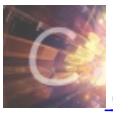
CRYPTO [61dctf]cry Writeup（RSA已知p的高位攻击）

原创

龙雪 于 2020-05-09 00:05:42 发布 2266 收藏 7

分类专栏： CTF 文章标签： 安全 经验分享

本文链接：https://blog.csdn.net/lostnerv/article/details/106009127



☑ *边学边做的大龄小白写了第一篇wp -.-*

[61dctf]cry

题目来源：https://www.jarvisoj.com/challenges

> Coppersmith攻击:已知p的高位攻击

- 关键点：用SageMath 恢复RSA完整的p

题目给了源码，其中print如下信息：

```
    print "====welcome to cry system===="
    (p,q,n,e,d)=rsa_gen()
    print "give you the public key:"
    print "n:"+hex(n).replace("L","")
    print "e:"+hex(e).replace("L","")
    try:
        c=int(raw_input("give me the crypted message in hex:")[2:].strip(),16)
        m=pow(c,d,n)
    except:
        print "wrong input"
    print "your message is",num2str(m)

    flag=open("pathtoflag","r").read().strip()
    aes_key=urandom(16)
    iv=urandom(16)
    cf=aes_cbc_encode(aes_key,iv,pad16(flag))
    ck=pow(str2num(aes_key),e,n)
    civ = pow(str2num(iv), e, n)
    print "encrypted flag:"+cf.encode("base64")+'#'+hex(ck).replace("L","")+'#'+hex(civ).replace("L","")+'#'+hex
(p).replace("L","")[2:182]+"##"
```

1. nc连上服务，根据提供的n、e，随意写个密文给服务器

```
    hex_m=str_m.encode("hex")
    c=pow(int(hex_m,16),e,n)
    print 'hex_c='+str(hex(c)).replace("L","")
```

回馈最终如下：

```
    encrypted flag:NkZJvVmju7Th59PChLXIT/c93tuE40SakEOywIPcH+c=
    #0x13f28958b67f35329ab7aee3737d8e3d4bdbaceed6395c944afc4d4dee871926fb17782868614787e1941bcccca1add9f80b2e65a
f88f9e220d099aa59966b22843167d7603ce7519cf6e90ab39d7e1ac4b5b24ed56c2e68af84f5b2775abbe950616c912bb5817dfc0f15518
a2eec266f99f11806912cbe8009fc40bc9d5a2b471f75fbdb44a90e640c73e3be8b17402b3b6a483aec8daa2c5a648a8d83f7c8288d878de
3436f04681ade0bf4459f4b77543cf104b161b761af7f375507f106f5e8ea170681e732af9f89f5299255f66f29cfa4cd8a1ad7d1114242b
3e53f18d4443bef3304a46182bf6039f514f53920415ea70184c52a82bd1d5f5e4496c4
    #0x1360e06b5e94fd1beec702b30593650c92c2d60819d1b206b02e2978742ed675001dcba874a6d15036b3d6355ff78ebe9f8f5a540
69a1e0afe11a089ca728954a38a372ee01abefea6197e24d91a6b21a98f3ea2f029d6ad23712cb0a1ada0bc70bc6e01e5ce3e7105a0b30e3
5fe898494514c726ea05d391542cd7cddd1d3cb191a5a90fe617cb9361660baaa7ac5bc72352dd3a5fd9c4b5a16e5a1496faedf9eebfab97
8df7799f7dc5208ddeddb8b071a540617df9ee037abbef5c8c53fc4c3a53fa6dd0834fb980e1138452e6b0e3db85d526b386b5e96e201619
6d8ffb9336c3b44b65deb039b0cb05930febb4ea1a82ede22ade1a0e59c607c08714196
    #960da3751599d2cae3b4495115fe18333e9d7163963bd7fa120faf80eb6322815901743301865f09cd4966cab28f9067c0782eef385
dca02636c14e54dffb07ffc348f2271c6d12f0382d4a71859df6d5cc57842b2b3000a1fe9##
```

给了180位16进制的p

2. 由源码 p = genprime(1024) 知p长1024，用Sage脚本，得10进制p

```
    n=xxxxxxxxx
    p=xxxxxxxxx

    pbits = 1024
    kbits = pbits-p.nbits()
    p=p<<kbits
    print "upper %d bits (of %d bits) is given" % (pbits-kbits, pbits)
    PR.<x> = PolynomialRing(Zmod(n))
    f = x + p
    x0 = f.small_roots(X=2^kbits, beta=0.4)[0]  # find root < 2^kbits with factor >= n^0.4
    print p+int(x0)
```

3. 源码给了好多函数可以直接利用，求d，解aes_key、iv出flag

```
    q =n/p
    d = primefac.modinv(e,(p-1)*(q-1)) % ((p-1)*(q-1))

    iv_m = pow(c_iv, d, n)
    iv=num2str(iv_m)

    aes_key_m = pow(c_aes, d, n)
    aes_key= num2str(aes_key_m)

    flag=aes_cbc_decode(aes_key,iv,flag16)
    print flag
```

> 参考了其他人的文章：
> CTF中RSA的一些攻击思路
> 第三届强网杯之copperstudy
> rsa高位攻击 恢复p