

Signin

Description

简单的签到

Solution

pad函数对42bytes的flag进行填充\x00操作填充到127bytes，即对flag进行85*8=680bit的移位

$$\begin{aligned}(2^{680} * flag)^3 &= c \mod p \\ flag^3 &= c * 2^{680*3*-1}\end{aligned}$$

然后考虑到flag为42*8=336位，p为1024位直接开三次方