2022DASCTF Apr X FATE 防疫挑战赛 CRYPTO easy_real

原创

雨后初雾& 已于 2022-04-23 19:35:40 修改 407 收藏 1
分类专栏： 密码学CTF 文章标签： CTF Crypt
于 2022-04-23 19:24:06 首次发布

逆向一道都不会，寄了。只做了密码的签到题

题目描述

```
import random
import hashlib

flag = 'xxxxxxxxxxxxxxxxxxx'
key = random.randint(1,10)
for i in range(len(flag)):
    crypto += chr(ord(flag[i])^key)
m = crypto的ascii十六进制
e = random.randint(1,100)
print(hashlib.md5(e))
p = 643104133067764064223340340471525819003656873743364188631911773389011986083 19
q = xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
n = p*q
c = pow(m,e,n)
print(n)
print(c)
#37693cfc748049e45d87b8c7d8b9aacd
#419735662257669656449056906068624008888418711356643013446194513077090682518789439467284146735
#329817686269717538993572242014386700097090672311062548480285081063481464782757203491339197264
```

从代码中不难看出

```
#37693cfc748049e45d87b8c7d8b9aacd 对应相应的e的md5值

到相应的网站解密

e=23
```

其他的分别定义

```
n=419735662257669656449056906068624008888418711356643013446194513077090682518789439467284146735079701594072
c=329817686269717538993572242014386700097090672311062548480285081063481464782757203491339197264039944641599
p = 643104133067764064223340340471525819003656873743364188631911773389011986083l9
```

根据代码，我们不难看出，这是典型的rsa加密

直接求出明文的数值

```
from Crypto.Util.number import inverse,long_to_bytes

n=419735662257669656449056906068624008888418711356643013446194513077090682518789439467284146735079701594072
c=329817686269717538993572242014386700097090672311062548480285081063481464782757203491339197264039944641599
p = 643104133067764064223340340471525819003656873743364188631911773389011986083l9
q=n//p
e=23
phi=(q-1)*(p-1)
d=inverse(e,phi)
m = pow(c, d, n)
print(m);
//m=297616873614238045584178413440743143478405791177342374375l382131043957
//m="ndios_;9kgE;WK8e;W?gWn<\;k|nu"
```

我们接着观察

> key是一个随机值
>
> 但是有范围的
>
> 我们直接暴力枚举

```
import random
import hashlib
import math
from Crypto.Util.number import inverse,long_to_bytes

n=419735662257669656449056906068624008888418711356643013446194513077090682518789439467284146735079701594072
c=329817686269717538993572242014386700097090672311062548480285081063481464782757203491339197264039944641599
p = 643104133067764064223340340471525819003656873743364188631911773389011986083l9
q=n//p
e=23
phi=(q-1)*(p-1)
d=inverse(e,phi)
m = pow(c, d, n)
print(m);
m="ndios_;9kgE;WK8e;W?gWn<\;k|nu"
for key in range(11):
  flag=""
  for i in range(len(m)):
    flag+=chr(ord(m[i])^key)
  print(flag)
```

```
j`mkw[?=ocA?SO<a?S;cSj8X?oxjq
kaljvZ><nb@>RN=`>R:bRk9Y>nykp
hboiuY=?maC=QM>c=Q9aQh:Z=mzhs
icnhtX<>l`B<PL?b<P8`Pi;[<l{ir
flag{W31coM3_C0m3_7o_f4T3ctf}
gm`fzV20bnL2^B1l2^6n^g5U2bug|
```

直接出flag

打了这么多比赛，还是菜。

很多题目赛后根本没复现，真是失败的菜鸡，呜呜呜。

校内可以交流的师傅太少，听说最近联合战队在招新，准备去试试。