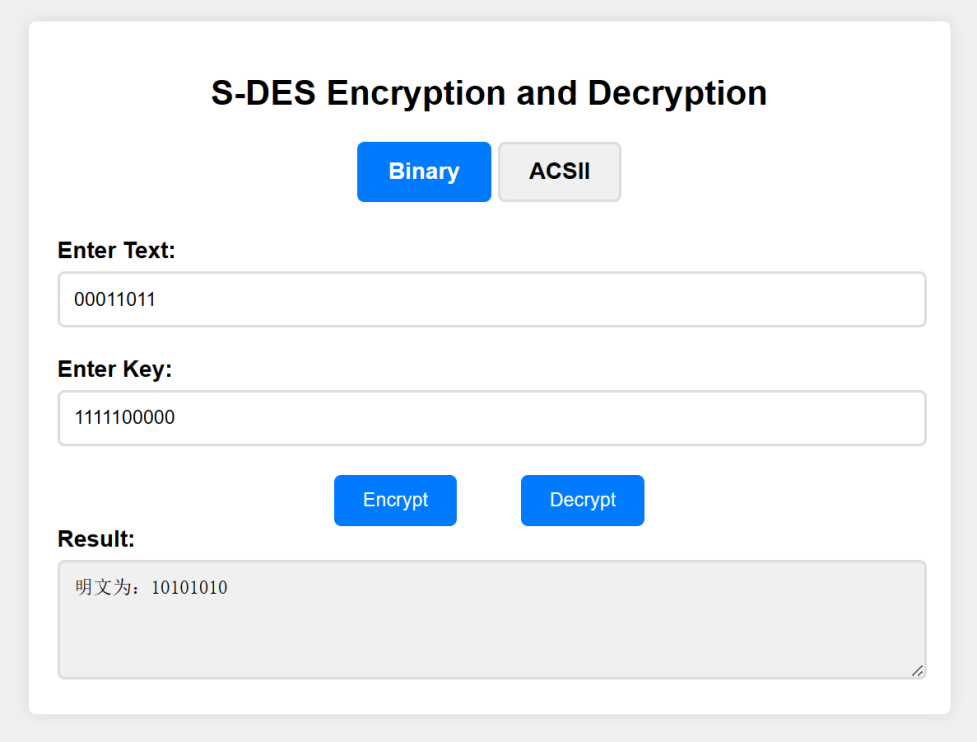
示例：明文为 CjkR
密钥为 1100010110
输出密文为 iS*r



3.3 二进制解密

（1） 选择 Binary
（2） 输入二进制密文，长度为 8bit 位
（3） 输入密钥，长度为 10bit 位
（4） 点击“Decrypt”
（5） 在 Result 框中得到解密后的明文

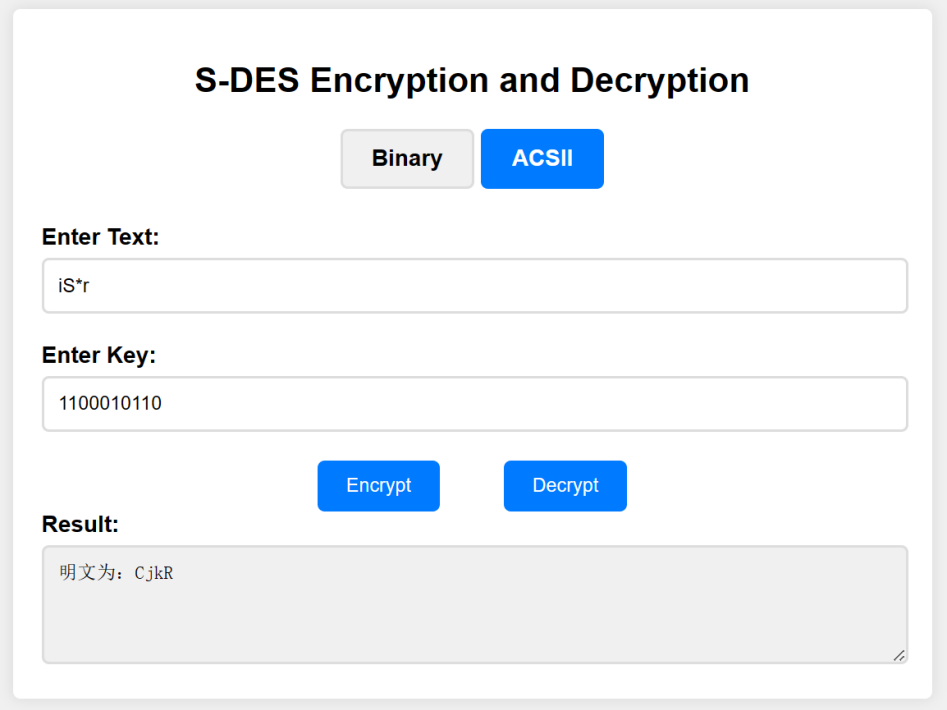
示例：密文为 00011011
密钥为 1111100000
输出明文为 10101010



3.4 ACSII 字符串解密

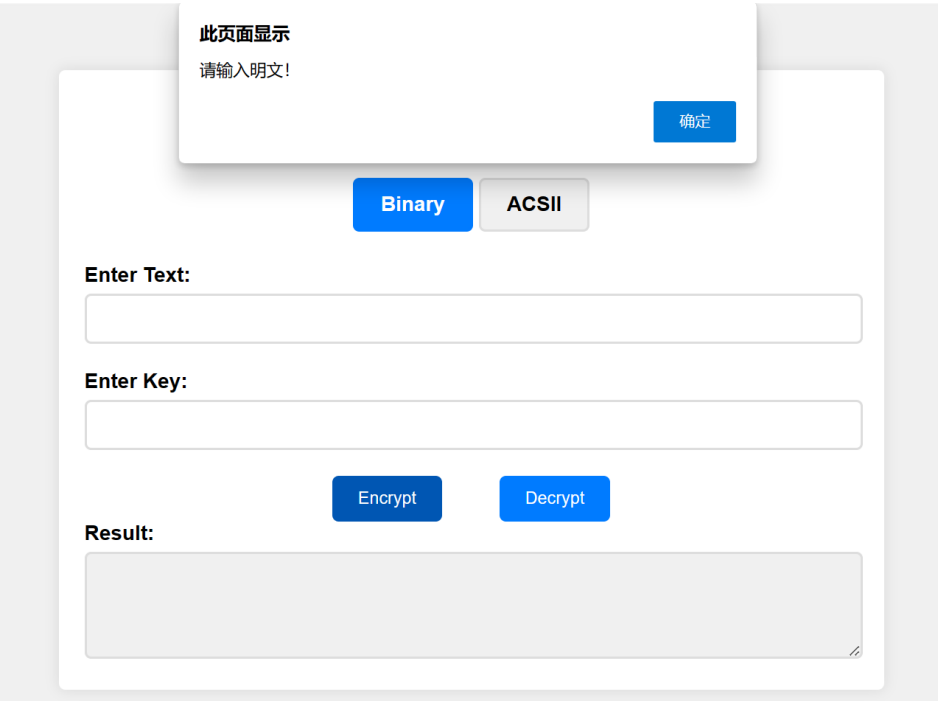
（1） 选择 ACSII
（2） 输入 ACSII 字符串
（3） 输入密钥，长度为 10bit 位
（4） 点击“Decrypt”
（5） 在 Result 框中得到解密后的明文

示例：明文为 iS*r
密钥为
输出密文为 CjkR

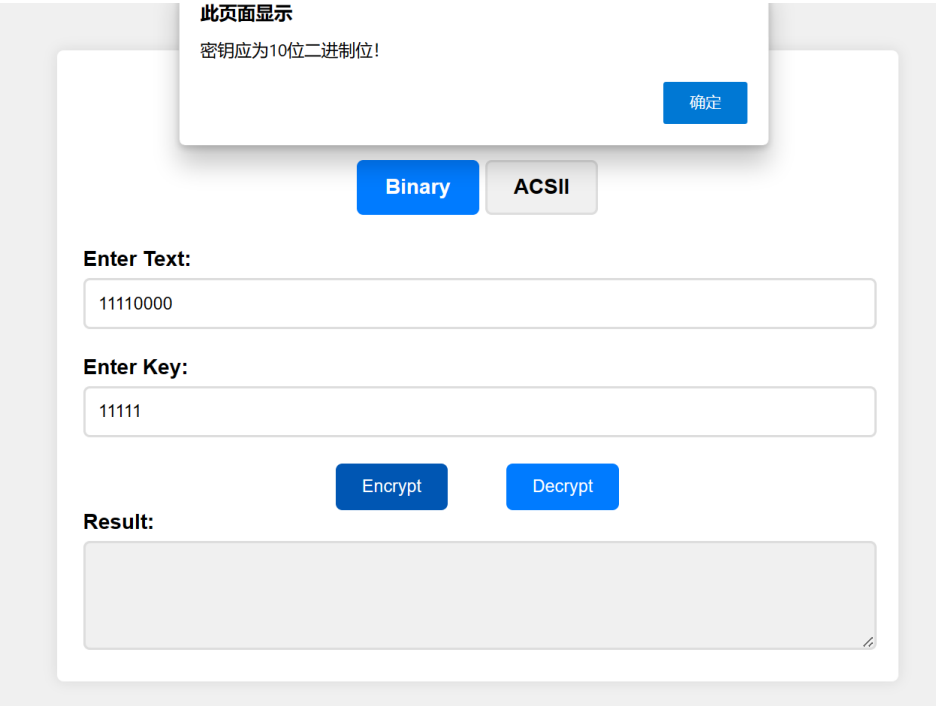


3.5 操作提示

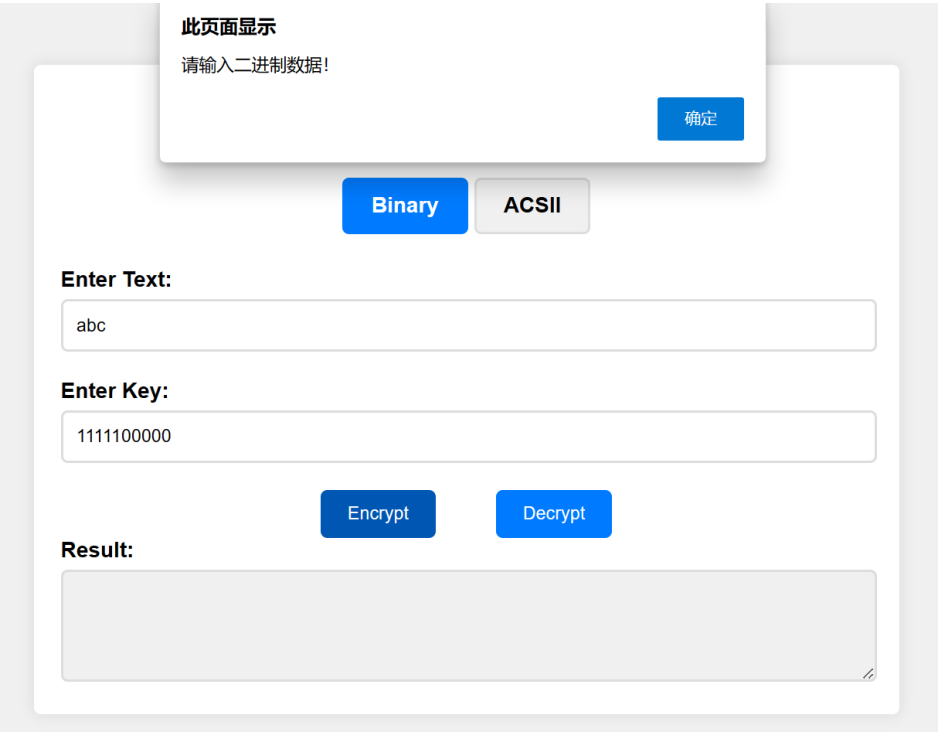
当明文为空时，提示“请输入明文！”



当密钥长度不是 10bit 位时，提示“密钥应为 10bit 位！”



当选择 Binary，但输入的 text 不是二进制时，提示“请输入二进制数据！”



4. 安全注意事项

请注意，S-DES 是一个教育性质的加密算法，其仅使用 8 位有效密钥，这意味着它不能够有效地处理大量数据，容易受到分析攻击。请勿将 S-DES 用于任何生产环境或实际应用中，以免造成数据泄漏或安全漏洞。如果您需要真正的数据安全，应该选择更强大、更安全的加密算法，如 AES（高级加密标准）等。

5. 参考资料

[1]Stallings, William. "Cryptography and Network Security: Principles and Practice." Prentice Hall, 2017.

[2]National Institute of Standards and Technology. "Data Encryption Standard (DES)." Federal Information Processing Standards Publication 46-3, 1999.

[3]Cryptography Stack Exchange. https://crypto.stackexchange.com/ .

[4]Khan Academy. "Introduction to Cryptography." https://www.khanacademy.org/computing/computer-science/cryptography .

6. 支持和反馈

如果您在使用程序时遇到问题或需要进一步帮助，请联系我们：leagueofcat@qq.com

7. 版本历史

版本 v1.0（2023 年 10 月 4 日），初始版本。