BUUCTF Crypto BabyRSA

原创

cxxxxxxxc 于 2021-07-15 21:06:57 发布 240 收藏 1

分类专栏： buuctf

本文链接：https://blog.csdn.net/m0_47305816/article/details/118767996

buuctf BabyRSA

首先查看给的已知条件

p+q : 0x1232fecb92adead91613e7d9ae5e36fe6bb765317d6ed38ad890b4073539a6231a66

(p+1)(q+1) : 0x5248becef1d925d45705a7302700d6a0ffe5877fddf9451a9c1181c4d8236580

e : 0xe6b1bee47bd63f615c7d0a43c529d219

d : 0x2dde7fbaed477f6d62838d55b0d0964868cf6efb2c282a5f13e6008ce7317a24cb57aec4

enc_flag : 0x50ae00623211ba6089ddfae21e204ab616f6c9d294e913550af3d66e85d0c0693e

分析已知条件，已知密文c，p+q,(p+1)(q+1),e,d求明文得到flag

由(p+1)(q+1)和p+q可计算得到pq，也就是n

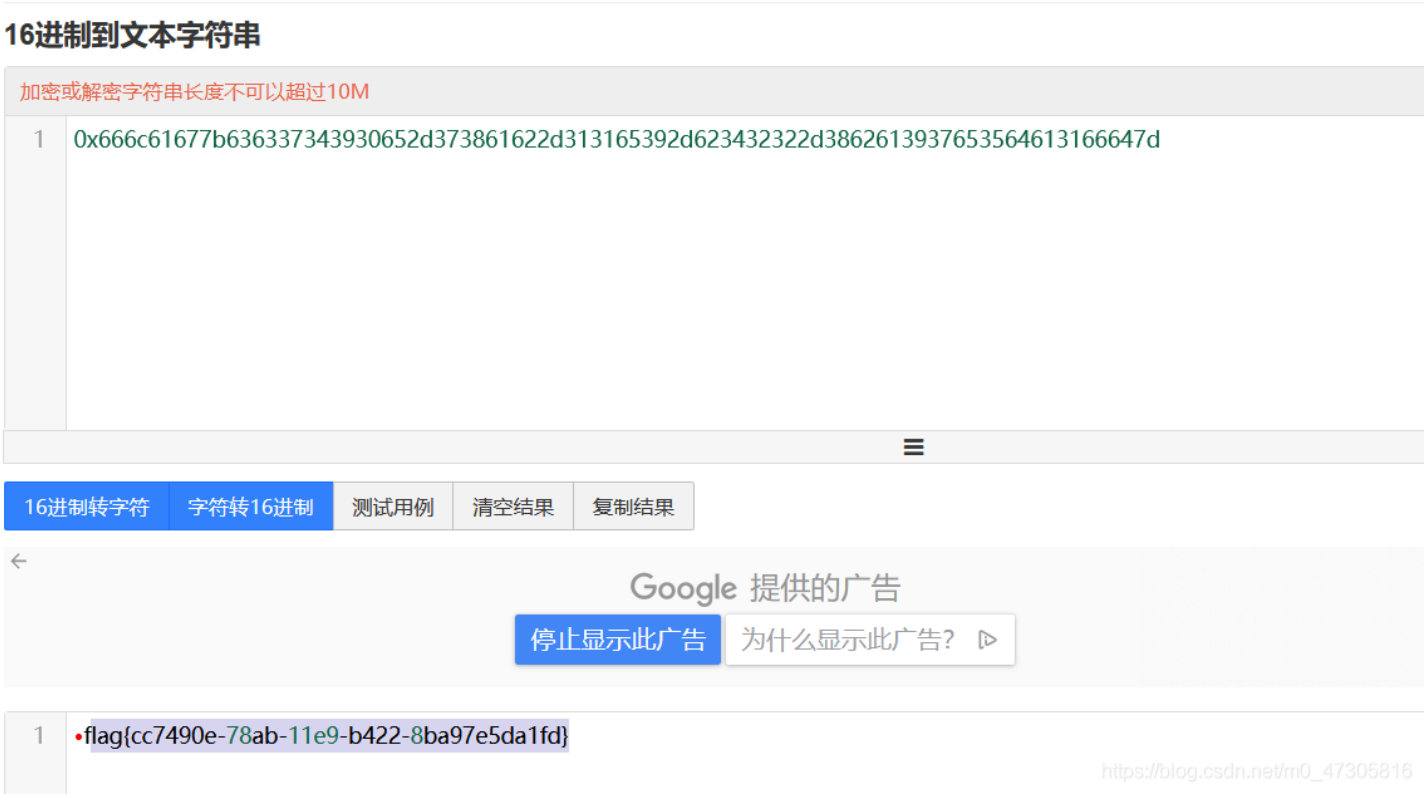
明文m=c^d mod n；

代码：

```
#(p+1)(q+1)
f=0x5248becef1d925d45705a7302700d6a0ffe5877fddf9451a9c1181c4d82365806085fd86fbaab08b6fc66a967b2566d743c626547203
b34ea3fdb1bc06dd3bb765fd8b919e3bd2cb15bc175c9498f9d9a0e216c2dde64d81255fa4c05a1ee619fc1fc505285a239e7bc655ec6605
d9693078b800ee80931a7a0c84f33c851740
#p+q
s=0x1232fecb92adead91613e7d9ae5e36fe6bb765317d6ed38ad890b4073539a6231a6620584cea5730b5af83a3e80cf30141282c97be44
00e33307573af6b25e2ea
#计算得到n值
n=f-s-1
print(n)
d=0x2dde7fbaed477f6d62838d55b0d0964868cf6efb2c282a5f13e6008ce7317a24cb57aec49ef0d738919f47cdcd9677cd52ac2293ec59
38aa198f962678b5cd0da344453f521a69b2ac03647cdd8339f4e38cec452d54e60698833d67f9315c02ddaa4c79ebaa902c605d7bda32ce
970541b2d9a17d62b52df813b2fb0c5ab1a5
c=0x50ae00623211ba6089ddfae21e204ab616f6c9d294e913550af3d66e85d0c0693ed53ed55c46d8cca1d7c2ad44839030df26b70f22a8
567171a759b76fe5f07b3c5a6ec89117ed0a36c0950956b9cde880c575737f779143f921d745ac3bb0e379c05d9a3cc6bf0bea8aa91e4d5e
752c7eb46b2e023edbc07d24a7c460a34a9a
#计算明文
print(hex(pow(c,d,n)))
```

得到结果：

```
0x666c61677b636337343930652d373861622d313165392d623432322d3862613937653564613166647d
```



最后进行16进制转字符得到flag{cc7490e-78ab-11e9-b422-8ba97e5da1fd}