easyrsa

发表于 2021-01-15 分类于 Challenge， 2020， 安洵杯， Crypto
Challenge | 2020 | 安洵杯 | Crypto | easyrsa

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/8581

题目考点

- *RSA*

解题思路

这道题首先将加密脚本给加密了,可以很明显的看出是python脚本的仿射加密

通过查找关键词可以对比出a = 9,b = 9,从而解出加密脚本

这道题一共有三个rsa的问题,对应的思路如下:

- *hint1 = 2 * d + 246810 * e* phi，根据数论知识,其实只要d满足e * dmodϕ(n)=1即可解密，所以在这里d = hint1 // 2*
- *解出的q非素数,把q分解成素数积来求得phi*
- *穷据两位十进制数字达到coppersmith攻击最低攻击条件*

```
#!/usr/bin/python
import gmpy2
from Crypto.Util.number import long_to_bytes
import math
n = 10050095014547257781432719892909820612730955980465259676378711053379530637537082959157449310691856567584792956476780977871348290765339769265796235196183464082153542864
c = 52262705117267321660701973837874987411677287785834474834962732197749215810569988736989307958145004878913157855633818600498353397545498845045063514126715713550603284912
hint = 13480577432861562444657449032280328354731669864721413848757635248243886718609427626373534255816900477328677963293936909991063998416526372478195884100957315624153195
d = hint // 2
q = gmpy2.powmod(c,d,n)

# ------------------
n = 13356199152371171423864151298780933053021224689256959302631941144979108419411587378130142259349580692787582829062967902009883418252801283546935247163508737540630653488
p = 68915932675833086420599381027064665855811232919574614999118405590975546124662615392023179696090301839380641071581245394925393057636827422843491637554457928436520524176
c = 65553658155452064459040687299632299415295760116470555100400688788937893101658136830409082198753928673469636810831761104117535054304536941814523449491308187105740319826

r = (n // p )// q
e = 65537
assert r*p*q == n

# q = 3 * 78234041
phi = (r-1) * (p-1) * (3-1) * (78234041 - 1)
d = gmpy2.invert(e,phi)
m = gmpy2.powmod(c,d,n)
print(long_to_bytes(m))
```

```
load("coppersmith.sage")
N = 14857387925078594782296815160632343246361073432459148990826882280149636079353743233970188012712079179396872746334143946166398665205889211414809061990804629906990919975

c = 14035143725862612299576867857272911865951893239411969382153274945929406881665641140566462510177132511558933111728871930062074990934496715765999564244916409345156132996
e = 5

#相差52位
m_start = 11239443406846515682004397310032293056196968050880696884154193656922259582646354037672076691689208477252910368708578177585615543361661522949580970926775441873111
m_end = 11239443406846515682004397310032293056196968050880696884154193656922259582646354037672076691689208477252910368708578177585615543361661522949580970926775441873118

step = 10000000000000000000000000000000000000000000000000

for m in range(m_start,m_end,step):
    try:
        ZmodN = Zmod(N)
        P.<x> = PolynomialRing(ZmodN)
        f = (m + x)^e - c
        dd = f.degree()
        beta = 1
        epsilon = beta / 7
        mm = ceil(beta**2 / (dd * epsilon))
        tt = floor(dd * mm * ((1/beta) - 1))
        XX = ceil(N**((beta**2/dd) - epsilon))
        roots = coppersmith_howgrave_univariate(f, N, beta, mm, tt, XX)
        print(bytes.fromhex(hex(m+roots[0])[2:]))
        break
    except:
        continue
```

Flag

- ***本文作者：** CTFHub*
- ***本文链接：** https://writeup.ctfhub.com/Challenge/2020/安洵杯/Crypto/dgy8FzDNxdavJ324FCTtjQ.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 # 2020 # Crypto # 安洵杯
easyaes
王牌特工