十分感谢你能来参加 imToken 的面试

考核说明

- 以下题目旨在考核您的实际代码编写能力，请按上线代码的标准完成以下题目。
- 在考核工程中可以使用 IDE 提醒，搜索 API 文档。但不允许直接搜索完整的解题内容和使用AI辅助工具编写代码
- 考核时间为2小时，但如果在规定时间内无法完成可以放弃部分题目或者使用注释补充自己的想法。但高质量的可运行的代码可获得最高分数
- 请使用 C++ 或者 Rust 作答

考核题目

计算题

题目1

在 p = 11579208923731619542357098500868790785326998466564056403945758400790883467166 3 有限域里计算 3749599548309381253082912034406892107395077837427705085763584522618399088953 2 的 3627388497631735087689293345018161343866446216090268213594136894568216387277 1 次方

题目2

在 Secp256k1 上存在 P1 (36034668029310999675425029227919426304128362788024891102120850317866231552679, 81120990977494636963407451456021843404486499021598452981689548730055179196713), P2 (17178020516540951919986460933710490672232047574774824837208169858689311129064, 71957217096292920627957410906773462576199313707110833846387209016083557649656)

a) 求 P1 的负数

b) 求 P1 + P2

c) 求 P1 *

11272252273680242517107462011973934283701666271392689921748647863305630666941 8

加解密

以下内容是一个加密文件，加密逻辑如下：

1. `Insecure Pa55w0rd`字符串转成bytes数组 passwordBytes（password.getBytes()）
2. passwordBytes 经过PBKDF2 KDF算法派生并取前16 bytes 作为 derivedKey ， 派生参数见下述配置
3. derviedKey 作为私钥配合 cipherparams.iv 作为salt，使用 "aes-128-ctr" 将密文加密

请根据上述内容将 ciphertext 解密出来

```
{
    "ciphertext":
"b88b6c828d266b6cc5659671ba650f36dbfb31d78bfdd3a3782afc944b1a4663",
    "mac": "96fc23e33077ff61194bc1daf7ed18200b0a018c6d079b3644e9d36477e877ad",
    "cipher": "aes-128-ctr",
    "cipherparams": {
      "iv": "5031a85957e7fdb47d6ece9d95adbc36"
    },
    "kdf": "pbkdf2",
    "kdfparams": {
      "dklen": 32,
      "c": 10240,
      "prf": "hmac-sha256",
      "salt": "fd9d44b2e8dee6ac977525028559171f84c3b796dc8a3b81527396b1222f46c9"
    }
  }
```

基础算法

题目1

假设有一个包含 n 个没有重复值的正整数数组full_array。有k个人，可以自由选择full_array中的数字，每个数字可以被多个人同时选择。每个人都想尽力让自己的累加和足够小，但是任何两个人的方案不能完全一致。
请设计一个算法，保证任何两个人的方案不能完全一致的情况下，k个人总的累加和，最小是多少。
注:n<=100000，k<=1000

题目2

一个字符串s，表示仓库的墙 与 货物，其中 | 表示墙, * 表示货物。
给定一个起始下标start和一个终止下标end，
找出子串中 被墙包裹的货物数量

比如

```
s = "|**|**|*"
start = 1, end = 7
```

start和end截出的子串是 `"**|**|*"`
被 | 包裹的 * 有两个，所以返回2

现在给定一系列的start，startIndices[]，和对应一系列的end ,endIndices[]
返回每一对[start,end]的截出来的货物数量

数据规模：
字符串s长度<=10^5
startIndices长度 == endIndices长度 <=10^5