密码学第三次实验报告

学号：2111033 姓名：艾明旭 专业：信息安全

⼀、实验内容说明

1、实验⽬的

通过⽤AES算法对实际的数据进⾏加密和解密来深刻了解AES的运⾏原理。

2、实验要求

. 实现AES的加密和解密，提交程序代码和执⾏结果。

\_x0019\_. 在检验雪崩效应中，要求⾄少改变明⽂和密⽂中各⼋位，给出统计结果并计算出平均值。

3、实验步骤

. 算法分析： 对课本中AES算法进⾏深⼊分析，对其中⽤到的基本数学算法、字节代换、⾏移位变换、

列混合变换原理进⾏详细的分析，并考虑如何进⾏编程实现。对轮函数、密钥⽣成等环节要有清晰的

了解，并考虑其每⼀个环节的实现过程。

\_x0019\_. AES实现程序的总体设计： 在第⼀步的基础上，对整个AES加密函数的实现进⾏总体设计，考虑数据

的存储格式，参数的传递格式，程序实现的总体层次等，画出程序实现的流程图。

. 在总体设计完成后，开始具体的编码，在编码过程中，注意要尽量使⽤⾼效的编码⽅式。

. 利⽤3中实现的程序，对AES的密⽂进⾏雪崩效应检验。即固定密钥，仅改变明⽂中的⼀位，统计密⽂

改变的位数；固定明⽂，仅改变密钥中的⼀位，统计密⽂改变的位数。

⼆、实验环境

操作系统：Windows 11

软件系统：Visual studio

编译⼯具：Visual studio 2022

编程语⾔：C++

三、实验过程

本次实验⾸先翻阅课本，对理论课上的知识进⾏回顾，然后设计整个实验的流程图以及各个结构体和函数的

⼤致思路，然后进⾏具体代码的编写实现，以下为具体过程：

1、流程分析

*密钥扩展*

AES 算法通过密钥扩展程序（

Key Expansion）将⽤户输⼊的密钥 K 扩展⽣成 Nb(Nr+1)个字，存放在⼀个线

性数组w[Nb\*(Nr+1)]中。具体如下：

. 位置变换函数loop\_wordbyte()，接受⼀个字 [a0, a1, a2, a3] 作为输⼊，循环左移⼀个字节后输出

[a1, a2, a3, a0]。

\_x0019\_. S盒变换函数wordbyte\_sub()，接受⼀个字 [a0, a1, a2, a3] 作为输⼊。S盒是⼀个16x16的表，其中

每⼀个元素是⼀个字节。对于输⼊的每⼀个字节，前四位组成⼗六进制数 x 作为⾏号，后四位组成的

⼗六进制数 y 作为列号，查找表中对应的值。最后函数输出 4 个新字节组成的 32-bit 字。（

S盒和逆S 盒在程序中已经提前声明了⼀个结构体）

. 轮常数Rcon[]，如何计算的就不说了，直接把它当做常量数组。

. 扩展密钥数组w[]的前 Nk 个元素就是外部密钥 K，以后的元素w[i]等于它前⼀个元素w[i-1]与前第 Nk

个元素w[i-Nk]的异或，即w[i] = w[i-1] XOR w[i-Nk]；但若 i 为 Nk 的倍数，则w[i] = w[i-Nk] XOR wordbyte\_sub(loop\_wordbyte(w[i-1])) XOR Rcon[i/Nk-1]。

在本次的实验中主要采⽤的是字符型的变量来进⾏参数的传递和转移，但是在计算的过程中会将字符型的数

组转变为数字，但由于128位的数字太⼤，所以将其分为4组，每⼀个都由四个8进制数来构成，如下所示：

vector<string> group\_key(string& key)

{

// 四组

vector<string> groups(4);

// 初始下标

int index = 0;

// 分组

for (string& g : groups)

{

g = key.substr(index, 8);

index += 8;

}

return groups;

}