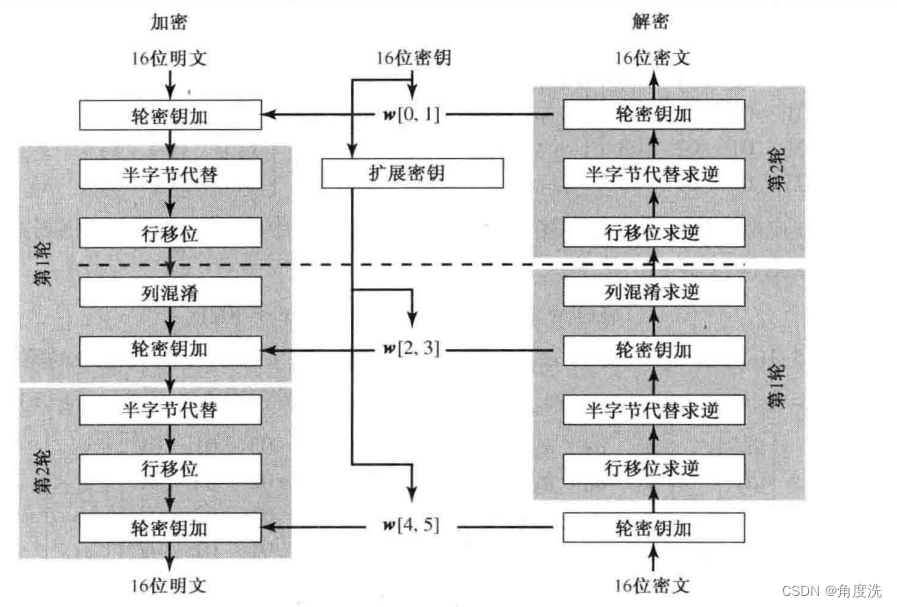
# 开发手册

1. **算法简介**

SAES（Symmetric Key Algorithm for Encryption and Decryption）算法是一种对称加密算法，它使用相同的密钥进行加密和解密操作。这种算法在安全性上比非对称加密算法更高，因为相同的密钥容易被破解，而不同的密钥需要更强大的计算能力才能破解。

SAES算法的工作原理是将需要加密的明文数据通过一系列的加密操作，生成密文数据。解密过程与加密过程相同，只是密钥的使用顺序相反。在加密和解密过程中，SAES算法会使用一些数学运算和置换操作，例如异或、置换、轮转等，以增加数据的复杂性和安全性。

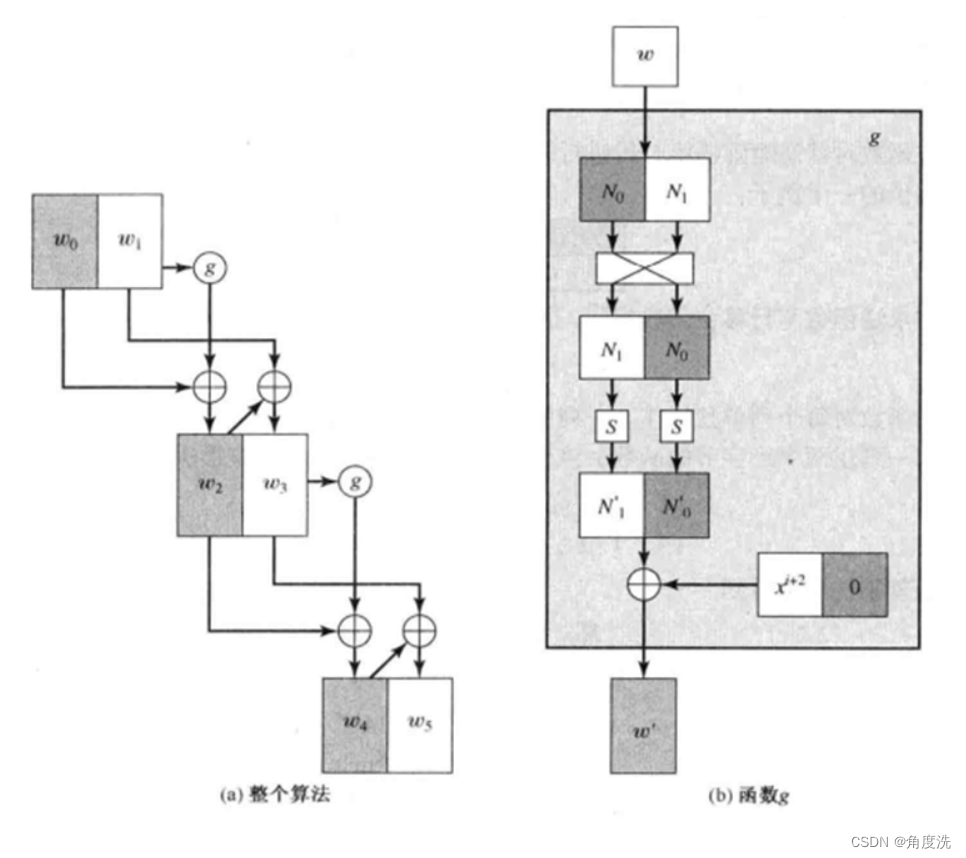
SAES算法具有较高的安全性和效率，因此在数据加密和保护方面得到了广泛的应用。然而，由于现代计算机的计算能力不断提高，SAES算法的安全性也面临着越来越大的挑战。因此，在使用SAES算法时，需要注意选择足够长和足够复杂的密钥，并采取其他安全措施来保护密钥和数据的安全性。



1. **功能需求分析**

**2.1基本装置设定**

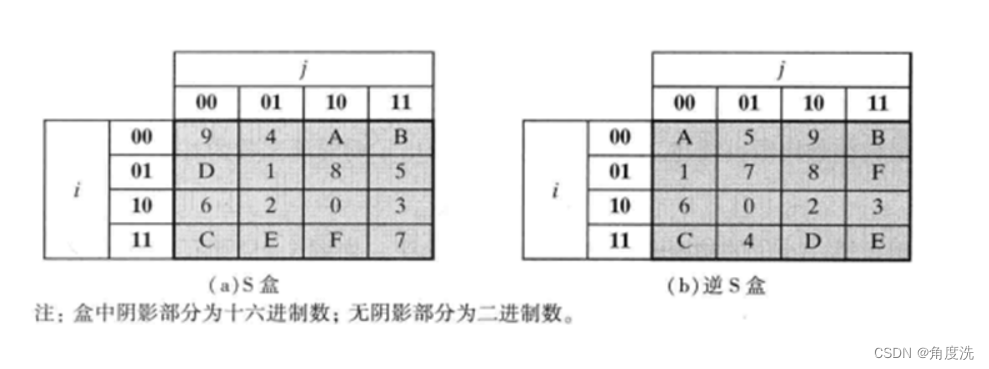
2.1.1密钥扩展



将16位密钥分为左右两部分，每一部分各8位。记原始密钥为第0个密钥。

2.1.2S盒

在计算第i个密钥时，首先将第i-1个密钥的右半部分（8位）进行左循环移位，即将第i-1个密钥的右半部分的左右4位进行交换，再将左循环移位后的第i-1个密钥的右半部分（8位）进行S盒置换，S-AES的S盒定义如下：



2.1.3****进行S盒置换后需要与轮常数进行异或****

示意图中函数g的步骤，将第i-1个密钥的右半部分（8位）执行完上述步骤后得到g(第i-1个密钥的右半部分)，将其与第i-1个密钥的左半部分（8位）进行****异或****得到第i个密钥的左半部分。

第i个密钥的右半部分由第i个密钥的左半部分与第i-1个密钥的右半部分进行****异或****得到。

**2.2基本功能实现**

根据S-AES算法编写和调试程序，提供GUI解密支持用户交互。输入可以是16bit的数据和16bit的密钥，输出是16bit的密文。

且考虑到**算法标准**，编写程序的时候需要使用相同算法流程和转换单元（替换盒、列混淆矩阵等），以保证算法和程序在异构的系统或平台上都可以正常运行。

**2.3扩展功能**

2.3.1扩展功能

加密算法的数据输入可以是ASII编码字符串(分组为1 Byte)，对应地输出也可以是ACII字符串(很可能是乱码)

2.3.2多重加密

1.双重加密

将S-AES算法通过双重加密进行扩展，分组长度仍然是16 bits，但密钥长度为32 bits。

2.中间相遇攻击

假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用中间相遇攻击的方法找到正确的密钥Key(K1+K2)。

3.三重加密

将S-AES算法通过三重加密进行扩展，按照32 bits密钥Key(K1+K2)的模式进行三重加密解密。

1. **设计实现**

3.1基本功能实现与扩展功能

部分js代码：

var s = [

    [9, 4, 10, 11],

    [13, 1, 8, 5],

    [6, 2, 0, 3],

    [12, 14, 15, 7]];

var antis = [

    [10, 5, 9, 11],

    [1, 7, 8, 15],

    [6, 0, 2, 3],

    [12, 4, 13, 14]];

var tihuanwei = [

    [0, 0, 0, 0],

    [0, 0, 0, 1],

    [0, 0, 1, 0],

    [0, 0, 1, 1],

    [0, 1, 0, 0],

    [0, 1, 0, 1],

    [0, 1, 1, 0],

    [0, 1, 1, 1],

    [1, 0, 0, 0],

    [1, 0, 0, 1],

    [1, 0, 1, 0],

    [1, 0, 1, 1],

    [1, 1, 0, 0],

    [1, 1, 0, 1],

    [1, 1, 1, 0],

    [1, 1, 1, 1]];

var rcon1 = [1, 0, 0, 0, 0, 0, 0, 0];

var rcon2 = [0, 0, 1, 1, 0, 0, 0, 0];

//function SAES(mingwen, key) {

function x\_de\_n\_fang\_cheng\_fx(xfx, a) {

    if (a[0] === 0) {

        for (let i = 0; i < 3; i++) {

            xfx[i] = a[i + 1];

        }

    } else {

        xfx[1] = a[2];

        xfx[2] = a[3] === 1 ? 0 : 1;

        xfx[3] = 1;

    }

}

function chengfa(a, b) {

    let result = new Array(4).fill(0);

    let xfx = new Array(4).fill(0);

    x\_de\_n\_fang\_cheng\_fx(xfx, a);

    let x2fx = new Array(4).fill(0);

    x\_de\_n\_fang\_cheng\_fx(x2fx, xfx);

    let x3fx = new Array(4).fill(0);

    x\_de\_n\_fang\_cheng\_fx(x3fx, x2fx);

    if (b[0] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= x3fx[i];

        }

    }

    if (b[1] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= x2fx[i];

        }

    }

    if (b[2] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= xfx[i];

        }

    }

    if (b[3] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= a[i];

        }

    }

    return result;

}

function yihuo8(a, b) {

    let t = new Array(8).fill(0);

    for (let i = 0; i < 8; i++)

        t[i] = a[i] ^ b[i];

    return t;

}

function yihuo4(a, b) {

    let t = new Array(4).fill(0);

    for (let i = 0; i < 4; i++)

        t[i] = a[i] ^ b[i];

    return t;

}

function s\_he\_tihuan(temp) {

    let t1 = 2 \* temp[0] + temp[1];

    let t2 = 2 \* temp[2] + temp[3];

    let t3 = 2 \* temp[4] + temp[5];

    let t4 = 2 \* temp[6] + temp[7];

    let tihuan1 = s[t1][t2];

    let tihuan2 = s[t3][t4];

    for (let i = 0; i < 4; i++)

        temp[i] = tihuanwei[tihuan1][i];

    for (let i = 0; i < 4; i++)

        temp[i + 4] = tihuanwei[tihuan2][i];

}

function antis\_he\_tihuan(temp) {

    let t1 = 2 \* temp[0] + temp[1];

    let t2 = 2 \* temp[2] + temp[3];

    let t3 = 2 \* temp[4] + temp[5];

    let t4 = 2 \* temp[6] + temp[7];

    let tihuan1 = antis[t1][t2];

    let tihuan2 = antis[t3][t4];

    for (let i = 0; i < 4; i++)

        temp[i] = tihuanwei[tihuan1][i];

    for (let i = 0; i < 4; i++)

        temp[i + 4] = tihuanwei[tihuan2][i];

}

function zuoyi(temp) {

    for (let i = 4; i < 8; i++) {

        let t = temp[0][i];

        temp[0][i] = temp[1][i];

        temp[1][i] = t;

    }

}

function youyi(temp) {

    for (let i = 4; i < 8; i++) {

        let t = temp[1][i];

        temp[1][i] = temp[0][i];

        temp[0][i] = t;

    }

}

function g(temp, rcon) {

    let t = new Array(8).fill(0);

    for (let i = 0; i < 8; i++)

        t[i] = temp[i];

    for (let i = 0; i < 4; i++) {

        let tt = t[i + 4];

        t[i + 4] = t[i];

        t[i] = tt;

    }

    s\_he\_tihuan(t);

    return yihuo8(t, rcon);

}

function liehunxiao(mingwen) {

    let si\_de2jinzhi = [0, 1, 0, 0];

    let m00 = new Array(4).fill(0);

    let m10 = new Array(4).fill(0);

    let m01 = new Array(4).fill(0);

    let m11 = new Array(4).fill(0);

    for (let i = 0; i < 4; i++) {

        m00[i] = mingwen[0][i];

        m10[i] = mingwen[0][i + 4];

        m01[i] = mingwen[1][i];

        m11[i] = mingwen[1][i + 4];

    }

    let n00 = yihuo4(m00, chengfa(si\_de2jinzhi, m10));

    let n10 = yihuo4(chengfa(si\_de2jinzhi, m00), m10);

    let n01 = yihuo4(m01, chengfa(si\_de2jinzhi, m11));

    let n11 = yihuo4(chengfa(si\_de2jinzhi, m01), m11);

    for (let i = 0; i < 4; i++) {

        mingwen[0][i] = n00[i];

        mingwen[0][i + 4] = n10[i];

        mingwen[1][i] = n01[i];

        mingwen[1][i + 4] = n11[i];

    }

}

function antiliehunxiao(mingwen) {

    let s1\_de2jinzhi = [1, 0, 0, 1];//9

    let s2\_de2jinzhi = [0, 0, 1, 0];//2

    let m00 = new Array(4).fill(0);

    let m10 = new Array(4).fill(0);

    let m01 = new Array(4).fill(0);

    let m11 = new Array(4).fill(0);

    for (let i = 0; i < 4; i++) {

        m00[i] = mingwen[0][i];

        m10[i] = mingwen[0][i + 4];

        m01[i] = mingwen[1][i];

        m11[i] = mingwen[1][i + 4];

    }

    let n00 = yihuo4(chengfa(s1\_de2jinzhi, m00), chengfa(s2\_de2jinzhi, m10));

    let n01 = yihuo4(chengfa(s1\_de2jinzhi, m01), chengfa(s2\_de2jinzhi, m11));

    let n10 = yihuo4(chengfa(s2\_de2jinzhi, m00), chengfa(s1\_de2jinzhi, m10));

    let n11 = yihuo4(chengfa(s2\_de2jinzhi, m01), chengfa(s1\_de2jinzhi, m11));

    for (let i = 0; i < 4; i++) {

        mingwen[0][i] = n00[i];

        mingwen[0][i + 4] = n10[i];

        mingwen[1][i] = n01[i];

        mingwen[1][i + 4] = n11[i];

    }

}

function lunmiyaojia(mingwen, key) {

    for (let i = 0; i < 2; i++)

        for (let j = 0; j < 8; j++)

            mingwen[i][j] ^= key[i][j];

}

function SAES(mingwen, key) {

    let key1 = new Array(2).fill(new Array(8).fill(0));

    let key2 = new Array(2).fill(new Array(8).fill(0));

    key1[0] = yihuo8(key[0], g(key[1], rcon1));

    key1[1] = yihuo8(key1[0], key[1]);

    key2[0] = yihuo8(key1[0], g(key1[1], rcon2));

    key2[1] = yihuo8(key2[0], key1[1]);

    lunmiyaojia(mingwen, key);

    s\_he\_tihuan(mingwen[0]);

    s\_he\_tihuan(mingwen[1]);

    zuoyi(mingwen);

    liehunxiao(mingwen);

    lunmiyaojia(mingwen, key1);

    s\_he\_tihuan(mingwen[0]);

    s\_he\_tihuan(mingwen[1]);

    zuoyi(mingwen);

    lunmiyaojia(mingwen, key2);

    return mingwen;

}

function SAES\_decrypt(mingwen, key) {

    var key1 = new Array(2);

    for (let i = 0; i < 2; i++) {

        key1[i] = new Array(8);

    }

    var key2 = new Array(2);

    for (let i = 0; i < 2; i++) {

        key2[i] = new Array(8);

    }

    // 解密过程

    key1[0] = yihuo8(key[0], g(key[1], rcon1));

    key1[1] = yihuo8(key1[0], key[1]);

    key2[0] = yihuo8(key1[0], g(key1[1], rcon2));

    key2[1] = yihuo8(key2[0], key1[1]);

    lunmiyaojia(mingwen, key2);

    youyi(mingwen);

    antis\_he\_tihuan(mingwen[0]);

    antis\_he\_tihuan(mingwen[1]);

    lunmiyaojia(mingwen, key1);

    antiliehunxiao(mingwen);

    youyi(mingwen);

    antis\_he\_tihuan(mingwen[0]);

    antis\_he\_tihuan(mingwen[1]);

    lunmiyaojia(mingwen, key);

    return mingwen;

}

var text = new Array(2);

for (let i = 0; i < 2; i++) {

    text[i] = new Array(8);

}

var key = new Array(2);

for (let i = 0; i < 2; i++) {

    key[i] = new Array(8);

}

var stext = new Array(2);

for (let i = 0; i < 2; i++) {

    stext[i] = new Array(8);

}

//先定义一个空数组装准备输入的数据

//连接、定义输入框，提交按钮和显示框

var dPut = document.getElementById("put");

var dBtn = document.getElementById("btn");

var dInt = document.getElementById("int");

dBtn.onclick = function array() {

    let tt = dPut.value;

    if (tt.length == 16 & (key[0].length + key[1].length) == 16) {

        for (let i = 0; i < 2; i++) {

            for (let j = 0; j < 8; j++) {

                text[i][j] = parseInt(tt[i \* 8 + j]);

            }

        }

        stext = SAES(text, key);

        let s = "密文为： ";

        for (let i of stext)

            for (let j of i)

                s += j;

        dInt.value = s;

        text = new Array(2);

        for (let i = 0; i < 2; i++) {

            text[i] = new Array(8);

        }

        stext = new Array(2);

        for (let i = 0; i < 2; i++) {

            stext[i] = new Array(8);

        }

    }

    else

        alert("请输入16bit密钥和16bit明文")

}

//输入密钥

var dPut2 = document.getElementById("put2");

var dBtn2 = document.getElementById("btn2");

dBtn2.onclick = function array() {

    key = new Array(2);

    for (let i = 0; i < 2; i++) {

        key[i] = new Array(8);

    }

    let tt = dPut2.value;

    if (tt.length == 16) {

        for (let i = 0; i < 2; i++) {

            for (let j = 0; j < 8; j++) {

                key[i][j] = parseInt(tt[i \* 8 + j]);

            }

        }

    }

    else

        alert("请输入16bit密钥")

}

//输入密文

var dPut3 = document.getElementById("put3");

var dBtn3 = document.getElementById("btn3");

dBtn3.onclick = function array() {

    let tt = dPut3.value;

    if (tt.length == 16 & (key[0].length + key[1].length) == 16) {

        for (let i = 0; i < 2; i++) {

            for (let j = 0; j < 8; j++) {

                stext[i][j] = parseInt(tt[i \* 8 + j]);

            }

        }

        text = SAES\_decrypt(stext, key);

        let s = "明文为： ";

        for (let i of text)

            for (let j of i)

                s += j;

        dInt.value = s;

        text = new Array(2);

        for (let i = 0; i < 2; i++) {

            text[i] = new Array(8);

        }

        stext = new Array(2);

        for (let i = 0; i < 2; i++) {

            stext[i] = new Array(8);

        }

    }

    else

        alert("请输入16bit密钥和16bit密文")

    console.log(tt.length);

    console.log(key[0].length + key[1].length);

}

3.2多重加密

3.2.1双重加密

部分js代码：

var s = [

    [9, 4, 10, 11],

    [13, 1, 8, 5],

    [6, 2, 0, 3],

    [12, 14, 15, 7]];

var antis = [

    [10, 5, 9, 11],

    [1, 7, 8, 15],

    [6, 0, 2, 3],

    [12, 4, 13, 14]];

var tihuanwei = [

    [0, 0, 0, 0],

    [0, 0, 0, 1],

    [0, 0, 1, 0],

    [0, 0, 1, 1],

    [0, 1, 0, 0],

    [0, 1, 0, 1],

    [0, 1, 1, 0],

    [0, 1, 1, 1],

    [1, 0, 0, 0],

    [1, 0, 0, 1],

    [1, 0, 1, 0],

    [1, 0, 1, 1],

    [1, 1, 0, 0],

    [1, 1, 0, 1],

    [1, 1, 1, 0],

    [1, 1, 1, 1]];

var rcon1 = [1, 0, 0, 0, 0, 0, 0, 0];

var rcon2 = [0, 0, 1, 1, 0, 0, 0, 0];

//function SAES(mingwen, key) {

function x\_de\_n\_fang\_cheng\_fx(xfx, a) {

    if (a[0] === 0) {

        for (let i = 0; i < 3; i++) {

            xfx[i] = a[i + 1];

        }

    } else {

        xfx[1] = a[2];

        xfx[2] = a[3] === 1 ? 0 : 1;

        xfx[3] = 1;

    }

}

function chengfa(a, b) {

    let result = new Array(4).fill(0);

    let xfx = new Array(4).fill(0);

    x\_de\_n\_fang\_cheng\_fx(xfx, a);

    let x2fx = new Array(4).fill(0);

    x\_de\_n\_fang\_cheng\_fx(x2fx, xfx);

    let x3fx = new Array(4).fill(0);

    x\_de\_n\_fang\_cheng\_fx(x3fx, x2fx);

    if (b[0] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= x3fx[i];

        }

    }

    if (b[1] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= x2fx[i];

        }

    }

    if (b[2] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= xfx[i];

        }

    }

    if (b[3] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= a[i];

        }

    }

    return result;

}

function yihuo8(a, b) {

    let t = new Array(8).fill(0);

    for (let i = 0; i < 8; i++)

        t[i] = a[i] ^ b[i];

    return t;

}

function yihuo4(a, b) {

    let t = new Array(4).fill(0);

    for (let i = 0; i < 4; i++)

        t[i] = a[i] ^ b[i];

    return t;

}

function s\_he\_tihuan(temp) {

    let t1 = 2 \* temp[0] + temp[1];

    let t2 = 2 \* temp[2] + temp[3];

    let t3 = 2 \* temp[4] + temp[5];

    let t4 = 2 \* temp[6] + temp[7];

    let tihuan1 = s[t1][t2];

    let tihuan2 = s[t3][t4];

    for (let i = 0; i < 4; i++)

        temp[i] = tihuanwei[tihuan1][i];

    for (let i = 0; i < 4; i++)

        temp[i + 4] = tihuanwei[tihuan2][i];

}

function antis\_he\_tihuan(temp) {

    let t1 = 2 \* temp[0] + temp[1];

    let t2 = 2 \* temp[2] + temp[3];

    let t3 = 2 \* temp[4] + temp[5];

    let t4 = 2 \* temp[6] + temp[7];

    let tihuan1 = antis[t1][t2];

    let tihuan2 = antis[t3][t4];

    for (let i = 0; i < 4; i++)

        temp[i] = tihuanwei[tihuan1][i];

    for (let i = 0; i < 4; i++)

        temp[i + 4] = tihuanwei[tihuan2][i];

}

function zuoyi(temp) {

    for (let i = 4; i < 8; i++) {

        let t = temp[0][i];

        temp[0][i] = temp[1][i];

        temp[1][i] = t;

    }

}

function youyi(temp) {

    for (let i = 4; i < 8; i++) {

        let t = temp[1][i];

        temp[1][i] = temp[0][i];

        temp[0][i] = t;

    }

}

function g(temp, rcon) {

    let t = new Array(8).fill(0);

    for (let i = 0; i < 8; i++)

        t[i] = temp[i];

    for (let i = 0; i < 4; i++) {

        let tt = t[i + 4];

        t[i + 4] = t[i];

        t[i] = tt;

    }

    s\_he\_tihuan(t);

    return yihuo8(t, rcon);

}

function liehunxiao(mingwen) {

    let si\_de2jinzhi = [0, 1, 0, 0];

    let m00 = new Array(4).fill(0);

    let m10 = new Array(4).fill(0);

    let m01 = new Array(4).fill(0);

    let m11 = new Array(4).fill(0);

    for (let i = 0; i < 4; i++) {

        m00[i] = mingwen[0][i];

        m10[i] = mingwen[0][i + 4];

        m01[i] = mingwen[1][i];

        m11[i] = mingwen[1][i + 4];

    }

    let n00 = yihuo4(m00, chengfa(si\_de2jinzhi, m10));

    let n10 = yihuo4(chengfa(si\_de2jinzhi, m00), m10);

    let n01 = yihuo4(m01, chengfa(si\_de2jinzhi, m11));

    let n11 = yihuo4(chengfa(si\_de2jinzhi, m01), m11);

    for (let i = 0; i < 4; i++) {

        mingwen[0][i] = n00[i];

        mingwen[0][i + 4] = n10[i];

        mingwen[1][i] = n01[i];

        mingwen[1][i + 4] = n11[i];

    }

}

function antiliehunxiao(mingwen) {

    let s1\_de2jinzhi = [1, 0, 0, 1];//9

    let s2\_de2jinzhi = [0, 0, 1, 0];//2

    let m00 = new Array(4).fill(0);

    let m10 = new Array(4).fill(0);

    let m01 = new Array(4).fill(0);

    let m11 = new Array(4).fill(0);

    for (let i = 0; i < 4; i++) {

        m00[i] = mingwen[0][i];

        m10[i] = mingwen[0][i + 4];

        m01[i] = mingwen[1][i];

        m11[i] = mingwen[1][i + 4];

    }

    let n00 = yihuo4(chengfa(s1\_de2jinzhi, m00), chengfa(s2\_de2jinzhi, m10));

    let n01 = yihuo4(chengfa(s1\_de2jinzhi, m01), chengfa(s2\_de2jinzhi, m11));

    let n10 = yihuo4(chengfa(s2\_de2jinzhi, m00), chengfa(s1\_de2jinzhi, m10));

    let n11 = yihuo4(chengfa(s2\_de2jinzhi, m01), chengfa(s1\_de2jinzhi, m11));

    for (let i = 0; i < 4; i++) {

        mingwen[0][i] = n00[i];

        mingwen[0][i + 4] = n10[i];

        mingwen[1][i] = n01[i];

        mingwen[1][i + 4] = n11[i];

    }

}

function lunmiyaojia(mingwen, key) {

    for (let i = 0; i < 2; i++)

        for (let j = 0; j < 8; j++)

            mingwen[i][j] ^= key[i][j];

}

function SAES(mingwen, key) {

    let key1 = new Array(2).fill(new Array(8).fill(0));

    let key2 = new Array(2).fill(new Array(8).fill(0));

    key1[0] = yihuo8(key[0], g(key[1], rcon1));

    key1[1] = yihuo8(key1[0], key[1]);

    key2[0] = yihuo8(key1[0], g(key1[1], rcon2));

    key2[1] = yihuo8(key2[0], key1[1]);

    lunmiyaojia(mingwen, key);

    s\_he\_tihuan(mingwen[0]);

    s\_he\_tihuan(mingwen[1]);

    zuoyi(mingwen);

    liehunxiao(mingwen);

    lunmiyaojia(mingwen, key1);

    s\_he\_tihuan(mingwen[0]);

    s\_he\_tihuan(mingwen[1]);

    zuoyi(mingwen);

    lunmiyaojia(mingwen, key2);

    return mingwen;

}

function SAES\_decrypt(mingwen, key) {

    var key1 = new Array(2);

    for (let i = 0; i < 2; i++) {

        key1[i] = new Array(8);

    }

    var key2 = new Array(2);

    for (let i = 0; i < 2; i++) {

        key2[i] = new Array(8);

    }

    // 解密过程

    key1[0] = yihuo8(key[0], g(key[1], rcon1));

    key1[1] = yihuo8(key1[0], key[1]);

    key2[0] = yihuo8(key1[0], g(key1[1], rcon2));

    key2[1] = yihuo8(key2[0], key1[1]);

    lunmiyaojia(mingwen, key2);

    youyi(mingwen);

    antis\_he\_tihuan(mingwen[0]);

    antis\_he\_tihuan(mingwen[1]);

    lunmiyaojia(mingwen, key1);

    antiliehunxiao(mingwen);

    youyi(mingwen);

    antis\_he\_tihuan(mingwen[0]);

    antis\_he\_tihuan(mingwen[1]);

    lunmiyaojia(mingwen, key);

    return mingwen;

}

var text = new Array(2);

for (let i = 0; i < 2; i++) {

    text[i] = new Array(8);

}

var key = new Array(2);

for (let i = 0; i < 2; i++) {

    key[i] = new Array(8);

}

var mykey2 = new Array(2);

for (let i = 0; i < 2; i++) {

    mykey2[i] = new Array(8);

}

var stext = new Array(2);

for (let i = 0; i < 2; i++) {

    stext[i] = new Array(8);

}

//先定义一个空数组装准备输入的数据

//连接、定义输入框，提交按钮和显示框

var dPut = document.getElementById("put");

var dBtn = document.getElementById("btn");

var dInt = document.getElementById("int");

dBtn.onclick = function array() {

    let tt = dPut.value;

    let keyhasValue = key.some(row => row.some(value => value !== undefined));

    console.log(keyhasValue);

    let key2hasValue = mykey2.some(row => row.some(value => value !== undefined));

    console.log(key2hasValue);

    if (keyhasValue & key2hasValue) {

        if (tt.length == 16 & (key[0].length + key[1].length) == 16) {

            for (let i = 0; i < 2; i++) {

                for (let j = 0; j < 8; j++) {

                    text[i][j] = parseInt(tt[i \* 8 + j]);

                }

            }

            text = SAES(text, key);

            stext = SAES(text, mykey2);

            let s = "密文为： ";

            for (let i of stext)

                for (let j of i)

                    s += j;

            dInt.value = s;

            text = new Array(2);

            for (let i = 0; i < 2; i++) {

                text[i] = new Array(8);

            }

            stext = new Array(2);

            for (let i = 0; i < 2; i++) {

                stext[i] = new Array(8);

            }

            flag = 0;

        }

        else

            alert("明文和每次密钥都是16bits");

    }

    else

        alert("请先输入两次密钥");

}

//输入密钥

var flag = 0;

var dPut2 = document.getElementById("put2");

var dBtn2 = document.getElementById("btn2");

dBtn2.onclick = function array() {

    let keyhasValue = key.some(row => row.some(value => value !== undefined));

    console.log(keyhasValue);

    if (!flag) {

        let tt16 = dPut2.value;

        let tt = parseInt(tt16, 16).toString(2).padStart(16, '0');

        console.log(tt);

        if (tt.length == 16) {

            for (let i = 0; i < 2; i++) {

                for (let j = 0; j < 8; j++) {

                    key[i][j] = parseInt(tt[i \* 8 + j]);

                }

            }

            flag++;

            dPut2.value = "";

            dInt.value = "请输入第二次的密钥";

        }

        else

            alert("请输入16bit密钥")

    }

    else {

        for (let i = 0; i < 2; i++) {

            mykey2[i] = new Array(8);

        }

        let tt16 = dPut2.value;

        let tt = parseInt(tt16, 16).toString(2).padStart(16, '0');

        console.log(tt);

        if (tt.length == 16) {

            for (let i = 0; i < 2; i++) {

                for (let j = 0; j < 8; j++) {

                    mykey2[i][j] = parseInt(tt[i \* 8 + j]);

                }

            }

            dInt.value = "两次密钥输入完成";

        }

        else

            alert("请输入16bit密钥")

    }

}

//输入密文

var dPut3 = document.getElementById("put3");

var dBtn3 = document.getElementById("btn3");

dBtn3.onclick = function array() {

    let tt = dPut3.value;

    let keyhasValue = key.some(row => row.some(value => value !== undefined));

    console.log(keyhasValue);

    let key2hasValue = mykey2.some(row => row.some(value => value !== undefined));

    console.log(key2hasValue);

    if (keyhasValue & key2hasValue) {

        if (tt.length == 16 & (key[0].length + key[1].length) == 16) {

            for (let i = 0; i < 2; i++) {

                for (let j = 0; j < 8; j++) {

                    stext[i][j] = parseInt(tt[i \* 8 + j]);

                }

            }

            stext = SAES\_decrypt(stext, mykey2);

            text = SAES\_decrypt(stext, key);

            let s = "密文为： ";

            for (let i of text)

                for (let j of i)

                    s += j;

            dInt.value = s;

            text = new Array(2);

            for (let i = 0; i < 2; i++) {

                text[i] = new Array(8);

            }

            stext = new Array(2);

            for (let i = 0; i < 2; i++) {

                stext[i] = new Array(8);

            }

            flag = 0;

        }

        else

            alert("明文和每次密钥都是16bits");

    }

    else

        alert("请先输入两次密钥");

}

3.2.2三重加密

部分js代码：

var s = [

    [9, 4, 10, 11],

    [13, 1, 8, 5],

    [6, 2, 0, 3],

    [12, 14, 15, 7]];

var antis = [

    [10, 5, 9, 11],

    [1, 7, 8, 15],

    [6, 0, 2, 3],

    [12, 4, 13, 14]];

var tihuanwei = [

    [0, 0, 0, 0],

    [0, 0, 0, 1],

    [0, 0, 1, 0],

    [0, 0, 1, 1],

    [0, 1, 0, 0],

    [0, 1, 0, 1],

    [0, 1, 1, 0],

    [0, 1, 1, 1],

    [1, 0, 0, 0],

    [1, 0, 0, 1],

    [1, 0, 1, 0],

    [1, 0, 1, 1],

    [1, 1, 0, 0],

    [1, 1, 0, 1],

    [1, 1, 1, 0],

    [1, 1, 1, 1]];

var rcon1 = [1, 0, 0, 0, 0, 0, 0, 0];

var rcon2 = [0, 0, 1, 1, 0, 0, 0, 0];

//function SAES(mingwen, key) {

function x\_de\_n\_fang\_cheng\_fx(xfx, a) {

    if (a[0] === 0) {

        for (let i = 0; i < 3; i++) {

            xfx[i] = a[i + 1];

        }

    } else {

        xfx[1] = a[2];

        xfx[2] = a[3] === 1 ? 0 : 1;

        xfx[3] = 1;

    }

}

function chengfa(a, b) {

    let result = new Array(4).fill(0);

    let xfx = new Array(4).fill(0);

    x\_de\_n\_fang\_cheng\_fx(xfx, a);

    let x2fx = new Array(4).fill(0);

    x\_de\_n\_fang\_cheng\_fx(x2fx, xfx);

    let x3fx = new Array(4).fill(0);

    x\_de\_n\_fang\_cheng\_fx(x3fx, x2fx);

    if (b[0] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= x3fx[i];

        }

    }

    if (b[1] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= x2fx[i];

        }

    }

    if (b[2] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= xfx[i];

        }

    }

    if (b[3] === 1) {

        for (let i = 0; i < 4; i++) {

            result[i] ^= a[i];

        }

    }

    return result;

}

function yihuo8(a, b) {

    let t = new Array(8).fill(0);

    for (let i = 0; i < 8; i++)

        t[i] = a[i] ^ b[i];

    return t;

}

function yihuo4(a, b) {

    let t = new Array(4).fill(0);

    for (let i = 0; i < 4; i++)

        t[i] = a[i] ^ b[i];

    return t;

}

function s\_he\_tihuan(temp) {

    let t1 = 2 \* temp[0] + temp[1];

    let t2 = 2 \* temp[2] + temp[3];

    let t3 = 2 \* temp[4] + temp[5];

    let t4 = 2 \* temp[6] + temp[7];

    let tihuan1 = s[t1][t2];

    let tihuan2 = s[t3][t4];

    for (let i = 0; i < 4; i++)

        temp[i] = tihuanwei[tihuan1][i];

    for (let i = 0; i < 4; i++)

        temp[i + 4] = tihuanwei[tihuan2][i];

}

function antis\_he\_tihuan(temp) {

    let t1 = 2 \* temp[0] + temp[1];

    let t2 = 2 \* temp[2] + temp[3];

    let t3 = 2 \* temp[4] + temp[5];

    let t4 = 2 \* temp[6] + temp[7];

    let tihuan1 = antis[t1][t2];

    let tihuan2 = antis[t3][t4];

    for (let i = 0; i < 4; i++)

        temp[i] = tihuanwei[tihuan1][i];

    for (let i = 0; i < 4; i++)

        temp[i + 4] = tihuanwei[tihuan2][i];

}

function zuoyi(temp) {

    for (let i = 4; i < 8; i++) {

        let t = temp[0][i];

        temp[0][i] = temp[1][i];

        temp[1][i] = t;

    }

}

function youyi(temp) {

    for (let i = 4; i < 8; i++) {

        let t = temp[1][i];

        temp[1][i] = temp[0][i];

        temp[0][i] = t;

    }

}

function g(temp, rcon) {

    let t = new Array(8).fill(0);

    for (let i = 0; i < 8; i++)

        t[i] = temp[i];

    for (let i = 0; i < 4; i++) {

        let tt = t[i + 4];

        t[i + 4] = t[i];

        t[i] = tt;

    }

    s\_he\_tihuan(t);

    return yihuo8(t, rcon);

}

function liehunxiao(mingwen) {

    let si\_de2jinzhi = [0, 1, 0, 0];

    let m00 = new Array(4).fill(0);

    let m10 = new Array(4).fill(0);

    let m01 = new Array(4).fill(0);

    let m11 = new Array(4).fill(0);

    for (let i = 0; i < 4; i++) {

        m00[i] = mingwen[0][i];

        m10[i] = mingwen[0][i + 4];

        m01[i] = mingwen[1][i];

        m11[i] = mingwen[1][i + 4];

    }

    let n00 = yihuo4(m00, chengfa(si\_de2jinzhi, m10));

    let n10 = yihuo4(chengfa(si\_de2jinzhi, m00), m10);

    let n01 = yihuo4(m01, chengfa(si\_de2jinzhi, m11));

    let n11 = yihuo4(chengfa(si\_de2jinzhi, m01), m11);

    for (let i = 0; i < 4; i++) {

        mingwen[0][i] = n00[i];

        mingwen[0][i + 4] = n10[i];

        mingwen[1][i] = n01[i];

        mingwen[1][i + 4] = n11[i];

    }

}

function antiliehunxiao(mingwen) {

    let s1\_de2jinzhi = [1, 0, 0, 1];//9

    let s2\_de2jinzhi = [0, 0, 1, 0];//2

    let m00 = new Array(4).fill(0);

    let m10 = new Array(4).fill(0);

    let m01 = new Array(4).fill(0);

    let m11 = new Array(4).fill(0);

    for (let i = 0; i < 4; i++) {

        m00[i] = mingwen[0][i];

        m10[i] = mingwen[0][i + 4];

        m01[i] = mingwen[1][i];

        m11[i] = mingwen[1][i + 4];

    }

    let n00 = yihuo4(chengfa(s1\_de2jinzhi, m00), chengfa(s2\_de2jinzhi, m10));

    let n01 = yihuo4(chengfa(s1\_de2jinzhi, m01), chengfa(s2\_de2jinzhi, m11));

    let n10 = yihuo4(chengfa(s2\_de2jinzhi, m00), chengfa(s1\_de2jinzhi, m10));

    let n11 = yihuo4(chengfa(s2\_de2jinzhi, m01), chengfa(s1\_de2jinzhi, m11));

    for (let i = 0; i < 4; i++) {

        mingwen[0][i] = n00[i];

        mingwen[0][i + 4] = n10[i];

        mingwen[1][i] = n01[i];

        mingwen[1][i + 4] = n11[i];

    }

}

function lunmiyaojia(mingwen, key) {

    for (let i = 0; i < 2; i++)

        for (let j = 0; j < 8; j++)

            mingwen[i][j] ^= key[i][j];

}

function SAES(mingwen, key) {

    let key1 = new Array(2).fill(new Array(8).fill(0));

    let key2 = new Array(2).fill(new Array(8).fill(0));

    key1[0] = yihuo8(key[0], g(key[1], rcon1));

    key1[1] = yihuo8(key1[0], key[1]);

    key2[0] = yihuo8(key1[0], g(key1[1], rcon2));

    key2[1] = yihuo8(key2[0], key1[1]);

    lunmiyaojia(mingwen, key);

    s\_he\_tihuan(mingwen[0]);

    s\_he\_tihuan(mingwen[1]);

    zuoyi(mingwen);

    liehunxiao(mingwen);

    lunmiyaojia(mingwen, key1);

    s\_he\_tihuan(mingwen[0]);

    s\_he\_tihuan(mingwen[1]);

    zuoyi(mingwen);

    lunmiyaojia(mingwen, key2);

    return mingwen;

}

function SAES\_decrypt(mingwen, key) {

    var key1 = new Array(2);

    for (let i = 0; i < 2; i++) {

        key1[i] = new Array(8);

    }

    var key2 = new Array(2);

    for (let i = 0; i < 2; i++) {

        key2[i] = new Array(8);

    }

    // 解密过程

    key1[0] = yihuo8(key[0], g(key[1], rcon1));

    key1[1] = yihuo8(key1[0], key[1]);

    key2[0] = yihuo8(key1[0], g(key1[1], rcon2));

    key2[1] = yihuo8(key2[0], key1[1]);

    lunmiyaojia(mingwen, key2);

    youyi(mingwen);

    antis\_he\_tihuan(mingwen[0]);

    antis\_he\_tihuan(mingwen[1]);

    lunmiyaojia(mingwen, key1);

    antiliehunxiao(mingwen);

    youyi(mingwen);

    antis\_he\_tihuan(mingwen[0]);

    antis\_he\_tihuan(mingwen[1]);

    lunmiyaojia(mingwen, key);

    return mingwen;

}

var text = new Array(2);

for (let i = 0; i < 2; i++) {

    text[i] = new Array(8);

}

var key = new Array(2);

for (let i = 0; i < 2; i++) {

    key[i] = new Array(8);

}

var mykey2 = new Array(2);

for (let i = 0; i < 2; i++) {

    mykey2[i] = new Array(8);

}

var flag = 0;

var stext = new Array(2);

for (let i = 0; i < 2; i++) {

    stext[i] = new Array(8);

}

//先定义一个空数组装准备输入的数据

//连接、定义输入框，提交按钮和显示框

var dPut = document.getElementById("put");

var dBtn = document.getElementById("btn");

var dInt = document.getElementById("int");

dBtn.onclick = function array() {

    let tt = dPut.value;

    let keyhasValue = key.some(row => row.some(value => value !== undefined));

    console.log(keyhasValue);

    let key2hasValue = mykey2.some(row => row.some(value => value !== undefined));

    console.log(key2hasValue);

    if (keyhasValue & key2hasValue) {

        if (tt.length == 16 & (key[0].length + key[1].length) == 16) {

            for (let i = 0; i < 2; i++) {

                for (let j = 0; j < 8; j++) {

                    text[i][j] = parseInt(tt[i \* 8 + j]);

                }

            }

            text = SAES(text, key);

            text = SAES\_decrypt(text, mykey2);

            stext = SAES(text, key);

            let s = "密文为： ";

            for (let i of stext)

                for (let j of i)

                    s += j;

            dInt.value = s;

            text = new Array(2);

            for (let i = 0; i < 2; i++) {

                text[i] = new Array(8);

            }

            stext = new Array(2);

            for (let i = 0; i < 2; i++) {

                stext[i] = new Array(8);

            }

            flag = 0;

        }

        else

            alert("明文和每次密钥都是16bits");

    }

    else

        alert("请先输入两次密钥");

}

//输入密钥

var dPut2 = document.getElementById("put2");

var dBtn2 = document.getElementById("btn2");

dBtn2.onclick = function array() {

    let keyhasValue = key.some(row => row.some(value => value !== undefined));

    console.log(keyhasValue);

    if (!flag) {

        let tt16 = dPut2.value;

        let tt = parseInt(tt16, 16).toString(2).padStart(16, '0');

        console.log(tt);

        if (tt.length == 16) {

            for (let i = 0; i < 2; i++) {

                for (let j = 0; j < 8; j++) {

                    key[i][j] = parseInt(tt[i \* 8 + j]);

                }

            }

            flag++;

            dPut2.value = "";

            dInt.value = "请输入第二次的密钥";

        }

        else

            alert("请输入16bit密钥")

    }

    else {

        for (let i = 0; i < 2; i++) {

            mykey2[i] = new Array(8);

        }

        let tt16 = dPut2.value;

        let tt = parseInt(tt16, 16).toString(2).padStart(16, '0');

        console.log(tt);

        if (tt.length == 16) {

            for (let i = 0; i < 2; i++) {

                for (let j = 0; j < 8; j++) {

                    mykey2[i][j] = parseInt(tt[i \* 8 + j]);

                }

            }

        }

        else

            alert("请输入16bit密钥")

    }

}

//输入密文

var dPut3 = document.getElementById("put3");

var dBtn3 = document.getElementById("btn3");

dBtn3.onclick = function array() {

    let tt = dPut3.value;

    let keyhasValue = key.some(row => row.some(value => value !== undefined));

    console.log(keyhasValue);

    let key2hasValue = mykey2.some(row => row.some(value => value !== undefined));

    console.log(key2hasValue);

    if (keyhasValue & key2hasValue) {

        if (tt.length == 16 & (key[0].length + key[1].length) == 16) {

            for (let i = 0; i < 2; i++) {

                for (let j = 0; j < 8; j++) {

                    stext[i][j] = parseInt(tt[i \* 8 + j]);

                }

            }

            stext = SAES\_decrypt(stext, key);

            stext = SAES(stext, mykey2);

            text = SAES\_decrypt(text, key);

            let s = "明文为： ";

            for (let i of stext)

                for (let j of i)

                    s += j;

            dInt.value = s;

            text = new Array(2);

            for (let i = 0; i < 2; i++) {

                text[i] = new Array(8);

            }

            stext = new Array(2);

            for (let i = 0; i < 2; i++) {

                stext[i] = new Array(8);

            }

            flag = 0;

        }

        else

            alert("明文和每次密钥都是16bits");

    }

    else

        alert("请先输入两次密钥");

}

1. **测试结果**

测试结果见测试结果文档。