攻防世界CRYPTO cr3-what-is-this-encryption writeup(待)

原创

Sprint#51264 于 2020-08-16 20:53:46 发布 589 收藏

分类专栏： CRYPTO

本文链接：https://blog.csdn.net/qq_45837896/article/details/108042392

RSA加密

根据题目所给的 pqec联想到密码学中学到的RSA加密算法

关于RSA：

（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]

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

题目中给出了p.q.e.c

那么很容易算出来φ(n),进而算出来d，然后得出c，可以跑一个脚本

```python
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)
```