关于rsa的总结1

原创

a3uRa 于 2018-04-14 09:29:51 发布 316 收藏

本文链接：https://blog.csdn.net/qq_41173457/article/details/79936854

ctf中的crypto项，关于rsa的考察是一类，来记录一下吧

首先介绍一下什么是公开密钥加密：公开密钥加密（英语：Public-key cryptography），也称为非对称加密（英语：asymmetric cryptography），是密码学的一种算法，它需要两个密钥，一个是公开密钥，另一个是私有密钥；一个用作加密的时候，另一个则用作解密。使用其中一个密钥把明文加密后所得的密文，只能用相对应的另一个密钥才能解密得到原本的明文；甚至连最初用来加密的密钥也不能用作解密。由于加密和解密需要两个不同的密钥，故被称为非对称加密；不同于加密和解密都使用同一个密钥的对称加密。虽然两个密钥在数学上相关，但如果知道了其中一个，并不能凭此计算出另外一个；因此其中一个可以公开，称为公钥，任意向外发布；不公开的密钥为私钥，必须由用户自行严格秘密保管，绝不通过任何途径向任何人提供，也不会透露给要通信的另一方，即使他被信任。

记一下相关的名词，知识点（cipher就是密文，c就是密文，n是两个大质数p、q的积，Modulus即为n，n的二进制表示时所占用的位数，就是所谓的密钥长度，公钥 （n,e）,私钥 (d,e)，欧拉函数，n=pq。只有将n因数分解，才能算出p和q。**加密要用公钥 (n,e)。解密要用私钥(n,d)。【pubkey.pem】是公钥文件，通过公钥文件可以得到e和n。【flag.enc】从文件名含有flag可以判断是加密后的密文。kali 》通过openssl对公钥文件【pubkey.pem】进行分解，使用命令【openssl rsa -pubin -text -modulus -in warmup -in pubkey.pem】，得到e= (0x)，Modulus即为n=。m为明文message。python的gmpy2模块。gmpy2.invert(e, (p-1)*(q-1))可求d。pow(c ,d ,n) 求m 明文。openssl。）**

关于**python的gmpy2模块，确实不好安装，不能像安装其他模块一样，pip install 模块名，的方式安装，linux和windows的gmpy2的安装还不一样，windows比linux好装些~，我的本机是win10的，反正我从kali虚拟机里第一遍没装成功，就放弃了，有空在搞吧，最后在本机win10的成功装上了。**

数学知识，不会，想学，但是，，，还是太懒惰了，寒假买的数学书，还没看多少，，哎~~

kali中的openssl命令，这也是一个点，有空在百度谷歌，学习学习，目前做题就积累了一个命令就是**openssl rsa -pubin -text -modulus -in warmup -in pubkey.pem**

~~~RSA攻击之共模攻击

链接：http://www.bystudent.com/?p=236

https://www.ichunqiu.com/writeup/detail/603

http://iromise.com/2016/11/29/RSA%E5%85%B1%E6%A8%A1%E6%94%BB%E5%87%BB/

以上三位大佬讲的非常详细了

共模即n相同，使用两个不同的e加密同一个明文m，