攻防世界 Crypto高手进阶区 4分题 equation-2

原创

思源湖的鱼 于 2020-12-16 13:20:22 发布 399 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 crypto rsa

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111248278

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的4分题

本篇是equation-2的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到一个flag流量包和一个mask图片

私钥编码的截图
只能看见最后5行

```
Os9mhOQRdqW2cwVrnNI72DLcAXpXUJ1HGwJBANWiJcDUGxZpnERxVw7s0913WXNtV4GqdxCzG0pG5EHThtoTRbyX0aqRP4U/hQ9tRoSoDmBn+3HPITsnbCy67VkCQBM4xZPTtUKM6Xi+16VTUnFVs9E4rqwIQCDAxn9UuVMBXlX2Cl0xOGUF4C5hItrX2woF7LVS5EizR63CyRcPovMCQQDVyNbcWD7N88MhZjujKuSrHJot7WcCaRmTGEIJ6TkU8NWt9BVjR4jVkZ2EqNd0KZWdQPukeynPcLlDEkIXyaQx
```

查了查
OPENSSL中RSA私钥文件（PEM格式）

```
RSAPrivateKey ::= SEQUENCE {
  version           Version,
  modulus           INTEGER,  -- n
  publicExponent    INTEGER,  -- e
  privateExponent   INTEGER,  -- d
  prime1            INTEGER,  -- p
  prime2            INTEGER,  -- q
  exponent1         INTEGER,  -- d mod (p-1)
  exponent2         INTEGER,  -- d mod (q-1)
  coefficient       INTEGER,  -- (inverse of q) mod p
  otherPrimeInfos   OtherPrimeInfos OPTIONAL
}
```

把上面的base64解码

```
3A CF 66 84 E4 11 76 A5  B6 73 05 6B 9C D2 3B D8   | :.f...v..s.k..;.
32 DC 01 7A 57 50 9D 47  1B 02 41 00 D5 A2 25 C0   | 2..zWP.G..A...%.
D4 1B 16 69 9C 44 71 57  0E EC D3 DD 77 59 73 6D   | ...i.DqW....wYsm
57 81 AA 77 10 B3 1B 4A  46 E4 41 D3 86 DA 13 45   | W..w...JF.A....E
BC 97 D1 AA 91 3F 85 3F  85 0F 6D 46 84 A8 0E 60   | .....?.?..mF...`
67 FB 71 CF 21 3B 27 6C  2C BA ED 59 02 40 13 38   | g.q.!;'l,..Y.@.8
C5 93 D3 B5 42 8C E9 78  BE D7 A5 53 52 71 55 B3   | ....B..x...SRqU.
D1 38 AE AC 08 40 20 C0  C6 7F 54 B9 53 01 5E 55   | .8...@ .. T.S.^U
F6 0A 5D 31 38 65 05 E0  2E 61 22 DA D7 DB 0A 05   | ..]18e...a".....
EC B5 52 E4 48 B3 47 AD  C2 C9 17 0F A2 F3 02 41   | ..R.H.G........A
00 D5 C8 D6 DC 58 3E CD  F3 C3 21 66 3B A3 2A E4   | .....X>...!f;.*.
AB 1C 9A 2D ED 67 02 69  19 93 18 42 09 E9 39 14   | ...-.g.i...B..9.
F0 D5 AD F4 15 63 47 88  D5 91 9D 84 A8 D7 74 29   | .....cG.......t)
95 9D 40 FB A4 7B 29 CF  70 B9 43 12 42 17 C9 A4   | ..@..{).p.C.B...
31                                                 | 1
```

然后找到三个0241标签头

于是得到最后三个值

- d mod (p-1)=x1

```
00d5a225c0d41b16699c4471570eecd3dd7759736d5781aa7710b31b4a46e441d386da1345bc97d1aa913f853f850f6d4684a80e6067fb71cf213b276c2cbaed59
```

- d mod (q-1)=x2

```
1338c593d3b5428ce978bed7a553527155b3d138aeac084020c0c67f54b953015e55f60a5d31386505e02e6122dad7db0a05ecb552e448b347adc2c9170fa2f3
```

- (q -1) mod p

```
00d5c8d6dc583ecdf3c321663ba32ae4ab1c9a2ded6702691993184209e93914f0d5adf415634788d5919d84a8d77429959d40fba47b29cf70b943124217c9a431
```

根据这三个值
推测p、q、e

```
d·e≡1 mod (p-1)(q-1)
则有d·e≡1 mod (p-1)与d·e≡1 mod (q-1)
x1·e≡1 mod (p-1) , x2·e≡1 mod (q-1)
(p-1)|(x1e-1)
(q-1)|(x2e-1)
记x1·e-1=r1·(p-1);
由于x1=d mod (p-1)，则x1<(p-1);
几乎可以看做x1·e=r1·(p-1)
必有r1<e
同理r2<e
故e取65537
```

于是有脚本

```
import gmpy2
import rsa
from Crypto.Util.number import isPrime

x1="0xd5a225c0d41b16699c4471570eecd3dd7759736d5781aa7710b31b4a46e441d386da1345bc97d1aa913f853f850f6d4684a80e6067fb71cf213b276c2cbaed59"
x2="0x1338c593d3b5428ce978bed7a553527155b3d138aeac084020c0c67f54b953015e55f60a5d31386505e02e6122dad7db0a05ecb552e448b347adc2c9170fa2f3"
x3="0xd5c8d6dc583ecdf3c321663ba32ae4ab1c9a2ded6702691993184209e93914f0d5adf415634788d5919d84a8d77429959d40fba47b29cf70b943124217c9a431"
x1=int(x1,16)
x2=int(x2,16)
x3=int(x3,16)

def genKey(X1,X2):
    e=65537
    N1=X1*e-1
    N2=X2*e-1
    print(N1)
    for r in range(e):
        if N1%(e-r)==0:
            p=int(N1//(e-r)+1)
            if isPrime(p)==1:
                print("r1=",r)
                break
    for r in range(e):
        if N2%(e-r)==0:
            q=int(N2//(e-r)+1)
            if isPrime(q):
                print("r2=",r)
                break
    n=p*q
    phi=(p-1)*(q-1)
    d = int(gmpy2.invert(e, phi))
    privatekey = rsa.PrivateKey(n, e, d, p, q)
    with open("flag.enc", "rb") as f:
        print(rsa.decrypt(f.read(), privatekey).decode())
genKey(x1,x2)
```

得到flag：`0ctf{Keep_ca1m_and_s01ve_the_RSA_Eeeequati0n!!!}`

结语

RSA的理解要加深