BugkuCTF-Crypto题给你私钥吧

原创

彬彬有礼am_03 于 2021-08-31 15:03:06 发布 1248 收藏 1

分类专栏： # BugkuCTF-Crypto 文章标签： 安全

本文链接：https://blog.csdn.net/am_03/article/details/120017354

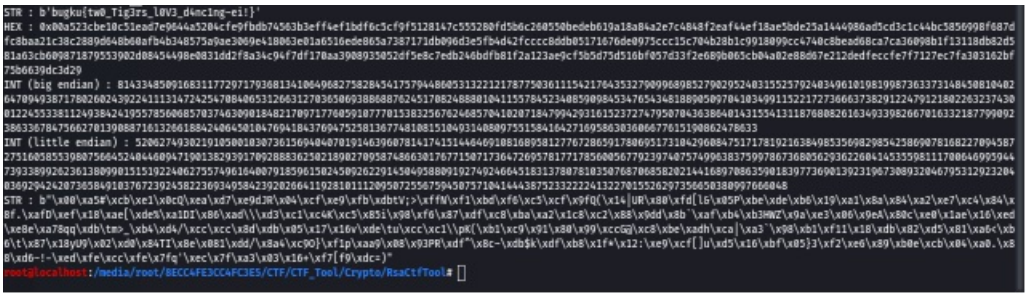
BugkuCTF-Crypto 专栏收录该内容

20 篇文章 1 订阅

订阅专栏

方法一

用 RsaCtfTool这个脚本工具。。。然后python RsaCtfTool.py --publickey pubkey.pem --uncipherfile flag.enc直接用公钥进行攻击解密



方法二

思路：高位攻击还原pq，然后生成密钥进行解密
分三步：

```
#第一步解析私钥文件，发现给了一个因数的高位，那么高位攻击还原p,q
n =26485201714915839490865227813246218372938736243516916108608439705738170543023112509150522274284238701776297205717958250714
pbar =16734350600597400338050606967960773738194020468617321418886005700490900605522051607428309016043083300742497098065574831
kbits =384
PR.<x> = PolynomialRing(Zmod(n))
f = x + pbar
x0 = f.small_roots(X=2^kbits, beta=0.4)[0]
p = x0 + pbar
print(p)
q = n // int(p)
print(q)
```

```
#第二步利用p,q,e,c生成私钥文件
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import gmpy2
e=65537
p=16734350600597400338050606967960773738194020468617321418886005700490900605522051607428309016043083300742497098065574831023
q=15779041771703527594319790482364514528114708525290524744726003405187869103474768430371533634850726792124965510326334791412
n=p*q
d=gmpy2.invert(e,(p-1)*(q-1))
privkey=RSA.construct((int(n),e,int(d)))
f = open('privkey2.pem','wb')
f.write(privkey.export_key())
f.close()
```

3.第三步通过私钥文件OAEP解密

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import base64

cipher_text=open(r"flag.enc","rb").read()
ciphertxt=base64.b64decode(cipher_text)

key=RSA.importKey(open(r"privkey2.pem").read())

cipher=PKCS1_OAEP.new(key)

message=cipher.decrypt(ciphertxt)
print(message)
```

#其实第二步也可以省略，主要考察rsa解析文件之类的