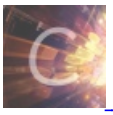
BUUCTF Crypto [GUET-CTF2019]BabyRSA wp

原创

嗵嘘的羊腰子 于 2020-03-16 16:22:27 发布 1244 收藏

分类专栏： BUUCTF Crypto 文章标签： python 密码学 rsa

本文链接：https://blog.csdn.net/weixin_44017838/article/details/104901893



这题RSA非常简单，给出了p+q和（p+1）*(q+1)的值，通过简单的拼凑就可以得到n和欧拉函数phin的值，直接求得flag出来，脚本如下

```
// python2
import gmpy2
a =0x1232fecb92adead91613e7d9ae5e36fe6bb765317d6ed38ad890b4073539a6231a6620584cea5730b5af83a3e80cf30141282c97be4
400e33307573af6b25e2ea
b=0x5248becef1d925d45705a7302700d6a0ffe5877fddf9451a9c1181c4d82365806085fd86fbaab08b6fc66a967b2566d743c626547203
b34ea3fdb1bc06dd3bb765fd8b919e3bd2cb15bc175c9498f9d9a0e216c2dde64d81255fa4c05a1ee619fc1fc505285a239e7bc655ec6605
d9693078b800ee80931a7a0c84f33c851740
e=0xe6b1bee47bd63f615c7d0a43c529d219
d=0x2dde7fbaed477f6d62838d55b0d0964868cf6efb2c282a5f13e6008ce7317a24cb57aec49ef0d738919f47cdcd9677cd52ac2293ec59
38aa198f962678b5cd0da344453f521a69b2ac03647cdd8339f4e38cec452d54e60698833d67f9315c02ddaa4c79ebaa902c605d7bda32ce
970541b2d9a17d62b52df813b2fb0c5ab1a5
enc_flag=0x50ae00623211ba6089ddfae21e204ab616f6c9d294e913550af3d66e85d0c0693ed53ed55c46d8cca1d7c2ad44839030df26b
70f22a8567171a759b76fe5f07b3c5a6ec89117ed0a36c0950956b9cde880c575737f779143f921d745ac3bb0e379c05d9a3cc6bf0bea8aa
91e4d5e752c7eb46b2e023edbc07d24a7c460a34a9a
n=b-a-1
phi=n-a+1
d=gmpy2.invert(e,phi)
m=pow(enc_flag,d,n)
flag=hex(m)[2:].decode('hex')
print(flag)
#flag{cc7490e-78ab-11e9-b422-8ba97e5da1fd}
```