开发手册

简介

S-AES （Simplified Advanced Encryption Standard）是一种简化版的 AES 算法，主要用于教学和学习加密原理。它保留了 AES 的核心概念，但简化了操作，使其更适合学习和理解加密算法的基本原理。该开发手册提供了 S-AES 算法的概述、详细步骤和函数接口。

1. 算法概述

S-AES 是一种对称密钥加密算法，它采用了与 AES 类似的操作，但更为简化。S-AES 加密过程包括以下步骤：

1.S-AES变换：包括半字节替换、行位移、列混淆和轮密钥加

2.密钥扩展：将初始密钥通过一系列操作生成轮密钥。

2.算法步骤

2.1 S-AES变换

字节替换：使用 S-box 对数据进行非线性替换。

行位移：对数据进行行位移操作。

列混淆：在有限域 GF2^4上进行列混淆操作。

轮密钥加：使用轮密钥与数据进行异或操作。

2.2 密钥扩展16 位初始密钥被分成两个8位字。

文本

低可信度描述已自动生成3.接口

3.1 密钥扩展

轮密钥生成 generate\_key(key)

输入参数：16bit的密钥

输出参数：三个轮密钥W1，W2，W3

3.2 S-AES变换

3.2.1 半字节代替 halfByteSubstitude(arr)

输入参数：16bit数组

输出参数：经过S盒替换处理后16bit数组

3.2.2 逆半字节代替inverseHalfByteSubstitude(arr)

输入参数：16bit数组

输出参数：经过S盒替换处理后16bit数组

3.2.3 行移位rowShift(arr)

输入参数：16bit数组

输出参数：经过行移位处理后16bit数组

3.2.4 列混淆 columnMix（arr）

输入参数：16bit数组

输出参数：经过列混淆处理后16bit数组

3.2.5 逆列混淆inverseColumnMix(arr)

输入参数：16bit数组

输出参数：经过逆列混淆处理后16bit数组

3.3 加密函数encode(key,content)

输入参数：16bit明文，16bit密钥

输出参数：经过加密后的16bit密文

3.4 解密函数decode(key,content)

输入参数：16bit密文，16bit密钥

输出参数：经过解密后的16bit明文

3.5 拓展功能

3.5.1 字符串转二进制String\_change(string)

输入参数：待加密的字符串

输出参数：包括每个字符的二进制编码数组

3.5.2 加密字符串encode\_str(key,string)

输入参数：16bit密钥，待加密的字符串

输出参数：经过加密后的密文字符串

3.5.3 解密字符串decode\_str(key,string)

输入参数：16bit密钥，待解密的字符串

输出参数：经过解密后的明文字符串

3.6.3 双重加密算法doubleEncode(key,content)

输入参数：32bit的密钥、16bit明文

输出参数：经过双重加密后的16bit的密文

3.6.4 双重解密算法doubleDecode(key,content)

输入参数：32bit的密钥、16bit密文

输出参数：经过双重解密后的16bit的明文

3.6.5 三重加密算法tribleEncode(key,content)

输入参数：32bit的密钥、16bit明文

输出参数：经过三重加密后的16bit的密文

3.6.6 三重解密算法tribleDecode(key,content)

输入参数：32bit的密钥、16bit密文

输出参数：经过三重解密后的16bit的明文

3.6.7 CBC加密字符串encodeCBCString(key,string)

输入参数：16bit密钥，明文字符串

输出参数：经过CBC加密后的16bit的密文

3.6.8 CBC解密字符串decodeCBCString(key,string)

输入参数：16bit密钥，密文字符串

输出参数：经过CBC解密后的16bit的明文

3.6.9 中间相遇攻击Meet\_in\_the\_Middle(ciphertext,plaintext)

输入参数：16bit密文，16bit明文

输出参数：经过中间相遇攻击得到的可能密钥