BUUCTF中Crypto的RSAROLL

原创

沐一 · 林 已于 2022-04-10 14:34:09 修改 130 收藏

分类专栏： CTF 密码学 文章标签： ctf

于 2022-03-18 10:03:17 首次发布

本文链接：https://blog.csdn.net/xiao__1bai/article/details/123567209

CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏

密码学

51 篇文章 1 订阅

订阅专栏

BUUCTF中Crypto的RSAROLL

.

.

照例下载附件，两个 txt 文件：

> RSA roll！roll！roll！
> Only number and a-z
> （don’t use editor
> which MS provide）

> {920139713,19}
> 704796792
> 752211152
> 274704164
> 18414022
> 368270835
> 483295235
> 263072905
> 459788476
> 483295235
> 459788476
> 663551792
> 475206804
> 459788476
> 428313374
> 475206804
> 459788476
> 425392137
> 704796792
> 458265677
> 341524652
> 483295235
> 534149509
> 425392137
> 428313374
> 425392137
> 341524652
> 458265677
> 263072905
> 483295235
> 828509797
> 341524652
> 425392137
> 475206804
> 428313374
> 483295235
> 475206804
> 459788476
> 306220148

.

.

说实话一开始我没看懂考啥，后来才发现这些数字中前面两个是`n,e`，后面是拆分的`密文 c`。原来题目的`roll`是滚动拼接`flag`的意思。想了想，这种多 RSA 参数的题，有点类似于我做过的 2022 年HGAME中CRYPTO的Easy RSA。

那直接套用脚本如下：

```python
import libnum
from Crypto.Util.number import long_to_bytes
list1=[704796792,
752211152,
274704164,
18414022,
368270835,
483295235,
263072905,
459788476,
483295235,
459788476,
663551792,
475206804,
459788476,
428313374,
475206804,
459788476,
425392137,
704796792,
458265677,
341524652,
483295235,
534149509,
425392137,
428313374,
425392137,
341524652,
458265677,
263072905,
483295235,
828509797,
341524652,
425392137,
475206804,
428313374,
483295235,
475206804,
459788476,
306220148]
flag=""
n=920139713
q=18443
p=49891
e=19
for i in list1:
 c=i
 d = libnum.invmod(e, (p - 1) * (q - 1))   #invmod(a, n) - 求a对于n的模逆,这里逆向加密过程中计算ψ(n)=(p-1)(q-1)，对ψ(n)保密,也就是对应根据ed=1modψ(n),求出d
 m = pow(c, d, n)        # pow(x, y[, z])--函数是计算 x 的 y 次方，如果 z 在存在，则再对结果进行取模，其结果等效于 pow(x,y) %z，对应前面解密算法中M=D(C)=C^d(mod n)
#print(m) #明文的十进制格式
 string = long_to_bytes(m)      # m明文，用长字节划范围
 flag+=string.decode()
print(flag)
```

```
└─$ python 15.py
flag{13212je2ue28fy71w8u87y31r78eu1e2}
```

.

.

解毕！

敬礼！