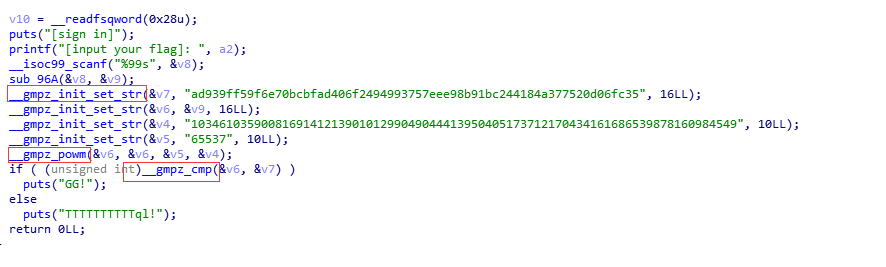
**题目分析**

拖进IDA后我们有注意到这几个函数。



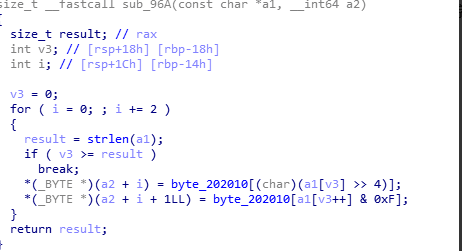
可以判断这是用了GMP大整数库。

我们查到了这两两个函数的功能：

把字符串初始化为gmp大整数：int mpz\_init\_set\_str(mpz\_t rop, char\*str, int base)

模幂运算rop=base^exp mod mod：void mpz\_powm (mpz\_t rop, mpz\_t base, mpz\_t exp, mpz\_t mod)

程序获取了我们的输入后传进了sub96A函数进行处理，sub96A函数功能是得到输入字符串的hex值字符串。



然后把输入的hex值字符串初始化成了大整数，最后进行了模幂运算，再将模幂运算得到的大整数与另一个初始化的大整数对比。

也就说只要满足这个等式就可以，其中a是输入字符串hex值初始化成的大整数：

(a ^ 65537)%103461035900816914121390101299049044413950405173712170434161686539878160984549

== 78510953323073667749065685964447569045476327122134491251061064910992472210485

**脚本**

from libnum import invmod  
  
p = 282164587459512124844245113950593348271  
q = 366669102002966856876605669837014229419  
n = p \* q  
#n = 103461035900816914121390101299049044413950405173712170434161686539878160984549  
assert n == p\*q  
e = 65537  
c = 78510953323073667749065685964447569045476327122134491251061064910992472210485  
phi = (p-1)\*(q-1)  
d = invmod(e, phi)  
#print pow(c, d, n)  
print hex(pow(c, d, n))[2:].rstrip('L').decode('hex')

flag为suctf{Pwn\_@\_hundred\_years}。