S-DES 加密解密程序开发手册

1. 简介

本开发手册提供了一个基于 S-DES（Simplified Data Encryption Standard）算法的加密解密程序的详细接口文档，用于对数据进行小规模加密和解密操作。通过使用 S-DES 算法，您可以保护敏感数据的安全性，确保其在传输过程中不被未经授权的人员访问。

在这份开发手册中，您将找到以下内容：

(1)组件及接口概述：介绍了加密解密程序的各个组件和对外提供的接口。

(2)使用示例：提供了一些示例代码，展示了如何使用加密解密程序完成加密和解密操作。

(3)注意事项：列出了在使用加密解密程序时需要注意的事项和建议。

通过阅读本开发手册，您将了解如何正确使用 S-DES 加密解密程序，以及如何保护您的数据安全。请确保遵守安全性原则，并妥善保管生成的密钥，以免数据被未授权的人员获取。

2. 组件及接口概述

本程序包含以下组件及其对应的接口：

2.1 Key Generation（密钥生成）

generateKey: 生成两个 8 位的子密钥。

参数：

p10：密钥置换盒。

p8: 密钥压缩装置。

key（密钥）: 加密所使用的密钥。

返回值：

keys: 一个 2 行 8 列数组，保存加密过程需要的两个子密钥。

2.2 Encrypt（加密）

encryptData: 使用 S-DES 算法对二进制明文进行加密。

参数：

plaintext（明文）: 需要加密的明文数据。

key（密钥）: 加密所使用的密钥。

返回值：

ciphertext（密文）: 加密后的密文数据。

encryptASCII: 使用 S-DES 算法对字符串明文进行加密。

参数：

plaintextASCII（明文）: 需要加密的明文数据。

key（密钥）: 加密所使用的密钥。

返回值：

ciphertextASCII（密文）: 加密后的密文数据。

2.3 Decrypt（解密）

decryptData: 使用 S-DES 算法对二进制明文进行解密。

参数：

ciphertext（密文）: 需要解密的密文数据。

key（密钥）: 解密所使用的密钥。

返回值：

plaintext（明文）: 解密后的明文数据。

decryptASCII: 使用 S-DES 算法对字符串密文进行解密。

参数：

ciphertextASCII（明文）: 需要解密的密文数据。

key（密钥）: 解密所使用的密钥。

返回值：

plaintextASCII（明文）: 解密后的明文数据。

2.4 UI 界面展示：

调用 UI 包下的 Main 类下的 main 函数，即可展示 UI 界面。

3. 使用示例（基于 java）

3.1 密钥生成

```
int[]P10 = {3, 5, 2, 7, 4, 10, 1, 9, 8, 6};
int[] P8 = {6, 3, 7, 4, 8, 5, 10, 9};

int[][] keys = KeyGeneration.generateKey(P10, P8, key);
System.out.println("密钥生成为: "+Arrays.toString(keys));
```

3.2 加密示例

```
String key = "0000011111";
```

```
int[] plaintext = {1,0,1,0,1,0,1,0};
int[] ciphertext = encryptData(plaintext, key);
System.out.println("数组类型 8bits 加密输出结果: " +
Arrays.toString(ciphertext));

String plaintextASCII = "fire an 10pm";
String ciphertextASCII = encryptASCII(plaintextASCII, key);
System.out.println("ASCII 码加密输出结果: " + ciphertextASCII);
```

3.3 解密示例

```
String key = "0000011111";
int[] ciphertext = {1, 1, 1, 0, 1, 0, 0, 0};
int[] plaintext = decryptData(ciphertext, key);
System.out.println("数组类型 8bits 解密输出结果: " +
Arrays.toString(plaintext));

String ciphertextASCII = "çlËcyË}Üé";
String plaintextASCII = decryptASCII(ciphertextASCII, key);
System.out.println("ASCII 码解密输出结果: " + plaintextASCII);
```

4. 注意事项

在使用加密解密功能之前，请确保输入的密钥和数据符合算法要求。

请妥善保管密钥，不要将密钥泄露给他人。

本程序仅适用于小规模的数据加密需求，不建议用于对大量或敏感数据进行加密。