# CTF 常用python库

原创

rang# 于 2020-12-14 17:55:31 发布 930 收藏 4

分类专栏： python库 文章标签： python



本文链接：https://blog.csdn.net/weixin_45859850/article/details/111180937





## gmpy2库

```
import gmpy2

gmpy2.mpz(x)#初始化一个大整数x

gmpy2.mpfr(x)#初始化一个高精度浮点数x

C = gmpy2.powmod(M,e,n)#幂取模，结果是 C = (M^e) mod n

d = gmpy2.invert(e,phi) # 求逆元，de = 1 mod (p-1)*(q-1)

gmpy2.is_prime(n) # 判断n是不是素数

gmpy2.gcd(a,b) # 欧几里得算法

gmpy2.gcdext(a,b) # 扩展欧几里得算法

gmpy2.iroot(x,n) # x开n次根
```

## Crypto库

## sympy库

```
在这里插入代码片
```

## Z3库

```
from z3 import *
#使用z3对二元二次方程进行求解
s = Solver()
#定义两个变量
p,q = Ints("p q")
#添加方程
s.add(p*p+q*q == x1)
s.add(p-q == x2)
s.add(p>0)
arr=[]
#校验是否有解
if s.check()==sat:
  arr=s.model()
print(arr)
```

## hashlib库