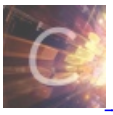
BUUCTF Crypto SameMod wp

原创

嗜嘘的羊腰子 于 2020-03-15 21:16:35 发布 1253 收藏 2

分类专栏： BUUCTF Crypto

本文链接：https://blog.csdn.net/weixin_44017838/article/details/104886290



这道题一看题目SameMod就可以猜到是RSA中的共模攻击

关于共模攻击的原理这里就不多赘述了，可以参考ctfwiki

https://wiki.x10sec.org/crypto/asymmetric/rsa/rsa_module_attack

下面直接给出本题脚本

```
// python2
from gmpy2 import invert
def gongmogongji(n, c1, c2, e1, e2):
    def egcd(a, b):
        if b == 0:
            return a, 0
        else:
            x, y = egcd(b, a % b)
            return y, x - (a // b) * y
    s = egcd(e1, e2)
    s1 = s[0]
    s2 = s[1]
    if s1 < 0:
        s1 = - s1
        c1 = invert(c1, n)
    elif s2 < 0:
        s2 = - s2
        c2 = invert(c2, n)
    m = pow(c1, s1, n) * pow(c2, s2, n) % n
    return m

n= 6266565720726907265997241358331585417095726146341989755538017122981360742813498401533594757088796536341941659691259323065631249
e1= 773
e2= 839
c1= 345352059272344393545115154524502586423238887172168232640891502434980406204197670236472866068291239690396819398113155311153734 9
c2= 567281802681629334407011933253662961945716357003630529686905353229310537969079338601906575446529286776952173641417080323830953 5

result = gongmogongji(n, c1, c2, e1, e2)
print(result)
#10210897103123119104101110119101116104105110107105116105115112111115115105981081011 25
#flag=hex(result)[2:].decode('hex')
result=str(result)
flag=""
i=0
while i < len(result):
    if result[i]=='1':
        c=chr(int(result[i:i+3]))
        i+=3
    else:
        c=chr(int(result[i:i+2]))
        i+=2
    flag+=c
print(flag)
#flag{whenwethinkitispossible}
```

做这题的时候一开始想到是将明文进行hex的，试了一下发现不对，才通过ascii的方式解得，flag需要是可见字符，所以不存在1开头的十位数，所以1开头的肯定是100以上的三位数，由此可解得flag