misc
卡中毒
crypto
Multi Prime RSA
RSA Attack 3
Block Cipher

misc

卡中毒

使用取证大师分析raw文件，在桌面上看到flag.zip;flag.txt;flag.wannaren文件，可知flag文件被勒索病毒感染。使用火绒的WannaRen解密软件解密，得到新佛曰密码。使用在线网站解密后可得到flag。

crypto

Multi Prime RSA

多素数/相同素数RSA解密。需要注意如下性质：

定理2：取值为素数方幂的欧拉函数

设p是素数，则对于任一正整数r，有

$$\varphi(p^r) = p^{r-1}(p-1).$$

证 明

由于互素的整数个数不易计算，下面从不互素的整数出发进行证明。

设集合$\Omega_{p^r} = \{1, 2, \cdots, p^r\}$，其中与$p^r$不互素的整数的个数即所求。对$\forall a \in \Omega_{p^r}$，利用互素整数的性质3推广，有$(a, p) = 1 = (a, p^r) = 1$。若$(a, p) \neq 1$，则$p \mid a$，从而$(a, p^r) \neq 1$，因此

$$\begin{aligned}(a, p^r) \neq 1 &\iff (a, p) \neq 1 \iff p \mid a \\ &\iff a = p, 2p, \cdots, p^{r-1}p,\end{aligned}$$

从而Ω_{p^r}中与p^r中不互素的整数的个数为p^{r-1}，于是得到

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1). \qquad \square$$

RSA Attack 3

低解密指数攻击。代码套一下就出来了

Block Cipher

分析后写出代码如下：

```
import operator

import re

from functools import reduce

``

def xor(a, b):

 assert len(a) == len(b)

 return bytes(map(operator.xor, a, b))

``

print(xor(xor(b'Up\x14\x98r\x14%\xb9',b'O\xff\xcd\xc3\x8b\\T\x8b'),b'\r\xe8\xb86\x9c33^'))
```

相继套入得到flag。