攻防世界 Crypto cr3-what-is-this-encryption

原创

==Microsoft== 于 2022-03-12 18:38:10 发布 19 收藏

分类专栏： Crypto 文章标签： ctf 密码

本文链接：https://blog.csdn.net/MrTreebook/article/details/123447965

攻防世界 Crypto cr3-what-is-this-encryption

1.分析题目

题目描述：Fady同学以为你是菜鸟，不怕你看到他发的东西。他以明文形式将下面这些东西发给了他的朋友

p=0xa6055ec186de51800ddd6fcbf0192384ff42d707a55f57af4fcfb0d1dc7bd97055e8275cd4b78ec63c5d592f567c66393a061324aa2e6a8d8fc2a910cbee1ed9

q=0xfa0f9463ea0a93b929c099320d31c277e0b0dbc65b189ed76124f5a1218f5d91fd0102a4c8de11f28be5e4d0ae91ab319f4537e97ed74bc663e972a4a9119307

e=0x6d1fdab4ce3217b3fc32c9ed480a31d067fd57d93a9ab52b472dc393ab7852fbcb11abbebfd6aaae8032db1316dc22d3f7c3d631e24df13ef23d3b381a1c3e04abcc745d402ee3a031ac2718fae63b240837b4f657f29ca4702da9af22a3a019d68904a969ddb01bcf941df70af042f4fae5cbeb9c2151b324f387e525094c41

c=0x7fe1a4f743675d1987d25d38111fae0f78bbea6852cba5beda47db76d119a3efe24cb04b9449f53becd43b0b46e269826a983f832abb53b7a7e24a43ad15378344ed5c20f51e268186d24c76050c1e73647523bd5f91d9b6ad3e86bbf9126588b1dee21e6997372e36c3e74284734748891829665086e0dc523ed23c386bb520 他严重低估了我们的解密能力

- 看到p,q,e,c
- 想到RSA加密

（1）任意选取两个不同的大素数p和q计算乘积$n = pq, \varphi(n) = (p-1)(q-1)$ [5]；

（2）任意选取一个大整数e，满足$gcd(e, \varphi(n)) = 1$，整数e用做加密钥（注意：e的选取是很容易的，例如，所有大于p和q的素数都可用） [5]；

（3）确定的解密钥d，满足$(de) mod \varphi(n) = 1$，即$de = k\varphi(n) + 1, k \geq 1$是一个任意的整数；所以，若知道e和$\varphi(n)$，则很容易计算出d [5]；

（4）公开整数n和e，秘密保存d [5]；

（5）将明文m（m<n是一个整数）加密成密文c，加密算法为 [5]

$$c = E(m) = m^e mod n$$

（6）将密文c解密为明文m，解密算法为 [5]

$$m = D(c) = c^d mod n$$

- 先把p,q,e转成十进制，再根据公式求出n,d,m
- n=p*q
- φ(N) = (p-1)(q-1)
- e * d % φ(N) = 1（d是私钥，e是公钥）
- m＝c^ d mod n (m是明文）
  需要一个解码的脚本

2.exp

```
import libnum
from Crypto.Util.number import long_to_bytes

q = int("0xa6055ec186de51800ddd6fcbf0192384ff42d707a55f57af4fcfb0d1dc7bd97055e8275cd4b78ec63c5d592f567c66393a061324aa2e6a8d8fc2a910cbee1ed9",16)
p = int("0xfa0f9463ea0a93b929c099320d31c277e0b0dbc65b189ed76124f5a1218f5d91fd0102a4c8de11f28be5e4d0ae91ab319f4537e97ed74bc663e972a4a9119307",16)

e = int("0x6d1fdab4ce3217b3fc32c9ed480a31d067fd57d93a9ab52b472dc393ab7852fbcb11abbebfd6aaae8032db1316dc22d3f7c3d631e24df13ef23d3b381a1c3e04abcc745d402ee3a031ac2718fae63b240837b4f657f29ca4702da9af22a3a019d68904a969ddb01bcf941df70af042f4fae5cbeb9c2151b324f387e525094c41",16)

c = 0x7fe1a4f743675d1987d25d38111fae0f78bbea6852cba5beda47db76d119a3efe24cb04b9449f53becd43b0b46e269826a983f832abb53b7a7e24a43ad15378344ed5c20f51e268186d24c76050c1e73647523bd5f91d9b6ad3e86bbf9126588b1dee21e6997372e36c3e7428473474889182966508 6e0dc523ed23c386bb520

n = q*p

d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n)
string = long_to_bytes(m)
print(string)
```


C:\Users\17849\Desktop>python flag.py
b'ALEXCTF{RS4_I5_E55ENT1AL_TO_DO_BY_H4ND}'
C:\Users\17849\Desktop>

得到flag