

# S-DES 加解密算法系统 操作手册

# 目录

S-DES 加解密算法系统 .....	1
一、 引言 .....	3
1.1 编写目的 .....	3
1.2 项目背景 .....	3
1.3 定义 .....	3
1.4 参考资料 .....	4
一、 软件概述 .....	4
2.1 目标 .....	4
2.2 功能 .....	4
2.3 性能 .....	4
二、 运行环境 .....	5
3.1 硬件 .....	5
3.2 支持软件 .....	5
三、 使用说明 .....	6
4.1 安装和初始化 .....	6
4.2 出错和恢复 .....	6
4.3 求助查询 .....	6
四、 运行说明 .....	6
5.1 运行表 .....	6
5.2 运行步骤 .....	7
六、 用户操作举例 .....	8
6.1 bit 形式加解密 .....	8
6.2 文件加解密 .....	9
6.3 明密文对照 .....	10
6.4 暴力破解 .....	11

# 一、引言

## 1.1 编写目的

本操作手册的编写目的是为了帮助用户全面了解和正确使用《加解密系统》，确保用户能够高效地操作系统，最大程度地发挥系统的功能和优势。本手册提供了详细的操作步骤和注意事项，旨在提高用户对系统的熟悉程度和操作技能，从而提升工作效率和系统使用效果。

本操作手册主要面向以下**读者对象**：

- **系统管理员**：负责系统的安装、配置和维护，确保系统的正常运行。
- **技术支持人员**：为用户提供技术支持和帮助，解决使用过程中遇到的问题。
- **普通用户**：日常使用系统进行文本加解密的工作人员，需了解系统的基本操作和功能使用。

通过本操作手册，以上读者对象可以全面了解系统的设计理念、功能模块和操作方法，确保在使用过程中能够正确操作，减少操作失误，提高工作效率。

## 1.2 项目背景

(1) **项目名称**：加解密系统

(2) **项目来源**：本项目源于重庆大学胡海波教授在信息安全导论课上对 S-DES 这一简化的数据加密标准的讲解，通过实现这一经典算法、建立 Web 用户页面，让用户可以直观、清晰、便捷地感受 S-DES 的功能，即对明文实现加密、对密文实现解密以及暴力破解密钥的功能。

## 1.3 定义

**专门术语的定义**：

- **S-DES**：S-DES（Simplified Data Encryption Standard）是一种简化版的数据加密标准，旨在用于教学和研究目的。相比于标准的 DES 算法，S-DES 具有较少的轮数和较短的密钥长度，使其更易于理解和实现，但安全性也相对较低。
- **加密**：加密是将明文（可读的信息）通过特定算法和密钥转换为密文（不可读的信息）的过程。其目的是保护信息内容，防止未经授权的访问和窃取。
- **解密**：解密是将密文通过特定算法和密钥转换回明文（可读的信息）的过程。它是加密的逆过程，允许授权用户恢复原始信息内容。
- **明文**：明文是指未经加密处理的、可以被人类直接读取和理解的原始信息或数据。它是加密过程的输入，经过加密后转换为密文。
- **密文**：密文是指经过加密算法和密钥处理后的、不可读的加密信息。它是加密过程的输出，只有拥有相应密钥的授权用户才能将其解密回明文。
- **密钥**：密钥是用于控制加密和解密过程的秘密参数或数据。它在加密算法中起到决定性作用，只有拥有正确密钥的用户才能成功解密密文，恢复明文。
- **暴力破解**：暴力破解是一种通过尝试所有可能的密钥组合，直到找到正确密钥以解密密文的方法。它是一种彻底但计算量巨大的攻击方式，通常用于破解对称加密或弱密码。

**缩写词的原文**：

- **S-DES: Simplified Data Encryption Standard**，是一种简化版的数据加密标准，旨在用于教学和研究目的。相比于标准的 DES 算法，S-DES 具有较少的轮数和较短的密钥长度，使其更易于理解和实现，但安全性也相对较低。

1.4 参考资料

【1】《数据加密标准 (DES) 规范》（美国国家标准与技术研究院）  
【2】《应用密码学》（Bruce Schneier 著）  
【3】《密码学与网络安全：原理与实践》（William Stallings 著）  
【4】《DES 及其安全性分析》（Eugene Spafford 著）  
【5】《理解密码学：学生与从业者的教科书》（Christof Paar, Jan Pelzl 著）

一、 软件概述

2.1 目标

本系统将基于 S-DES 加解密算法，设计“bit 模式”、“文件加解密”、“明密文对照”、“暴力破解”四个功能模块，通过 S-DES 原理进行明文加密、密文解密、密钥拆解，并且具备 bit 输入和文件上传两种形式的处理能力。此外，该系统将设计一个 GUI 用户界面，可视化加解密、暴力拆解的进度，让用户更清晰感受系统过程。

2.2 功能

序号	功能名称	功能描述
1	bit 形式加密	输入 8bit 形式的明文数据和 10bit 形式的密钥，系统将输出经 S-DES 算法加密的 8bit 密文。
2	bit 形式解密	输入 8bit 形式的密文数据和 10bit 形式的密钥，系统将输出经 S-DES 算法解密的 8bit 明文。
3	上传文本进行加密	选择待加密的本地的明文文件并输入 10bit 形式的密钥，系统将输出经 S-DES 算法加密的密文文件，并且可选择是否保存到本地。
4	上传文本进行解密	选择待解密的本地的密文文件并输入 10bit 形式的密钥，系统将输出经 S-DES 算法解密的明文文件，并且可选择是否保存到本地。
5	明密文对照	输入 10bit 密钥和明文后，可查看经 S-DES 加密的密文结果并将二者进行对比；同样的，输入 10bit 密钥和密文后，可查看经 S-DES 解密的明文结果并将二者进行对比。
6	暴力拆解获得密钥	对于已获得的明密文对，通过暴力拆解的方法获得密钥，此外，通过多线程提高拆解速率。

2.3 性能

➤ 精度

1. 加解密准确性:

系统应确保加解密操作的准确性，期望解密后的数据与原始数据完全一致。任何位错误率应低于 0.01%，以保证数据的完整性。

2. 密钥安全性:

生成和管理的密钥应能防止未授权访问，密钥的泄露率应控制在 1% 以下。这要求系统在密钥存储和传输过程中采用有效的安全措施。

➤ 时间特性

1. 加解密时间:

在服务器端完成加解密操作的时间应控制在 2 秒以内，以适应用户的即时需求。在高并发场景下，系统应能保持这一性能。

2. 响应时间:

系统的所有交互操作响应时间应控制在 0.5 秒以内，确保用户操作的流畅性和及时性。

3. 报告生成时间:

加密和解密操作后的报告生成时间应不超过 5 秒，即使在高负载情况下也能快速提供结果，方便用户查看和使用。

➤ 适应性

➤ 支持的并行操作用户数:

系统应能支持不限制终端数的访问，并在局域网环境下支持至少 100 个并行用户，在互联网环境下支持不少于 500 个并行用户，以适应不同规模的需求。

➤ 处理数据量:

系统应能处理单次操作不超过 1,000,000 个比特的数据，并支持最大 50MB 大小的密文，确保能应对大规模数据加解密任务。

➤ 报告流畅性:

由 S-DES 生成的加解密报告应流畅且格式正确，确保用户能够快速理解和使用报告内容，便于后续的安全分析和审计。

## 二、 运行环境

### 3.1 硬件

硬件类别	具体要求
服务器与网络接口	a) 支持至少 1Gbps 以太网连接，确保快速数据传输。 b) 支持高速数据存取和处理，如 SATA 或 SSD 硬盘接口。
用户终端设备	a) 支持标准网络接口的设备（PC、平板、手机）。 b) 浏览器应支持访问 Web 应用。

### 3.2 支持软件

支持软件类别	具体要求
Web 服务器	支持 HTTP/HTTPS 通信，提供 RESTful API 或 GraphQL 接口。
第三方服务接口	支持与第三方服务集成，如电子邮件、短信服务，采用 Webhooks 或

### 三、 使用说明

#### 4.1 安装和初始化

- (1) 存储形式：程序以压缩包（ZIP）的形式存储。
- (2) 解压缩：Introduction-to-Information-Security.zip
- (3) 用 vscode 运行 app.py

#### 4.2 出错和恢复

- 文件未找到：**  
含义：系统未能找到指定的文件。  
措施：检查文件路径是否正确，确保文件存在并重新尝试。
- 权限不足：**  
含义：用户没有执行该操作所需的权限。  
措施：联系系统管理员，获取必要的权限。
- 内存不足：**  
含义：系统内存不足，无法完成操作。  
措施：关闭其他不必要的程序，增加系统内存或优化内存使用。
- 输入错误：**  
含义：用户输入的密钥、明文或密文的长度和类型（数字、字符串或文件）不符合标准。  
措施：按照提示格式重新输入。

#### 4.3 求助查询

- 文档帮助：**  
查看系统的文档或用户手册，获取操作指南和问题解决方案。
- 技术支持：**  
电话支持：拨打软件开发小组成员电话，向开发人员寻求帮助。  
邮件支持：发送邮件至技术支持团队，描述问题并附上相关截图或日志文件。

### 四、 运行说明

#### 5.1 运行表

运行情况	运行目的
常规运行	正常使用系统进行明密文加解密和暴力拆解获得密钥。

测试运行	对系统进行功能测试和性能测试，验证其各项功能和性能指标。
维护运行	系统的维护和更新，包括算法优化和系统升级。
紧急恢复运行	在系统发生故障时，进行紧急恢复操作，确保系统快速恢复正常运行。

5.2 运行步骤

5.2.1 运行控制

**权限管理：**确保操作员具备必要的权限，可以访问和操作系统的各项功能。

**运行环境：**确保运行环境满足系统要求，包括操作系统、硬件配置。

5.2.2 操作信息

**运行目的：**

确定每次运行的具体目的，例如进行常规检测、测试新功能或进行系统维护。

**操作要求：**

确保操作员了解系统操作流程和相关要求，具备基本的技术知识和操作技能。

**启动方法：**

通过系统界面登录并启动检测功能。

**其他事项：**

- 确保系统日志记录开启，方便后续问题排查和分析。
- 定期检查系统状态，确保运行正常。

5.2.4 启动或恢复过程

**启动过程：**

登录系统，确保用户权限正确。

选择要运行的功能模块，输入必要的参数。

点击“启动”按钮，开始运行检测任务。

监控运行过程中的日志信息，确保无异常情况。

**恢复过程：**

检查系统日志，确定故障原因。

使用备份文件恢复数据，如从/backup/目录恢复。

重新启动系统或相关服务。

检查系统状态，确保恢复正常后，通知相关人员。

## 六、 用户操作举例

### 6.1 bit 形式加解密

加密算法系统

选择加密模式:

S-DES

bit模式

文件加解密

明密文对照

暴力破解

bit模式

密钥 (二进制):

请输入密钥

明文:

请输入明文

密文:

加密/解密结果

加密

解密

© 2024 信息安全导论.20221982潘铷葳20221385江佳艺

这是一个 bit 形式加解密操作页面，用于对 bit 形式的文本进行加解密处理。请按以下步骤操作：

- 输入 10bit 密钥：在“密钥（二进制）”输入框中，输入您希望使用的密钥。
- 输入明文：在“明文”输入框中，输入您的 10bit 形式的明文。
- 进行加密：点击“加密”按钮，加密结果将出现在“密文”显示框中。
- 输入密文：“在密文”输入框中，输入您的 10bit 形式的密文。
- 进行解密：点击“解密”按钮，解密结果将出现在“明文”显示框中。



6.2 文件加解密

加密算法系统

选择加密模式:

S-DES

bit模式

文件加解密

明文文对照

暴力破解

文件加解密

密钥 (二进制):

请输入密钥

选择文件:

选择文件

未选择文件

文件加密

文件解密

保存文件

© 2024 信息安全导论.20221982潘铷葳20221385江佳艺

这是文件加解密页面，请按照以下步骤操作：

- 输入 10bit 密钥：在“密钥（二进制）”输入框中，输入您希望使用的密钥。
- 选择文件：点击“选择文件”，在本地选择要加密或解密的文件。
- 文件加密/解密：根据加密或解密需求点击“文件加密”或“文件解密”按钮；
- 保存文件：点击“保存文件”按钮，保存加密或解密的文件、。

6.3 明密文对照

加密算法系统

选择加密模式:

S-DES

bit模式

文件加解密

明密文对照

暴力破解

明密文对照

密钥 (二进制):

请输入密钥

明文:

请输入明文

密文 (二进制) :

对应的密文

© 2024 信息安全导论.20221982潘铷葳20221385江佳艺

这是明密文对照功能页面，请按照以下步骤操作：

- 输入密钥：输入 10bit 二进制密钥；
- 输入明文：输入字符串作为明文；
- 获得密文：S-DES 对明文进行加密后，密文实时显示在“对应的密文”窗口。

### 6.4 暴力破解

## 加密算法系统

选择加密模式:

S-DES

bit模式

文件加解密

明密文对照

暴力破解

### 暴力破解

线程数量:

4

明文:

00110101

密文:

11001101

开始暴力破解

破解成功, 找到的密钥为: 1101010011, 1001010011

© 2024 信息安全导论.20221982潘钊藏20221385江佳艺

这是暴力拆解页面，请按照以下步骤操作：

- 填写进程数量：改变进程数量可控制拆解速率。
- 输入明文：输入 **10bit** 明文。
- 输入密文：输入 **10bit** 密文。
- 开始暴力破解：点击“开始暴力破解”按钮，等待进度条加载完毕后，下方结果显示栏将显示出暴力拆解的密钥结果。