**S-AES（Simplified Advanced Encryption Standard）**

**开发手册**

1. **概述**

本手册旨在介绍S-AES（Simplified Advanced Encryption Standard）加密算法的实现细节，包括算法的基本结构、关键函数以及如何使用这些函数进行加密操作。

1. **算法结构**

S-AES算法由以下基本组成部分构成：

* **初始轮密钥加（AddRoundKey）**：将密钥与明文进行异或操作。
* **轮函数**：包括半字节替代（SubBytes）、行移位（ShiftRows）和列混淆（MixColumns）。
* **最终轮密钥加（AddRoundKey）**：在最后一轮加密后，将密钥与中间结果进行异或操作。

1. **关键函数说明**
2. 半字节替代（SubBytes）

半字节替代是S-AES中最核心的步骤，它通过一个固定的S盒（Substitution Box）对每个半字节进行替换。S盒是一个4x4的矩阵，其中每个元素是一个8位的值。对于16位的输入，每个半字节都会被S盒中的一个值替换。

1. 行移位（ShiftRows）

行移位是S-AES中的一个步骤，它通过将每一行循环左移一定的位数来打乱数据。在S-AES中，第一行保持不变，第二行左移一位，第三行左移两位，第四行左移三位。

1. 列混淆（MixColumns）

列混淆是S-AES中的一个步骤，它通过将每一列与一个固定的矩阵进行矩阵乘法操作来打乱数据。在S-AES中，这个矩阵是一个4x4的矩阵，每个元素是一个8位的值。

1. 密钥扩展

S-AES使用一个16位的密钥，并通过密钥扩展算法生成两个16位的轮密钥。密钥扩展算法包括以下步骤：

1. 将16位的密钥分成两个8位的部分（w0和w1）。
2. 对w1进行循环左移一位（RotWord）。
3. 对循环左移后的结果进行S盒替换（SubWord）。
4. 将替换后的结果与一个固定的轮常量（Rcon）进行异或操作。
5. 将结果与w0进行异或操作，生成第一个轮密钥（w2）。
6. 将w2与w1进行异或操作，生成第二个轮密钥（w3）。
7. **加解密过程说明**

### 加密过程

S-AES的加密过程包括以下步骤：

1. **初始轮密钥加**：将明文与第一个轮密钥（w2）进行异或操作。
2. **第一轮**：
   * **半字节替代（SubBytes）**：使用S盒对每个半字节进行替换。
   * **行移位（ShiftRows）**：将每一行循环左移一定的位数。
   * **列混淆（MixColumns）**：对每一列进行矩阵乘法操作。
   * **轮密钥加（AddRoundKey）**：将结果与第二个轮密钥（w3）进行异或操作。
3. **最终轮**：
   * **半字节替代（SubBytes）**：使用S盒对每个半字节进行替换。
   * **行移位（ShiftRows）**：将每一行循环左移一定的位数。
   * **轮密钥加（AddRoundKey）**：将结果与第一个轮密钥（w2）进行异或操作。

### 解密过程

S-AES的解密过程是加密过程的逆过程，包括以下步骤：

1. **初始轮密钥加**：将密文与第一个轮密钥（w2）进行异或操作。
2. **第一轮**：
   * **逆行移位（Inverse ShiftRows）**：将每一行循环右移一定的位数。
   * **逆半字节替代（Inverse SubBytes）**：使用逆S盒对每个半字节进行替换。
   * **轮密钥加（AddRoundKey）**：将结果与第二个轮密钥（w3）进行异或操作。
   * **逆列混淆（Inverse MixColumns）**：对每一列进行逆矩阵乘法操作。
3. **最终轮**：
   * **逆行移位（Inverse ShiftRows）**：将每一行循环右移一定的位数。
   * **逆半字节替代（Inverse SubBytes）**：使用逆S盒对每个半字节进行替换。
   * **轮密钥加（AddRoundKey）**：将结果与第一个轮密钥（w2）进行异或操作。
4. **使用说明**
5. **加密**

**输入**

明文：16位二进制字符串（只包含0和1）或ASCII码字符串。

密钥：16位二进制字符串（只包含0和1）。

**输出**

密文：16位二进制字符串（加密后的结果）或ASCII码字符串。

1. **解密**

**输入**

密文：16位二进制字符串（只包含0和1）或ASCII码字符串。

密钥：16位二进制字符串（只包含0和1）。

**输出**

明文：16位二进制字符串（只包含0和1）或ASCII码字符串。

1. **注意事项**

**输入验证：**确保输入的明文和密钥都是有效的二进制字符串或ASCII码字符串，并且长度正确，否则无法得到正确加解密结果。

**安全性：**S-AES的密钥长度较短（仅16位），因此其安全性较低，不适合用于实际的安全应用。建议使用更安全的加密算法，如AES，其密钥长度为128位、192位或256位。

1. **结论**

本手册详细介绍了S-AES加密算法的实现细节，包括关键函数的说明和使用方法。通过遵循本手册的指导，用户可以轻松地实现S-AES加密和解密过程。