实验 **2 AES** 密码体制

一．实验目的  
通过实现 AES 算法，以及对实际的数据进行加密和解密，加深对 AES 密码体制原理的理解。

二．实验环境  
硬件设备： PC 机  
操作系统： windows 2000 操作系统  
编程工具： Matlab， VC++或 Eclipse

三．**AES** 简介  
 信息加密根据采用的密钥类型可以划分为对称密码算法和非对称密码算法。对称密码算法是指加密系统的加密密钥和解密密钥相同，或者虽然不同，但是可以从其中任意一个推导出另一个，更形象的说就是用同一把钥匙开锁和解锁。在对称密码算法的发展历史中曾出现过多种优秀的算法，包括 DES、 3DES、 AES 等。  
 2000年10月，NIST（美国国家标准和技术协会）宣布通过从 15 种候选算法中选出的一项新的高级加密标准（AES）规范 Rijndael。Rijndael 这个名字是从它的两个发明者 Rijmen和 Daemen 的名字得来的。  
 AES 是迭代、对称密钥分组的密码体制，它可以使用 128、192和256位密钥，并且用128 位（16 字节）分组加密和解密数据。基于代换与置换运算。置换是对数据重新进行安排，代换是将一个数据单元替换为另一个。详细的加解密过程请参考官方标准：http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

四．实验步骤  
1.根据附录提供的算法与代码， 实现AES加密算法，使算法能够对128位的数据加密。要求能够处理密钥为128位，数据分组为128位，也即16字节的情况。

2． 使用下面数据测试你的算法：  
定义加密过程轮数为 Nr=10

密钥  
0X2B,0X7E,0X15,0X16, 0X28,0XAE,0XD2,0XA6, 0XAB,0XF7,0X15,0X88, X09,0XCF,0X4F,0X3C

明文  
0X32,0X43,0XF6,0XA8, 0X88,0X5A,0X30,0X8D, 0X31,0X31,0X98,0XA2,

0XE0,0X37,0X07,0X34

密文  
0X39,0X25,0X84,0X1D, 0X02,0XDC,0X09,0XFB, 0XDC,0X11,0X85,0X97,  
0X19,0X6A,0X0B,0X32  
3．修改加密算法，令Nr＝10，密钥的所有字节都是0。使用步骤2中的明文，计算并记录密文。  
（答案： e5 27 93 6d 04 9f 88 87 2a 49 03 30 5b 97 5b d1）  
4．将步骤2中的明文，改变1位，其它不变。记录密文中有多少字节发生变化。多重复几次，观察 AES 的扩散和混乱的效果。  
5．实现 AES 解密算法，要求同步骤 1。使用步骤2中的数据测试算法。  
6．修改解密算法，令 Nr=10，Key为全0，密文为步骤2中的密文。运行解密算法，记录明文。  
注意，要求将源代码以及每一步的结果写入报告

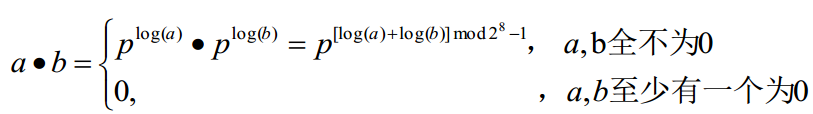
五、思考题  
研究 AES 密文的随机性，探讨使用加密算法做为随机数发生器的可行性。

六、附录  
1． GF(2)多项式乘法运算  
GF(2)上的多项式系数仅有0，1两种情况。 GF（2）的 7 次多项式可以使用 8 位二进制数表示：例如 x7+x5+1 可以表示为（10100001）。算法中的多项式的输入输出都是以这种形式表示的。不可约多项式，一般的对于有限域 GF（28） 上都是 8 次多项式，其最高阶的项的系数比为 1，因此可以省略表示，于是用一个 8 位二进制数表示。  
输入：两个最高次数为 7 次的多项式 A(x),B(x)，一个 GF(2)上的 8 次多项式 M(x)  
输出： A(x)\*B(x) modM(x)  
具体 C 语言形式代码如下：  
BYTE Multi\_P(BYTE Ax, BYTE Bx, BYTE Mx)  
{  
 BYTE Cx=0;  
 for(int i=0; i<8;i++)  
 {  
 Cx = ((Cx & 0x80) ==0)?(Cx<<1):(Mx^(Cx<<1));  
 if((Ax&0x80)!=0)  
 {  
 Cx = Cx ^ Bx;  
 }  
 Ax = Ax<<1;  
 }  
 return Cx;  
}

2．有限域 GF（28）上的运算有限域 GF（28）的元素为多项式，最高次数小于等于7

加法： 多项式加法，也就是对应的系数相加模 2。若以二进制数表示一个多项式，那么两个多项式相加相当于两个二进制数相异或。  
代码如下：  
BYTE GF\_add(BYTE x,BYTE y){ return ( x ^ y ); }

乘法：多项式 A(x),B(x),不可约多项式 M(x)。  
A(x)\*B(x) mod M(x)

计算方法有两种：  
1） 通过直接调用函数 Multi\_P 实现。  
2） 根据有限域的性质，采用指数形式计算。  
即：每个元素 a 都可以表示为 px， p 是域中的本原元, x=log(a)。元素 a,b  
相乘的结果相当于：  
  
于是 ，如果建立 GF（28）所有元素的对数表，及指数表，那么就可以通过查  
表得到结果。显然同第一种方法相比，这种计算方法更快。  
代码如下：  
BYTE GF\_Mul(BYTE x, BYTE y)  
{  
 if(x!=0 && y!=0)  
 {  
 // GF\_2\_8\_pow 是指数表， GF\_2\_8\_log 是对数表  
 return GF\_2\_8\_pow[(GF\_2\_8\_log[x] + GF\_2\_8\_log[y])%0xFF];  
 }  
 else  
 {  
 return 0;  
 }  
}  
至于指数表、 对数表的建立，可以通过调用 Multi\_P 来实现，比如  
p3 mod m(x)=(((p\*p) mod m(x))\*p) mod m(x)  
调用两次函数 Multi\_P 就可以得到 p3 mod m(x)。通过这种方式就可以得到指数  
表，然后由指数表反推就得到对数表。 这里需要特别注意对于 0 的处理。  
逆运算：已知任意一个非零元素 a，求其逆元 a-1，使得 a·a-1=1。  
求逆元的快速的方法，就是通过查表，先求出 log(a),然后，计算逆元的指数 log(a)  
＝，最后通过查指数表求出 p，也就是 a 的逆元。  
特别地： 0 没有逆元，直接返回 0。  
算法如下：  
BYTE GF\_Reverse(BYTE x)  
{  
 // GF\_2\_8\_pow 是指数表， GF\_2\_8\_log 是对数表  
 return x!=0?GF\_2\_8\_pow[(0xFF-GF\_2\_8\_log[x])]:0;  
}  
3． AES 基本运算  
为了简化运算， 接下来介绍的算法都是基于这样的假设：  
a) 算法密钥为 128 位，每个块为 128 位，也就是 16 个字节。  
b) 每种变换算法的输入都是一个块，也就是每次处理 16 个字节  
AES 加密过程由 4 个基本基本动作组成，包括： S 盒变换、行移位变化、列混合变换、轮密钥加法变换。 接下来，我们看看这些细节是如何实现的。  
1） S 盒变换  
算法：通过查表 SBox 实现。以 16 个字节为基本单位，分别对每个字节查表替换以  
相应的表中内容。  
void SubBytes(BYTE state[16])  
{  
 for(int i=0; i<16;i++)  
 {  
 state[i] = SBox[state[i]];  
 }  
 return;  
}  
SBox 可以通过计算生成。 也可以以全局数组的形式直接写入代码中。  
以下方法用来计算 SBox[x]  
BYTE c= 0x63;  
求字节 x 的逆： b = GF\_Reverse(x)  
然后，依次计算每一位  
 for i=0 to 7  
 //bit(b,i)返回字节 b 的第 i 位的值： 0 或 1。 ⊕为异或预算  
 B= bit(b, i) ⊕bit(b, (i+4)mod8) ⊕ bit(b, (i+5) mod8)  
 ⊕ bit(b, (i+6)mod8) ⊕bit(b, (i+7)mod8) ⊕ bit(c, i)  
 setbit(SBox[x], i, B) //设置 SBox[x]的第 i 位为 B  
endfor  
2） 行移位变换  
这个变换很简单：输入为 state[16]。state[0]-state[3]不变 state[4]-state[7]循环左移 1 个字节， state[8]-state[11] 循环左移2个字节，state[12]-state[15] 循环左移 3 个字节。算法如下：  
输入：16个字节构成的一个块 state[16]  
输出：变换后的结果保存在 state[16]  
Void ShiftRows( BYTE state[16])  
{  
 BYTE t[4];  
 for(int i=1; i<4; i++)  
 {  
 for( int j=0; j<4; j++ )  
 {  
 t[j] = state[ i\*4 + (j+i)%4 ];  
 }  
 memcpy(state+4\*i, t, 4);  
 }  
}  
3） 列混合变换  
输入： 16 个字节构成的一个块： state[16]  
输出：变换后的结果保存在 state[16]  
算法：按列处理，每列表示为 s(x) = S[3][i]x3+ S[2][i]x2+ S[1][i]x+ S[0][i]，然后计算  
[{03}x3+{01}x2+{01}X+{02}]\*s(x) mod (x4+1) 得到新的多项式，其系数对应S[0][i]-S[3][i]变换后的字节值。

Void MixColumns(BYTE state[16])  
{  
 BYTE temp[4][4];  
 memcpy(temp, state, 16); //将 state复制到 temp中，temp[i][j]=state[i\*4+j]

for(int i=0; i<4; i++) //第 i 列

{

for(int j=0; j<4; j++) //第 j 行， ⊕为异或运算  
{  
 state[j\*4+i] =  
 GF\_Mul(0x2, temp[j][i])  
 ⊕GF\_ Mul (0x3, temp[(j+1) mod 4][i])

⊕temp[ (j+2)mod 4 ][i] ⊕temp[ (j+3)mod 4 ][i] ;  
 }  
 }  
}  
  
4） 轮密钥加法变换  
每个块的加密都要经过 Nr（不妨取 Nr＝10） 轮变换。 在第 i 轮变换，使用第 i 个扩展密钥 k(i)变换是输入与密钥异或的过程  
代码如下：  
void AddRoundKey(BYTE state[16],BYTE key[16])  
{  
 for(int i=0; i<4; i++)  
 {  
 for( int j=0; j<4; j++ )  
 {  
 state[ i\*4 + j] = state[ i\*4 + j] ⊕key[j\*4+i];  
 }  
 }  
}  
5） 密钥扩展算法  
选取 128 位的密钥，也就是 16 个字节的密钥，通过扩展算法，生成 Nr 个扩展密钥。  
对于第 r 轮(r 从 1 开始计数)用的密钥  
输入： r 表示当前要扩展第 r 轮密钥， r>0  
数组 key 的前 16 字节放入第 r-1 轮密钥  
输出： 数组 key 的后 16 字节写入第 r 轮密钥  
注意： 第 0 轮的密钥也就是初始密钥  
void make\_key(BYTE key[32], int r)  
{  
 const BYTE RC[10]={0x1,0x2,0x4,0x8,0x10,0x20,0x40,0x80,0x1B,0x36};  
 BYTE \*temp = key;  
 DWORD \*dw\_key= (( DWORD\*)(temp));  
 //存储第四个双字，也就是最后 4 个字节  
 DWORD dw3= dw\_key[3];  
 //对第一个字，旋转并替换  
 BYTE t = temp[4\*3+0];  
 temp[4\*3+0] = gSBox[temp[4\*3+1]];  
 temp[4\*3+1] = gSBox[temp[4\*3+2]];  
 temp[4\*3+2] = gSBox[temp[4\*3+3]];  
 temp[4\*3+3] = gSBox[t];  
 //对第一个字，异或  
 temp[4\*3] = temp[4\*3]^RC[r-1];  
 //第 i－1 个字 与 第 i-3 个字  
 for(int i=4; i<7;i++)  
 {  
 dw\_key[i] = dw\_key[i-1]^dw\_key[i-4];  
 }  
 dw\_key[7] = dw\_key[6]^dw3;  
 dw\_key[3] = dw3;  
}  
通过反复调用函数 make\_key 就可以生成任意轮扩展密钥。 对于 128 位的密钥，可  
以取 Nr=10。  
4． AES 加密算法  
这里仅仅描述对 1 个块的加密，对更长的数据，则需要依据不同的模式，使用加密算法。算法如下：  
输入：明文 in ， 密钥 key  
输出：密文 out  
AESEncrypt(BYTE in[16],BYTE out[16]， BYTE key[16])  
{  
 BYTE state[16];  
 int Nr = 10;  
 将 in 看作 4×4 的矩阵，做转置运算： state[ i\*4+j ] = in[ j\*4+i ]  
 生成 10 轮扩展密钥，记录在数组 key\_expand[11][16]中  
 AddRoundKey（state, key\_expand[0], 1）  
 for( round = 1; round<Nr; round++)  
 {  
 SubBytes(state);  
 ShiftRows(state);  
 MixColumns(state);  
 AddRoundKey(state, key\_expand[round]);  
 }将state 看作 4×4 的矩阵，做转置运算： out[ i\*4+j ] = state[ j\*4+i ]  
}  
5． AES 解密算法  
解密算法同加密算法的过程基本相同，具体运算需要 S 盒变换、行移位、列混合的逆运算。 扩展密钥使用顺序相反，先用第 Nr 轮扩展密钥，在使用 Nr－1 轮扩展密钥，直到第 0 轮扩展密钥。 过程不再详述。  
报告要求：  
1） 要求字数不少于 1000 字  
2） 列出参考文献。包括作者，标题，出处，日期等。  
3） 可以两人合作。请在报告中注明你们是如何分工的。

六、实验代码

#include <stdio.h>

#define N 4

static unsigned char Sbox[16\*16] = // S盒

{

//0 1 2 3 4 5 6 7 8 9 a b c d e f

/\*0\*/ 0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5, 0x30, 0x01, 0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x76,

/\*1\*/ 0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59, 0x47, 0xf0, 0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4, 0x72, 0xc0,

/\*2\*/ 0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xcc, 0x34, 0xa5, 0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x15,

/\*3\*/ 0x04, 0xc7, 0x23, 0xc3, 0x18, 0x96, 0x05, 0x9a, 0x07, 0x12, 0x80, 0xe2, 0xeb, 0x27, 0xb2, 0x75,

/\*4\*/ 0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e, 0x5a, 0xa0, 0x52, 0x3b, 0xd6, 0xb3, 0x29, 0xe3, 0x2f, 0x84,

/\*5\*/ 0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5b, 0x6a, 0xcb, 0xbe, 0x39, 0x4a, 0x4c, 0x58, 0xcf,

/\*6\*/ 0xd0, 0xef, 0xaa, 0xfb, 0x43, 0x4d, 0x33, 0x85, 0x45, 0xf9, 0x02, 0x7f, 0x50, 0x3c, 0x9f, 0xa8,

/\*7\*/ 0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf5, 0xbc, 0xb6, 0xda, 0x21, 0x10, 0xff, 0xf3, 0xd2,

/\*8\*/ 0xcd, 0x0c, 0x13, 0xec, 0x5f, 0x97, 0x44, 0x17, 0xc4, 0xa7, 0x7e, 0x3d, 0x64, 0x5d, 0x19, 0x73,

/\*9\*/ 0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a, 0x90, 0x88, 0x46, 0xee, 0xb8, 0x14, 0xde, 0x5e, 0x0b, 0xdb,

/\*a\*/ 0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5c, 0xc2, 0xd3, 0xac, 0x62, 0x91, 0x95, 0xe4, 0x79,

/\*b\*/ 0xe7, 0xc8, 0x37, 0x6d, 0x8d, 0xd5, 0x4e, 0xa9, 0x6c, 0x56, 0xf4, 0xea, 0x65, 0x7a, 0xae, 0x08,

/\*c\*/ 0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc6, 0xe8, 0xdd, 0x74, 0x1f, 0x4b, 0xbd, 0x8b, 0x8a,

/\*d\*/ 0x70, 0x3e, 0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0e, 0x61, 0x35, 0x57, 0xb9, 0x86, 0xc1, 0x1d, 0x9e,

/\*e\*/ 0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9, 0x8e, 0x94, 0x9b, 0x1e, 0x87, 0xe9, 0xce, 0x55, 0x28, 0xdf,

/\*f\*/ 0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x68, 0x41, 0x99, 0x2d, 0x0f, 0xb0, 0x54, 0xbb, 0x16

};

static unsigned char RoundKey[N][N] = // 轮密钥

{

0X2B,0X7E,0X15,0X16, 0X28,0XAE,0XD2,0XA6, 0XAB,0XF7,0X15,0X88,0X09,0XCF,0X4F,0X3C

};

void SubBytes(unsigned char State[N][N]) // 字节替代

{

int i, j;

char high;

char low;

for (i = 0; i < N; i ++)

{

for (j = 0; j < N; j ++)

{

low = State[i][j] & 0x0F; // 取低4位

high = (State[i][j] >> 4)&0x0f; // 取高4位

State[i][j] = Sbox[16\*high + low];

}

}

}

void ShiftRows(unsigned char State[N][N]) // 行移位

{

int i, j, k;

int shiftnum = 0;

char tmp;

for (i = 0; i < N; i ++)

{

for (j = 0; j < shiftnum; j ++) // 循环左移一次

{

tmp = State[i][0];

for (k = 0; k < N-1; k ++)

{

State[i][k] = State[i][k+1];

}

State[i][k] = tmp;

}

shiftnum ++; // 移位次数+1

}

}

unsigned char gfmultby01(unsigned char b)

{

return b;

}

unsigned char gfmultby02(unsigned char b)

{

if (b < 0x80)

return (unsigned char)(int)(b <<1);

else

return (unsigned char)( (int)(b << 1) ^ (int)(0x1b) );

}

unsigned char gfmultby03(unsigned char b)

{

return (unsigned char) ( (int)gfmultby02(b) ^ (int)b );

}

unsigned char choose(unsigned char a, unsigned char b)

{

if (a == 0x01)

{

return gfmultby01(b);

}

if (a == 0x02)

{

return gfmultby02(b);

}

if (a == 0x03)

{

return gfmultby03(b);

}

return b;

}

void MixColumns(unsigned char State[N][N]) // 列混合

{

unsigned char mix[N][N] =

{

0x02, 0x03, 0x01, 0x01,

0x01, 0x02, 0x03, 0x01,

0x01, 0x01, 0x02, 0x03,

0x03, 0x01, 0x01, 0x02

};

unsigned char tmp[N];

unsigned char end[N][N];

int i, j, k;

for (i = 0; i < N; i++)

{

for (j = 0; j < N; j++)

{

for (k = 0; k < N; k++)

{

tmp[k] = choose(mix[i][k], State[k][j]);

}

end[i][j] = tmp[0] ^ tmp[1] ^ tmp[2] ^ tmp[3];

}

}

for (i = 0; i < N; i++)

{

for (j = 0; j < N; j++)

{

State[i][j] = end[i][j];

}

}

}

void AddRoundKey(unsigned char State[N][N], unsigned char RoundKey[N][N])

{

int i,j;

for (j = 0; j < N; j ++)

{

for (i = 0; i < N; i ++)

State[i][j] = State[i][j] ^ RoundKey[i][j];

}

}

int main()

{

int i, j, tmp;

unsigned char State[N][N];

printf("请输入数据：");

for (i = 0; i < N; i++)

{

for (j = 0; j < N; j++)

{

scanf("%x", &State[i][j]); //0x19 0x3d 0xe3 0xbe 0xa0 0xf4 0xe2 0x2b 0x9a 0xc6 0x8d 0x2a 0xe9 0xf8 0x48 0x08

}

}

for (i = 0; i < N; i++)

{

for (j = 0; j < i+1; j++)

{

tmp = State[i][j];

State[i][j] = State[j][i];

State[j][i] = tmp;

}

}

printf("\n原始数据为：(列优先)\n");

for (i = 0; i < N; i++)

{

for (j = 0; j < N; j++)

{

printf("%0x ", State[i][j]);

}

printf("\n");

}

printf("\n");

SubBytes(State);

printf("字节替代后：\n");

for (i = 0; i < N; i++)

{

for (j = 0; j < N; j++)

{

printf("%0x ", State[i][j]);

}

printf("\n");

}

printf("\n");

ShiftRows(State);

printf("行移位后：\n");

for (i = 0; i < N; i++)

{

for (j = 0; j < N; j++)

{

printf("%0x ", State[i][j]);

}

printf("\n");

}

printf("\n");

MixColumns(State);

printf("列混合后：\n");

for (i = 0; i < N; i++)

{

for (j = 0; j < N; j++)

{

printf("%0x ", State[i][j]);

}

printf("\n");

}

printf("\n");

AddRoundKey(State, RoundKey);

printf("轮密钥加后：\n");

for (i = 0; i < N; i++)

{

for (j = 0; j < N; j++)

{

printf("%0x ", State[i][j]);

}

printf("\n");

}

return 0;

}