

## Week4-Theffth

写在前面：灰常灰常感谢协会的各位学长们提供的这么好而且难得的入门向学习机会，这四周虽然没有做出什么题目，但是相对自身而言还是收获颇丰，还有学长们非常用心的wp，提供了很多的学习方向，再次感谢各位大神！

### Misc:

#### 1.暗藏玄机

打开题目，看到两张图片，更悲伤了...，怎么就开学了（哭），第一想法stegsolve-image combiner，没有什么发现，binwalk再分离一下，还是没什么发现，最后查到相同的双图类型一般都是盲水印，于是跑脚本：

```
root@kali:~# python bwm.py decode 1.png 2.png out.png
image<1.png> + image(encoded)<2.png> -> watermark<out.png>
root@kali:~#
```



得到flag:hgame{h1de\_in\_THE\_p1Cture}

### Crypto:

#### 1.easy\_rsa

打开题目，观察题目特点，是m,N相同，用不同私钥加密的一类，于是考虑共模攻击，查到wiki上面的解法：

```
import gmpy2
n =
0x9439682bf1b4ab48c43c524778c579cc844b60872275725c1dc893b5bcb358b9f136e4dab2a06318bb0c80e
202a14bc54ea334519bec023934e01e9378abf329893f3870979e9f2f2be8fff4df931216a77007a2509f49f6
97bf286285e97fac5dc6e4a164b5c2cc430887b18136437ba67777bda05aafdeaf918221c812b4c7d1665238f
84ab0fab7a77fcae92a0596e58343be7a8e6e75a5017c63a67eb11964970659cd6110e9ec6502288e9e443d86
229ef2364dfecb63e2d90993a75356854eb874797340eece1b19974e86bee07019610467d44ec595e04af02b5
74a97fa98bdb2e779871c804219cab715f4a80fef7f8fb52251d86077560b39c1c2a1
e1 = 0x33240

e2 = 0x3e4f

message1 =
0x7c7f315a3ebbe305c1ad8bd2f73b1bb8e300912b6b8ba1b331ac2419d3da5a9a605fd62915c11f8921c4505
25d2efda7d48f1e503041498f4f0676760b43c770ff2968bd942c7ef95e401dd7facbd4e5404a0ed3ad96ae50
5f87c4e12439a2da636f047d84b1256c0e363f63373732cbaf24bda22d931d001dcca124f5a19f9e28608ebd9
0161e728b782eb67deeba4cc81b6df4e7ee29a156f51a0e5148618c6e81c31a91036c982debd1897e6f3c1e5e
248789c933a4bf30d0721a18ab8708d827858b77c1a020764550a7fe2ebd48b6848d9c4d211fd853b7a02a859
fa0c72160675d832c94e0e43355363a2166b3d41b8137100c18841e34ff52786867d

message2 =
0xf3a8b9b739196ba270c8896bd3806e9907fca2592d28385ef24afadc2a408b7942214dad5b9e14808ab988f
b15fbd93e725edcc0509ab0dd1656557019ae93c38031d2a7c84895ee3da1150eda04cd2815ee3debaa7c2651
b62639f785f6cabf83f93bf3cce7778ab369631ea6145438c3cd4d93d6f2759be3cc187651a33b3cc4c3b4776
04477143c32dfff62461fd9f8aa879257489bbf977417ce0f8e89e3f2464475624aafe57dd9ea60339793c
69b53ca71d745d626f45e6a7beb9fcb9d1a259433d36139345b7bb4f392e78f1b5be0d2c56ad50767ee851fa
c670946356b3c05d0605bf243b89c7e683cc75030b71633632fb95c84075201352d6

# s & t
gcd, s, t = gmpy2.gcdext(e1, e2)
if s < 0:
    s = -s
    message1 = gmpy2.invert(message1, n)
if t < 0:
    t = -t
    message2 = gmpy2.invert(message2, n)
plain = gmpy2.powmod(message1, s, n) * gmpy2.powmod(message2, t, n) % n
print plain
```

解出答案明显比17位长的多，emmmm，然后回想了一下上周的套路，注意到e1,e2必须互质，于是验证了一把：

number

$$209472 = 2^6 \cdot 3 \cdot 1091$$

number

$$15951 = 3 \cdot 13 \cdot 409$$

发现公因子3，因此改 $e_1=69824$ ， $e_2=5317$ ，得到：

```
C:\WINDOWS\SYSTEM32\cmd.exe
211655262573966881062823795220179644607412162371069
e
:
-----
(program exited with code: 0)
请按任意键继续. . .
```

这个答案和 $e$ 不变时相同，暂时还不是很清楚为什么，但是猜想 $e$ 的公因子不影响

当攻击者截获  $c_1$  和  $c_2$  后，就可以恢复出明文。用扩展欧几里得算法求出  $re_1 + se_2 = 1 \bmod n$  的两个整数  $r$  和  $s$ ，由此可得：

$$\begin{aligned} c_1^r c_2^s &\equiv m^{re_1} m^{se_2} \bmod n \\ &\equiv m^{(re_1 + se_2)} \bmod n \\ &\equiv m \bmod n \end{aligned}$$

$r, s$ 的求解，但此时的明文需要开三次方：

```
C:\WINDOWS\SYSTEM32\cmd.exe
211655262573966881062823795220179644607412162371069
(mpz(59594981651654789L), True)
-----
(program exited with code: 0)
请按任意键继续. . .
```

得到十七位明文，即：hgame{59594981651654789}