**//陈坦访SA15011010**

**//网络安全 文件加解密程序**

#include <memory.h>

#include <stdio.h>

#include <string.h>

#include <stdlib.h>

#include "aes.h"

#pragma comment(lib,"libeay32.lib")

int encrypt\_file(char inString[], char passwd[],char\* enString){

int i,j, len, nLoop, nRes;

unsigned char buf[16];

unsigned char buf2[16];

unsigned char aes\_keybuf[32];

AES\_KEY aeskey;

int pwdLen=strlen(passwd);

int inLen=strlen(inString);

// 准备32字节(256位)的AES密码字节

memset(aes\_keybuf,0x90,32);

if(pwdLen<32){ len=pwdLen; } else { len=32;}

for(i=0;i<len;i++) aes\_keybuf[i]=passwd[i];

// 输入字节串分组成16字节的块

nLoop=inLen/16; nRes = inLen%16;

// 加密输入的字节串

AES\_set\_encrypt\_key(aes\_keybuf,256,&aeskey);

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

memset(buf,0,16);

for(j=0;j<16;j++)

buf[j]=inString[i\*16+j];

AES\_encrypt(buf,buf2,&aeskey);

for(j=0;j<16;j++)

enString[i\*16+j]=buf2[j];

}

if(nRes>0){

memset(buf,0,16);

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

buf[j]=inString[i\*16+j];

AES\_encrypt(buf,buf2,&aeskey);

for(j=0;j<16;j++)

enString[i\*16+j]=buf2[j];

//puts("encrypt");

}

enString[i\*16+j]=0;

return 0;

}

int decrypt\_file(char enString[], char passwd[],char\* deString){

int i,j, len, nLoop, nRes;

unsigned char buf[16];

unsigned char buf2[16];

unsigned char aes\_keybuf[32];

AES\_KEY aeskey;

int pwdLen=strlen(passwd);

int inLen=strlen(enString);

// 准备32字节(256位)的AES密码字节

memset(aes\_keybuf,0x90,32);

if(pwdLen<32){ len=pwdLen; } else { len=32;}

for(i=0;i<len;i++) aes\_keybuf[i]=passwd[i];

// 输入字节串分组成16字节的块

nLoop=inLen/16; nRes = inLen%16;

AES\_set\_decrypt\_key(aes\_keybuf,256,&aeskey);

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

memset(buf,0,16);

for(j=0;j<16;j++) buf[j]=enString[i\*16+j];

AES\_decrypt(buf,buf2,&aeskey);

for(j=0;j<16;j++) deString[i\*16+j]=buf2[j];

}

if(nRes>0){

memset(buf,0,16);

for(j=0;j<16;j++) buf[j]=enString[i\*16+j];

AES\_decrypt(buf,buf2,&aeskey);

for(j=0;j<16;j++) deString[i\*16+j]=buf2[j];

//puts("decrypt");

}

deString[i\*16+nRes]=0;

return 0;

}

int encryptCmd(char cmd[], char inString[], char passwd[],char\* res){

if(0==strcmp(cmd,"enc")){

encrypt\_file(inString, passwd,res);

}

else if(0==strcmp(cmd,"dec")){

decrypt\_file(inString, passwd,res);

}

return 0;

}

int main(int argc, char\* argv[])

{

char inString[2000];

char outString[2000];

char filename[200]="inString.txt";

char passwd[55] = "0123456789ABCDEFGHIJK";

memset(inString,0,sizeof(inString));

memset(outString,0,sizeof(outString));

char cmd[10];

printf("请输入操作类型(enc or dec): ");

while(EOF!=scanf("%s",cmd)){

memset(inString,0,sizeof(inString));

memset(outString,0,sizeof(outString));

printf("请输入需要加解密的文件名: ");

scanf("%s",filename);

printf("请输入密钥: ");

scanf("%s",passwd);

//读取文件

FILE\* infile=fopen(filename,"rb");

fread(inString,sizeof(char),2000,infile);

fclose(infile);

encryptCmd(cmd,inString,passwd,outString);

{

char outfilename[50]="";

strcpy(outfilename,cmd);

strcat(outfilename,filename);

FILE\* outfile=fopen(outfilename,"wb+");

fwrite(outString, strlen(outString),1,outfile);

fclose(outfile);

if(!strcmp("enc",cmd)){

printf("加密结果输出在%s文件中\n",outfilename);

}

else if(!strcmp("dec",cmd)){

printf("加密结果输出在%s文件中\n",outfilename);

}

}

printf("\n\n请输入操作类型(enc or dec): ");

}

system("pause");

return 0;

}