MediumRSA-writeup

原创

网安小小白 已于 2022-03-18 21:10:51 修改 3211 收藏

分类专栏： CTF 文章标签： 信息安全 CTF writeup
于 2022-03-18 21:03:53 首次发布

MediumRSA

RSA基础

选取两个大素数。p,q计算

$n=$

计算$\phi(n)$

$\phi(n)=(p-1)($

选取一个随机数e,$gcd(e,\phi(n))=1$,其中 $1<$

计算e的逆元,使用拓展欧几里得算法。

$ed\equiv 1 mod \phi(n)$

其中e为公钥，d为私钥。

对密文m加密

$c=m^e mod n$

解密

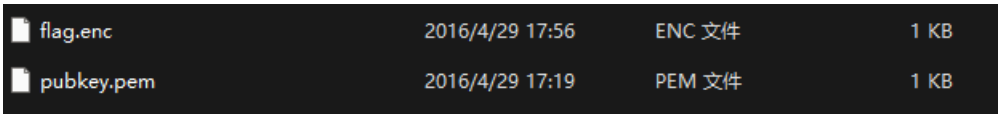
$m=c^d=m^{ed} mod n$

例题

1. 下载文件

mediumRSA.rar

下载下来解压获得两个文件。



其中，flag.enc是加密后的密文，pubkey.pem是公钥。通过openssl工具可以读取公钥文件

2. 在linux环境下（kali，Ubuntu）输入以下命令：

```
openssl rsa -pubin -text -modulus -in warmup -in pubkey.pem
```

```
rao@Mr-Rao:/mnt/d/Download/mediumRSA$ openssl rsa -pubin -text -modulus -in warmup -in pubkey.pem
RSA Public-Key: (256 bit)
Modulus:
    00:c2:63:6a:e5:c3:d8:e4:3f:fb:97:ab:09:02:8f:
    1a:ac:6c:0b:f6:cd:3d:70:eb:ca:28:1b:ff:e9:7f:
    be:30:dd
Exponent: 65537 (0x10001)
Modulus=C2636AE5C3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD
writing RSA key
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMJjauXD2OQ/+5erCQKPGqxsC/bNPXDr
yigb/+1/vjDdAgMBAAE=
-----END PUBLIC KEY-----
```

其中

modulus是模数，

exponent是e，

3. 分解n

因为只给出了n，和e。其中e无从下手，所以只能分解n，RSA的困难问题就是大整数的分解。只要能分解n，即可获得私钥。

可以通过在线网站分解， http://www.factordb.com/index.php

用Python 输出n的10进制的值，输入到网站得到分解结果

		Result:
status (?)	digits	number
FF	77 (show)	8792434826...61<77> = 2751278603513489281732851743815811522 99<39> · 3195763168144789498705901641930480412 39<39>

得到p和q

```
n = 0xC2636AE5C3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD
e = 0x10001
p = 275127860351348928173285174381581152299
q = 319576316814478949870590164193048041239
```

计算phi_n,

```
phi_n = (p - 1) * (q - 1)  # 计算phi_n
```

结算e的逆元，可以通过扩展欧几里得算法，或者直接调用库。

```
d = int(gmpy2.invert(e, phi_n))  # 库函数返回结果不是int，后面需要int类型，转为int类型。
```

构造私钥

```
private = rsa.PrivateKey(n, e, d, p, q)  # 构造私钥
```

打开文件并解密。

```
with open("flag.enc", 'rb') as f:  # 读取文件
    print(rsa.decrypt(f.read(), private).decode())  # 解密，解码
```

得到结果

完整代码

```
import gmpy2
import rsa

n = 0xC2636AE5C3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD
e = 0x10001
p = 275127860351348928173285174381581152299
q = 319576316814478949870590164193048041239

phi_n = (p - 1) * (q - 1)  # 计算phi_n
d = int(gmpy2.invert(e, phi_n))  # 转为int类型。

private = rsa.PrivateKey(n, e, d, p, q)  # 构造私钥

with open("flag.enc", 'rb') as f:  # 读取文件
    print(rsa.decrypt(f.read(), private).decode())  # 解密，解码
```

Author: 41–21032202031-饶刚; Time:2022-3-18