

## 已知

$p$ 、 $e$ 、 $c$

## 特点分析

$e=2$

则  $e$  与  $(p-1)$  不互素

直接考虑爆破，发现非常非常慢。说明一般情况下还是不要用爆破这种效率很低的操作（

于是采用 `sage` 在有限域进行开根

## 可能遇到的问题

$c$  是  $p$  的二次剩余， $c$  在模  $p$  意义下开根必然有一对解

其中一个是 `flag` 一个不是

挨个 `long_to_bytes` 看看哪个能得到人类可识别的字符串即可