攻防世界 Crypto高手进阶区 5分题 Easy-one

原创

思源湖的鱼 于 2021-01-04 14:18:05 发布 127 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112102890

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的5分题

本篇是Easy-one的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到一段c和一对明文密文和一个要解密的密文

```c
#include <stdlib.h>
#include <stdio.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 || !output) {
  printf("Error\n");
  return 0;
 }
 char k[] = "CENSORED";
 char c, p, t = 0;
 int i = 0;
 while ((p = fgetc(input)) != EOF) {
  c = (p + (k[i % strlen(k)] ^ t) + i*i) & 0xff;
  t = p;
  i++;
  fputc(c, output);
 }
 return 0;
}
```

是使用`k[]`和`input`经过加密算法后生成`output`
那不就逆着来就是了

尝试对msg001.enc解密

```python
f1=open("msg001",'rb+')
f2=open("msg001.enc",'rb+')
p=f1.read()
c=f2.read()
a=0
b=0
t=0
k='CENSORED'
flag=""
for i in range(len(c)):
 a=ord(c[i])
 b=(c-i*i-(ord(k[i%len(k)])^t))&0xff
 t=b
 flag+=chr(b)
print(flag)
```

结果得到一堆乱码
没有得到对应的明文

那看来是k是个例子
不是真k

先得到k

```
f1=open("msg001",'rb+')
f2=open("msg001.enc",'rb+')
p=f1.read()
c=f2.read()
p =[ ord(i) for i in p]
c =[ ord(i) for i in c]
t=0
key=""
for i in range(len(p)):
 k=((c[i]-p[i]-i*i)^t)&0xff
 t=p[i]
 key=key+chr(k)
print(key)
```

得到k：`VeryLongKey YouWillNeverGuess`

然后解密

```
f=open("msg002.enc",'rb+')
c=f.read()
c=[ord(i) for i in c]
t=0
flag=""
key="VeryLongKeyYouWillNeverGuess"
key =[ord(i) for i in key]
for i in range(len(c)):
 p=(c[i]-(key[i%len(key)]^t)-i*i)&0xff
 t=p
 flag+=chr(p)
print(flag)
```

得到flag

```
CTF{6d5eba48508efb13dc87220879306619}
```

结语

重点是求k