

HGAME2023-writeup-Week4 by crumbling

[Crypto](#)

- [LLLCG](#)
-

Crypto

LLLCG

相对于输出的值，增量模 n 很小。

```
from Crypto.Util.number import *
from random import randint
from sage.all import next_prime
n = next_prime(2**360)
seed1=11376601256353152185503962572833792711262816547071400246285651162390432276
54756862152080704553915295597833918194897961244358284543325452196119976528044019
410771533996460493628849739976409844578782648330528014140288383
seed2=10896510524738352828273081283110658285613966633649112409729597889095153066
16863980465990986336276384903707375227394223034256042622812751981085694555292380
38866457344842006422913342167824060644151888704413267011559130185793503076927127
15993675813772474243280626352888321213313718894912395388422448776832449873890579
41199373965
m=seed2//seed1
print(long_to_bytes(m))
```