WeakRSA

发表于 2021-01-21 分类于 Challenge ， 2017 ， HCTF ， Extra
Challenge | 2017 | HCTF | Extra | WeakRSA

点击此处获得更好的阅读体验

WriteUp 来源

https://xz.aliyun.com/t/1589

题目考点

解题思路

已知部分 d 的最低有效位，是可以还原出 d 的，原理部分。但对于已知的位数是有要求的

其中 M=2^k，k 是 d 的最低有效位的位数出题时没测试好，本来是要给的位数不够还原，需要爆破的，给下脚本

```
#!/usr/bin/python
#-*- coding:utf-8 -*-

import sys, re
from libnum import nroot
from Crypto.Util.number import size

n = 24129492308224479830531863430667763206113500947912894148049103046436751018902380216549212087945014575866175372699327952352562583984599024982322742653474650254469019243
e = 65537

low_d2 = 58502105042243779040030927793473642167117490345311828777326272723727699009660868431125282048528958230023783207342012219791178732940043860984302461944922966247750
low_bits = 1028
test = pow(3, e, n)

i = 0
prefix = []
for a in range(2):
    for b in range(2):
        prefix.append(str(a) + str(b))

for bf in prefix:
    low_d = int(bin(low_d2)[2:], 2)
    for k in xrange(1, e):
        d = (k * n + 1) / e
        d >>= low_bits
        d <<= low_bits
        d |= low_d
        if (e * d) % k == 1:
            if pow(test, d, n) == 3:
                    print k, d
```

Flag

```
无
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2017/HCTF/Extra/27hn1QeLzZ6tYEzyiZatQc.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2017 # HCTF # Extra
BabyRSA
破解加密数据