

小塔WEEK2眼泪汪汪的wp

crypto

RSA Attack

看了一下附件发现明显是给了 n 求 p, q 的问题

于是用yafu将 n 分解为 p, q

```
D:\yafu-1.34>yafu-x64.exe
factor(700612512827159827368074182577656505408114629807)

fac: factoring 700612512827159827368074182577656505408114629807
fac: using pretesting plan: normal
fac: no tune info: using qs/gnfs crossover of 95 digits

starting SIQS on c48: 700612512827159827368074182577656505408114629807

==== sieving in progress (1 thread):    1232 relations needed ====
====                               Press ctrl-c to abort and save state                               ====

SIQS elapsed time = 0.0409 seconds.
Total factoring time = 0.0463 seconds

***factors found***

P24 = 715800347513314032483037
P24 = 978782023871716954857211

ans = 1
```

然后把 p, q 代入写一个代码:

```
import libnum
from Crypto.Util.number import long_to_bytes
e = 65537
n = 700612512827159827368074182577656505408114629807
c = 122622425510870177715177368049049966519567512708
q = 715800347513314032483037
p = 978782023871716954857211
d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n)
string = long_to_bytes(m)
print(string)
```

解出来就得到了flag

Chinese Character Encryption

用记事本打开附件里的enc文件，得到汉字

题目给了四个hint:

Hint1: 该题的加密方式只与汉字的拼音有关，汉字拼音以pypinyin包的查询结果为准，一个汉字只唯一表示一个字母，一个字母可以加密成多个不同的汉字。

Hint2: 本加密方法是基于ASCII编码的，理论上可表示所有的ASCII字符。

Hint3: <https://baike.baidu.com/item/拼音声调>

Hint4: 声调在本加密中单独起作用，即声调在哪个字母上不影响加密结果。(轻声不做任何处理)

根据hint1里说加密和拼音有关的提示，使用pypinyin库，得到每行的拼音

(且根据hint3和hint4 将音调统一换成数字放在拼音末尾，如：['xing2'], ['dan4'])

因为hint2里说加密基于ASCII编码，且每行均代表flag，就先将每行第一个拼音拿出来单独研究

发现规律：

每行对应位置上，在拼音个数相同的情况下，拼音中每个字母的ASCII值加上音调值相同

且轻声不能当做音调值为0或者5，而是要单独做处理。

(很遗憾我没有找到全部的规律，只是判断出与模运算有关，所以只能先用偏移量做)

写一个笨蛋才会用的代码：

```
list=[['ying',1], ['quan',2]...]#省略处理成嵌套数组的数据

for i in range(47):
    a = list[i][0]
    b = list[i][1]
    if len(a) == 3:
        c = chr(ord(a[0])+ord(a[1])+ord(a[2])+b-312+ord('h'))
    elif len(a) == 4:
        c = chr(ord(a[0])+ord(a[1])+ord(a[2])+ord(a[3])+b-440+ord('h'))
    elif len(a) == 5:
        c = chr(ord(a[0])+ord(a[1])+ord(a[2])+ord(a[3])+ord(a[4])+b-551+ord('w'))
    else : c = a #将无法处理的数据先保留，然后手动用偏移量解决
    print(c)
```

运行完成得到flag

RSA Attack2

从附件可以看出题目把flag分为三部分加密

task1: 已知e, n1, c1, n2, c2

求出n1与n2的最大公因数即为q，之后就可以得到p,r和d，从而求解m

```
import gmpy2
import binascii
e = 65537
n1 = ...
c1 = ...
n2 = ...
c2 = ...
```

```
#上省略文件路径和数据
p = gmpy2.gcd(n1,n2)
q = n1 // p
s = (p-1)*(q-1)

d = gmpy2.invert(e,s)
m = gmpy2.powmod(c1,d,n1)
print(binascii.unhexlify(hex(m)[2:]))
```

task2: 已知e(很小), n(很大), c

考虑低加密指数攻击

```
import gmpy2
import os
from functools import reduce
from Crypto.Util.number import long_to_bytes
def func(items):
    N = reduce(lambda x, y: x * y, (i[1] for i in items))
    result = 0
    for a, n in items:
        m = N // n
        d, r, s = gmpy2.gcdext(n, m)
        if d != 1:
            raise Exception("Input not pairwise co-prime")
        result += a * s * m
    return result % N, N
e = 7
n = []
c = []
##省略文件路径和数据
data = list(zip(c, n))
x, n = func(data)
m = gmpy2.iroot(gmpy2.mpz(x), e)[0].digits()
string = long_to_bytes(m)
print(string)
```

task3: 已知n,e1,e2,c1,c2

RSA的共模攻击, 可以在不知道d1,d2的情况下, 解出m

```
from gmpy2 import invert as invert
from gmpy2 import gcdext as gcdext
import libnum

n = ...
c1 = ...
c2 = ...
e1 = 2519901323
e2 = 3676335737
s = gcdext(e1, e2)
s1 = s[1]
s2 = -s[2]

c2 = invert(c2, n)
m = (pow(c1,s1,n) * pow(c2, s2, n)) % n
print (m)
```

misc

一张怪怪的名片

附件得到一张含有二维码的图片



将里面的二维码用ps切出来，然后拼起来，但是发现扫不出来：

以为是自己拼的技术不好，所以自己又画了一个：

发现还是扫不出来。根据补充的hint的提示发现该二维码损坏，使用QRazyBox得到信息：

```
[0100] [00011110]
[011010000110111010001101110100011011100000110111001100100111010001001010110010011111101101
Mode Indicator : 8-bit Mode (0100)
Character Count Indicator : 30
Decoded data : https://homdginc~.homeboy.com/k5
```

```
[0100] [11101100] [000100011111110101000000010001]
Mode Indicator : 8-bit Mode (0100)
Character Count Indicator : 236
Decoded data :  
```

Final Decoded string : <https://homdginc~.homeboy.com/k5>  

"https"提示这个应该是一个网站，于是用后面的关键字搜索一下：

homeboyc博客



网页

图片

视频

学术

词典

地图

7 条结果

时间不限

 **博客重新上线**

<https://homeboyc.cn/blog/博客重新上线>

2021-1-5 · **博客** 关于 友链 闽ICP备2021002495号 闽公网安备 35030302354429号 **博客重新上线**

Jan 5, 2021 One minute read 恢复 把之前的wordpress**博客**重启了一下，挑选了一些好的文章搬...

 **宅男的天台**

<https://homeboyc.cn>

2021-2-6 · 宅男的天台 asjd的**博客** Nov 3, 2021 阳光长跑小程序逆向 Aug 25, 2021 Scrapy对抗 Cloudflare反爬5秒盾 Aug 12, 2021 易班登录流程逆向小记 Aug 1, 2021 快速照片扫描方法记录 ...

[易班登录流程逆向小记](#) · [完成OpenCV分类器训练的最简单方法](#) · [laosb的春节红包打开方式](#)

有点东西，点进去康康 通过友情链接找到包含“鸿贵安”信息的博客，


博客 关于 友链

友链

下面是Atom的小伙伴们

鸿贵安的自留地

得到flag提示：



鸿贵安的自留地

我是谁？没有绝对安全的系统！

© 鸿贵安 2022

Home About Friend Link

靠嫩娘 盗号死XX

麻了，居然被盗号了。评论： 露尔： 都说了别用弱密码，就是不听。还有，不许把我信息塞到你的密码里！！

Tue, Jan 25, 2022

FL4G

宝，想你，呜呜。宝，下面的fl4g的密码你应该知道的，我就不说了噢噢。对了，宝，你可以用这个网站解密 CyberChef。 我先用“Derive PBKDF2 key”把密码转成了key（salt=1），然后交给AES加密模块用ECB模式加密了（别忘了base64）。The following text is the ciphertext of fl4g after AES-128 encryption.

Sun, Jan 23, 2022

HAPPY BIRTHDAY

宝！19岁生日快乐！关于礼物 关于小猫咪 这是一个钧瓷猫猫，我感觉挺可爱的，而且钧瓷特色是一窑万色，同一批瓷器烧出来的颜色都不会完全相同，每一只猫猫都是独一无二的。猫猫身上的裂纹也是钧瓷的特色，平时多给猫猫用开水冲冲，能让猫猫的裂纹更丰富（大概就是利用釉料的收缩率和胚的收缩率不同做到的）关于小恐龙游戏机 本来都已经做好了，打算送的是一块绝版的开发板，但是很奇怪的给丢了，也不知道是丢在了科协的实验室还是机电助手的办公室。最后重新买了一块开发板把程序烧写进去，也就是你收到的这一块。这块开发板带 esp8266和一块ssd1306的屏幕，如果你自己有兴趣，也可以拿这块开发板做一些其他好玩的东西。