**实验二 AES算法实验**

信息安全1501 沈鑫楠 3150604028

一、实验目的

1.掌握AES算法的基本原理

2.了解AES运算的实现方法

二、实验环境

1.操作系统为Windows XP

2.信息安全综合实验系统

三、实验内容

1.AES算法的原理与过程

2.数据加解密运算

3.AES算法的编程实现

四、实验步骤

（一）AES加密原理

1.打开实验系统，点击“对称密码算法”——“AES”——”AES算法流程“

2.输入密钥，点击字节矩阵，字节矩阵显示

3.依次点击“RotWord”(循环左移)、”SubWord”(字节替换)、”轮常量异或“、”与W0异或“,生成W4

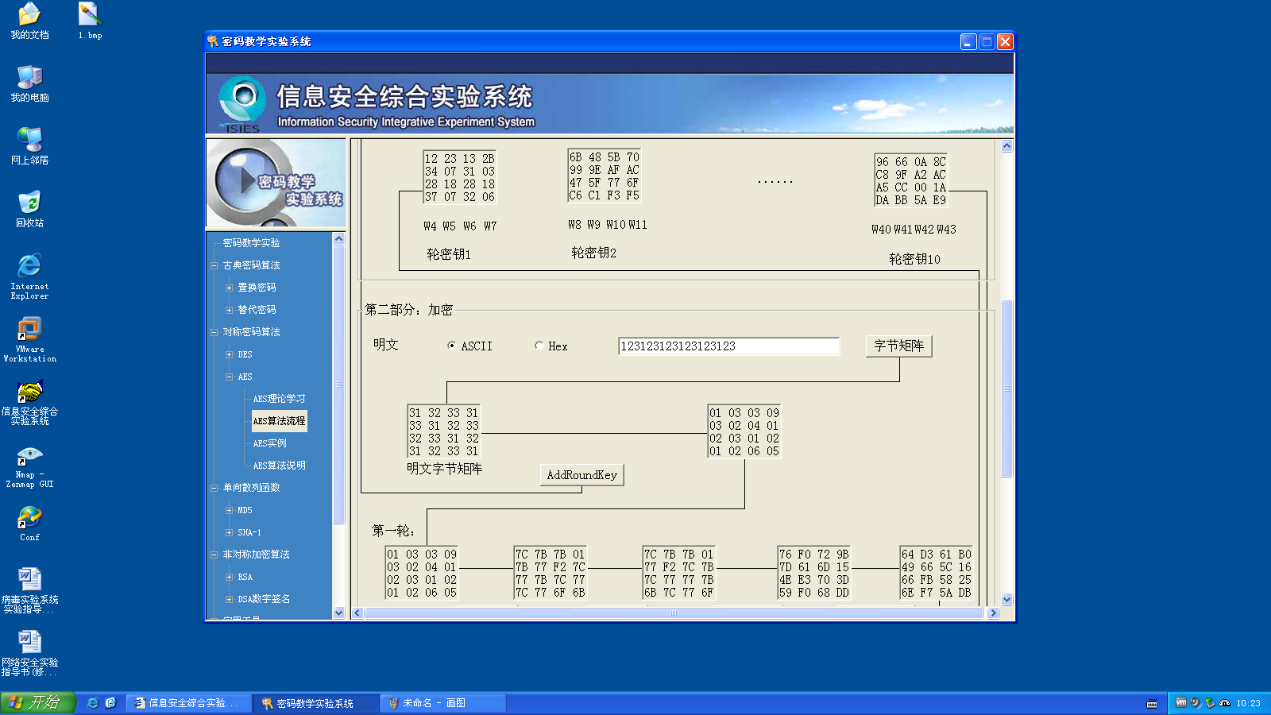
4.W1与W4异或生成W5，以此方法生成W6和W7

5.依次生成所有轮密钥

6.生成论密钥1~10矩阵

7.输入明文，点击“字节矩阵“，生成明文字节矩阵

8.点击“AddRoundKey”进行初始轮密钥加运算

9.依次点击“SubBytes”(字节替换)、”ShiftRows”(行移位)、”MixColumns”(列混淆)、“AddRoundKey”(轮密钥加)，进行一轮加密运算

10.共进行10轮运算，其中最后一轮不进行列混淆的运算

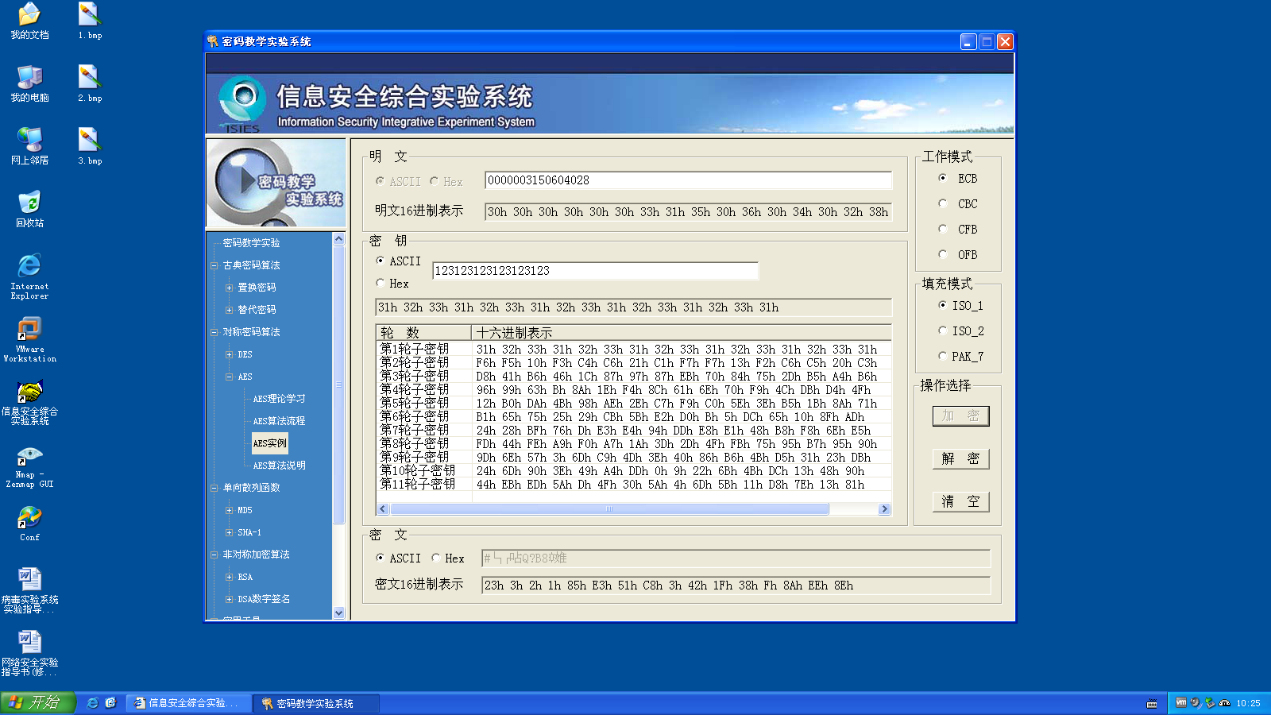
11.最后生成密文字节矩阵

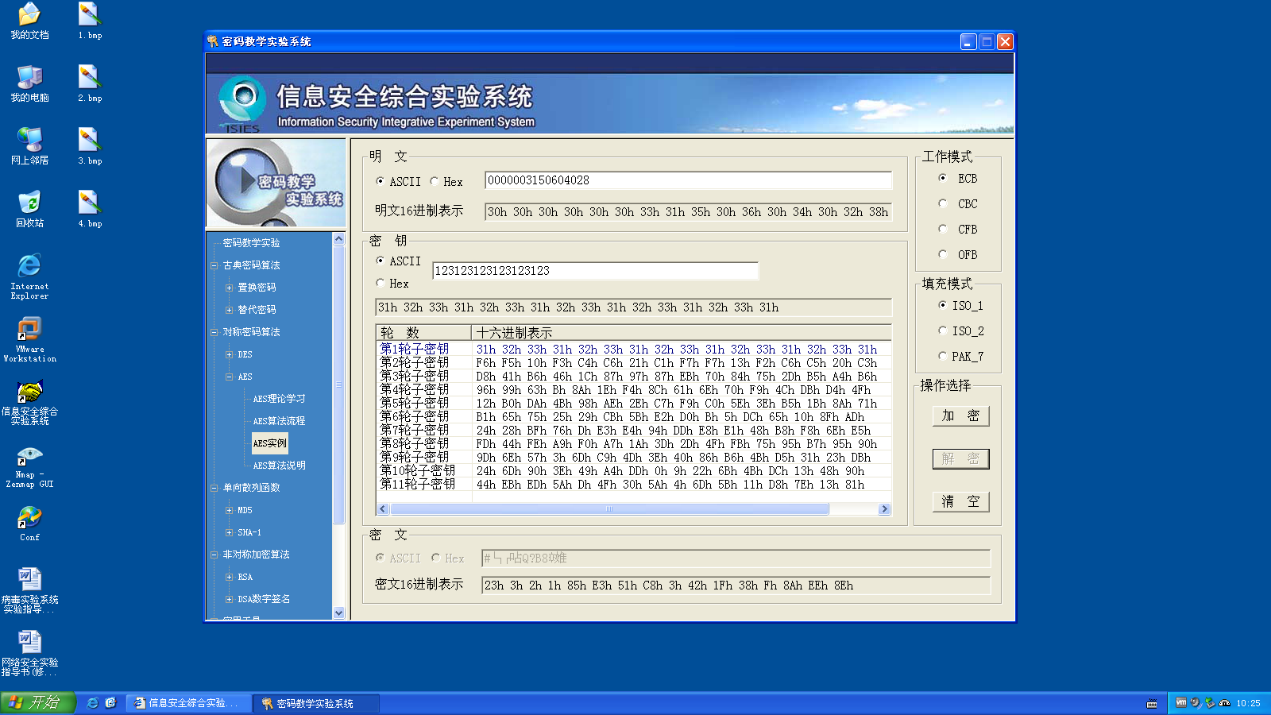


（二）AES加解密运算

1.打开实验系统，选择“对称加密算法“——”AES“——”AES实例“

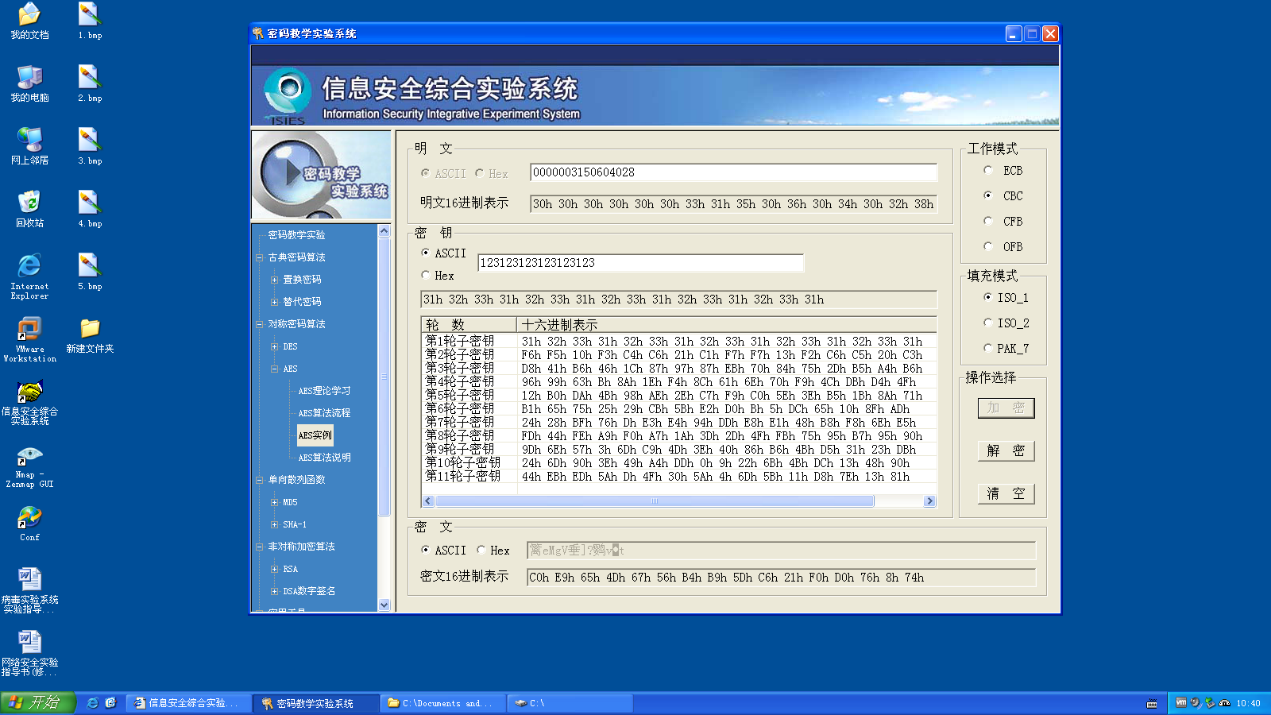
2.输入明文和密钥，选择ECB模式，点击加密

3.可以看到10轮加密中每一轮的子密钥和加密最终结果

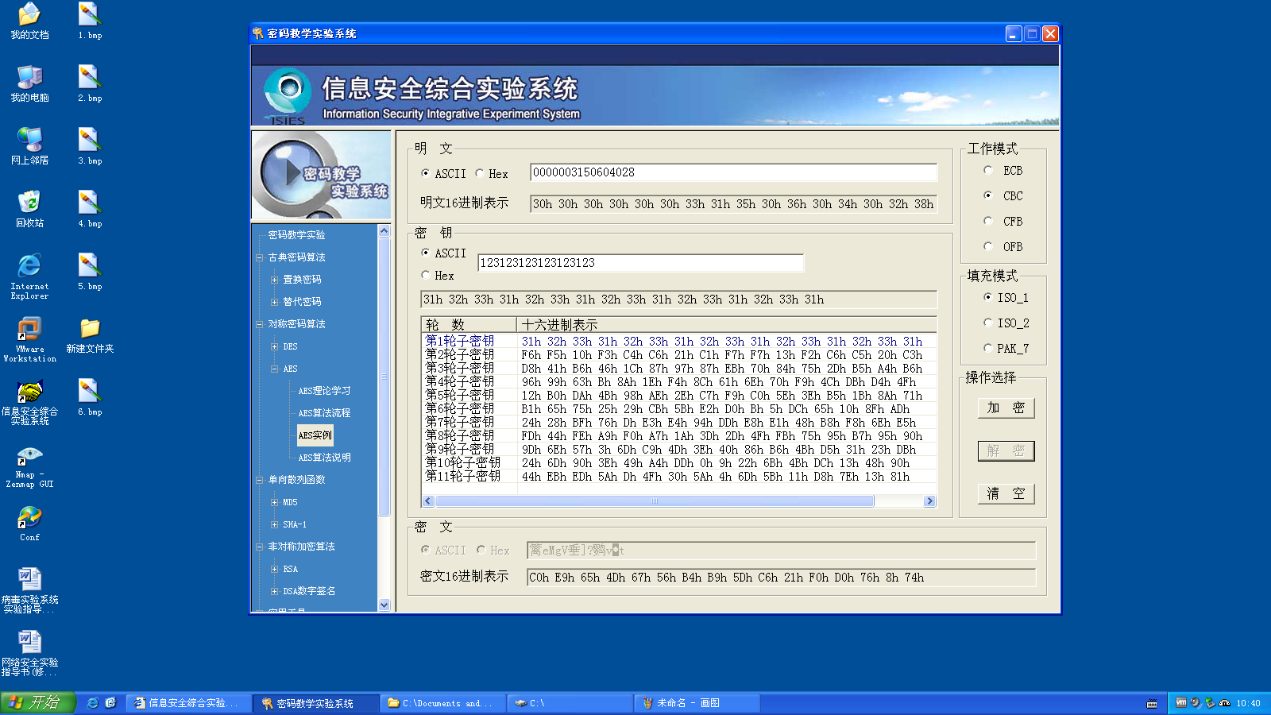
4.点击解密，可以看到每一轮的字密钥和解密出的明文

5.选择CBC模式，输入明文和密钥，点击加密

6.可以看到每一轮的子密钥和最后的加密结果



7.点击解密，同样可以看到每一轮的子密钥和解密恢复出的明文



（三）AES算法编程实现

1.主要源代码

#include "RIJNDAEL.h"

#include <stdio.h>

#include <time.h>

#include <stdlib.h>

#define MAXNUM 255

#define RAND\_MAX 0x7fff

void main()

{

int i;

u4byte IV[4]={0x12345678,0x90123456,0x78901234,0x56789012};//初始向量IV

u4byte ori1[4],ori2[4],ri[8],ri1[4],ri2[4];

u4byte out\_block1[4],de\_block1[4];

u4byte out\_block2[4],de\_block2[4];

u4byte out\_block[8],de\_block[8];

u4byte in\_key[4]={0x11111111,0x22222222,0x33333333,0x44444444};//密钥初始化

u4byte plaint\_block1[4]={0x31506040,0x28315060,0x40283150,0x60402831};//明文块1

u4byte plaint\_block2[4]={0x50604028,0x31506040,0x28315060,0x40283150};//明文块2

u4byte x1,x2,x3,x4;

time\_t t; //这两行保证每次产生的随机数不同

srand( (unsigned) time( &t ) );

printf("ECB~~Start~~~~~~~~~~~~~~\n");

//产生随机密钥

for(i=0;i<4;i++){

x1 = rand()\*MAXNUM/RAND\_MAX;

x2 = rand()\*MAXNUM/RAND\_MAX;

x3 = rand()\*MAXNUM/RAND\_MAX;

x4 = rand()\*MAXNUM/RAND\_MAX;

in\_key[i] = 0;

in\_key[i] = x1;

in\_key[i]<<=8;

in\_key[i] += x2;

in\_key[i]<<=8;

in\_key[i] += x3;

in\_key[i]<<=8;

in\_key[i] += x4;}

set\_key(in\_key,128);//设置128位的密钥

encrypt(plaint\_block1,out\_block1);//加密明文块1

encrypt(plaint\_block2,out\_block2);//加密明文块2

//拼接密文块

for (i=0;i<4;i++) out\_block[i]=out\_block1[i];

for (i=4;i<8;i++) out\_block[i]=out\_block2[i-4];

printf("Encryption:\n密文： \n");

for(i=0;i<8;i++) printf("%x",out\_block[i]);

printf("\n");

decrypt(out\_block1,de\_block1);//解密密文块1

decrypt(out\_block2,de\_block2);//解密密文块2

//拼接明文块

for (i=0;i<4;i++) de\_block[i]=de\_block1[i];

for (i=4;i<8;i++) de\_block[i]=de\_block2[i-4];

printf("Decryption!\n恢复原文： \n");

for(i=0;i<8;i++) printf("%x",de\_block[i]);

printf("\n");

printf("CBC~~Start~~~~~~~~~~~~~~\n");

//产生随机密钥

for(i=0;i<4;i++){

x1 = rand()\*MAXNUM/RAND\_MAX;

x2 = rand()\*MAXNUM/RAND\_MAX;

x3 = rand()\*MAXNUM/RAND\_MAX;

x4 = rand()\*MAXNUM/RAND\_MAX;

in\_key[i] = 0;

in\_key[i] = x1;

in\_key[i]<<=8;

in\_key[i] += x2;

in\_key[i]<<=8;

in\_key[i] += x3;

in\_key[i]<<=8;

in\_key[i] += x4;}

set\_key(in\_key,128);//设置128位的密钥

for (i=0;i<4;i++) ori1[i]=plaint\_block1[i]^IV[i];//与初始向量异或

encrypt(ori1,out\_block1);//加密生成密文块1

for (i=0;i<4;i++) ori2[i]=out\_block1[i]^plaint\_block2[i];//与密文块1异或

encrypt(ori2,out\_block2);//加密生成密文块2

//拼接密文块

for (i=0;i<4;i++) ri[i]=out\_block1[i];

for (i=4;i<8;i++) ri[i]=out\_block2[i-4];

printf("Encryption:\n密文： \n");

for(i=0;i<8;i++) printf("%x",ri[i]);

printf("\n");

decrypt(out\_block1,de\_block1);//解密密文块1

decrypt(out\_block2,de\_block2);//解密密文块2

for (i=0;i<4;i++) ri2[i]=out\_block1[i]^de\_block2[i];//与密文块1异或

for (i=0;i<4;i++) ri1[i]=IV[i]^de\_block1[i];//与IV异或

//拼接明文块

for (i=0;i<4;i++) ri[i]=ri1[i];

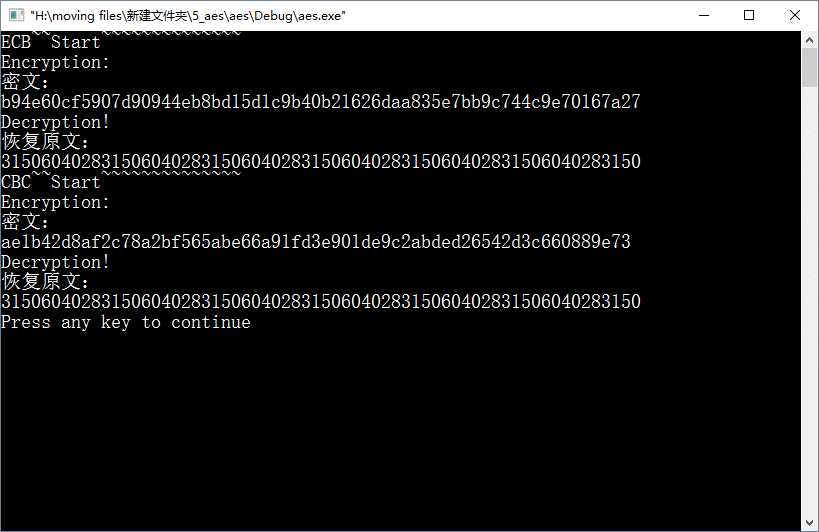
for (i=4;i<8;i++) ri[i]=ri2[i-4];

printf("Decryption!\n恢复原文： \n");

for(i=0;i<8;i++)printf("%x",ri[i]);

printf("\n");

}

2.运行结果截图

六、实验心得

通过这次试验，我对AES算法的原理和实现方法有了一个基本的了解，并能够通过编程的方法实现简单实现AES算法。我熟悉了整个AES的算法，了解了加解密的基本原理，从密钥的扩展到加密的具体步骤。这次试验也让我更加熟练地使用实验环境，掌握了实验系统的使用方法。