Crackme4 解题思路

考察知识点：数学
代码处理：控制流扁平化混淆，指令替换混淆，虚假控制流混淆
难度：非常难
Flag: flag{47,73,81,142,155,183,185,198,234}

叹息之墙 解题思路

逆向可知 输入的数字进入了 4 个流程

1）判断顺序 判断是否越界（1106）

2）依据这些数作为下标 从指定数组（命名为 elist）取出若干个 32 位无符号整型 并求和

3）以和作为指数 以“NCTF”作为底数 以 0xFFFFD307 作为模数 求模幂

4）判断模幂结果是否是 “2018”，如果是 则显示 flag 正确

分析：

1）有用信息有 2 个数：数组长度 1106 和 模数 0xFFFFD307，其它信息均与解题方法无直接关系

2）已知模数后 可求解阶 可分解阶

3）分解阶后 会发现 有 6 个素因子 且全是小素因子（随机情况下 不会全是小素因子 所以可以断定 这是出题者有意为之）

4）而且 所有素因子之和的 2 倍正好是 1106

因此可以断定 对数组访问的下标 是模幂运算的指数对 6 个素因子分别的余数（或者余数的一一映射）且一次映射 2 个数

求解：

根据“NCTF”和“2018”求解最小指数解 是容易的（时间小于 1 秒）

但 只要从 elist 中挑出的所有数字之和 与最小指数解 对阶同余 就算解题正确（此题有多解）

由于从 elist 中挑出的每 2 个数会针对阶的某一个素因子 因此 这 2 个数一定要保证与其它素因子所构成的基底正交 否则此题将难解

也就是说 这 2 个数必须不会影响模幂结果在以其它素因子为阶的子群上的计算结果 必须在其它素因子所对应的乘法子群上表现为 1

这 2 个数是如何结合的呢？

答案只能是：相加

因为这些从 elist 中挑出来的数都是相加的

编程 对 elist 里的每个数进行搜索 找到其配对 使得：GCD（配对的 2 个数之和，

大群阶 ）= 大群阶/某个小素因子

并针对这个小素因子 求配对和的余数（其结果正好能遍历所有可能的余数。这也证实了上述分析的正确性）

剩下的工作就简单了

根据最小指数解对每个小素因子的余数 选择合适的配对 一共从 elist 中挑出 6 个配对 排序 按照格式构造出 flag 即可