攻防世界Crypto Easy-one （无脑科普向

原创

Gm1y 于 2019-08-13 00:06:45 发布 1447 收藏 2
分类专栏： 原题复现 文章标签： 攻防世界 crypto

本文链接：https://blog.csdn.net/jcbx_/article/details/99353450

Easy-one

做题思路：
题目说让我们破解msg002.enc的内容，然后给了msg001 和msg001.enc还有加密代码。我们要解密就要逆用这个加密算法，从msg001.enc解密就能得到msg001。注意代码里的k[]=“”是假的，本题需要我们利用msg001和msg001.enc去得到k，然后再用k代入解密算法解密msg002.enc才能得到flag。

思路讲了，有想法的就去试一下，不会的来看无脑科普：

下载得到四个文件。首先打开encryptor.c，一开始看也是一点都没看懂，然后查了一下资料。现在来科普一下argc和argv。

int main(int argc,char**argv)和int main(int argc,char *argv[])是一样的

argc是一个数，表示参数的个数；

argv 是一个指针数组，他的元素个数是argc，存放的是指向每一个参数的指针。
例如：在cmd里调用该代码生成的程序时

```
D:\Download\cryptology problem\GFSJ\GFSJ004-crypto100>working.exe ab
USAGE: working.exe input output
```

此时argc为2，argv[0]是指向working.exe的指针，argv[1]是指向ab字符串的指针。

```
D:\Download\cryptology problem\GFSJ\GFSJ004-crypto100>working.exe 22 11
Error!
```

此时argc为3，argv[0]是指向working.exe的指针，argv[1]和argv[2]分别指向22
和11。

好，下面深入分析。看代码：

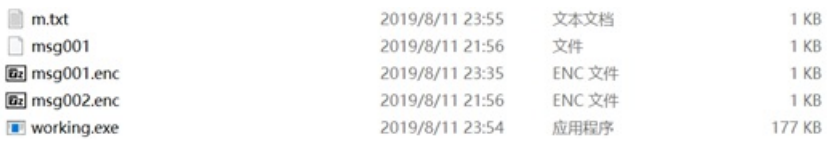
```
#include<stdio.h>
#include<stdlib.h>
#include<string.h>
int main(int argc,char **argv)
{
 if(argc!=3)
 {
  printf("USAGE: %s input output\n",argv[0]);return 0;
 }
 FILE *input=fopen(argv[1],"rb");
 FILE *output=fopen(argv[2],"wb");
 if(input==NULL)
 {
  printf("input Error!\n");return 0;
 }
 if(output==NULL)
 {
  printf("output Error!\n");return 0;
 }
```

看FILE那行，C的FILE函数可以百度自学，argv[1]后面是“rb”，所以它指向的文件是要存在的，不然没有办法打开文本文件读取数据；其次argv[2]后面是“wb”，如果没有该文件就会自动创建一个文件。

第一行命令：argv[1]是字符串a，显然不是一个文件，所以显示input Error!

而且还会在该目录创建一个文件b。（虽然没有数据

而这里argv[1]指向的是msg001，是一个文件，就没有报错，而且还会生成m.txt文件（如下图



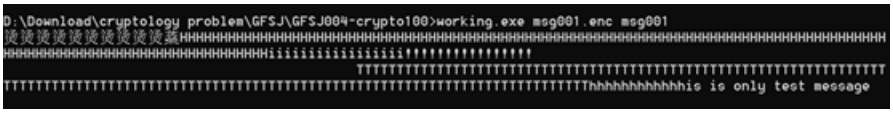
分割线hhh。。。
0xff:1111 1111
&0xff的作用是截取出后八位数据。
如：（0000 0001 1111 1000）&0xff=1111 1000

好了，讲重点：
一开始我的想法是读取msg001和msg001.enc的字符串然后再进行解密的，然后发现

```
while((p=fgetc(input))!=EOF||(c=fgetc(output))!=EOF)

 {printf("%c ",c);}
```

while()这样用会出问题。。。



所以把msg001写进代码里当作数组就行了。

解密代码（解k）如下：

```
#include<stdio.h>
#include<stdlib.h>
#include<string.h>
int main(int argc,char **argv)
{
 if(argc!=2)
 {
  printf("USAGE: %s input output\n",argv[0]);return 0;
 }
 FILE *input=fopen(argv[1],"rb");
 char k[]="Hi! This is only test message";
 char p,t=0;
 char m;
 unsigned int i=0,j;
 while(i<strlen(k))
 {
  p=fgetc(input);
  for(j=0;j<128;j++)
  {
   m=(p-(j^t)-i*i)&0xff;
   if(m==k[i])
   { i++;
    printf("%c",j);
    t=m;
    break;
   }
  }

 }
 return 0;
}
```

结果

```
D:\Download\cryptology problem\GFSJ\GFSJ004-crypto100>working.exe msg001.enc
VeryLongKeyYouWillNeverGuessU
```

k为VeryLongKeyYouWillNeverGuess

然后把加密代码转换成解密代码再代入k即可得到flag！

只是在加密代码里把这一段改了就ok

```
while((p=fgetc(input))!=EOF)
 {
  c=(p-(k[i%strlen(k)]^t)-i*i)&0xff;
  t=c;
  i++;
  fputc(c,output);
 }
```

然后输入命令。。。

```
D:\Download\cryptology problem\GFSJ\GFSJ004-crypto100>working.exe msg002.enc flag.txt
```

大功告成！

参考链接： https://blog.csdn.net/zz_Caleb/article/details/89575430