大学最关键的就是数学物理基础。除了数学物理基础之外，其他的都是数学物理原理的推论。像无线通信这样的东西，没有任何的原创性，一点儿原创性都没有，不需要任何思考，无非是一群工贼偷走了物理学家做的发电机，然后办了一些会议，让别的人 fork，照着这台机器模仿，做出来了就去拿什么爱拽补一的什么奖章。

换句话说，工科的原创性研究基本是没有的，无非就是到哪个地方去抄点东西。遇到什么工程难题，百度、谷歌，大不了到知乎上面提问。理科的研究人员是真正的思考者，而工科的研究人员无非是一群玩乐高玩具的人。这些玩具还不知道是从哪家小孩那里抢过来的。现在互联网通畅了，我看他想搞个轮子，就随便就近找个网站就有了。

最近一些新闻在讲，人工智能会逐步代替人类，我看工科人都首当其冲。只要我们写个自动连接搜索引擎的脚本，让它搜索“怎么做‘一些宇宙真理’这道题”，它自己东找到西找到，不用几分钟就能拼拼凑凑找到答案。我看这样的人工智能，也不用几行代码，又比工科人便宜，还比他们诚实可靠。

今天他们工科的人说什么有人发明了斯纳德，说这个东西特别好。我看啊，又是从哪里复制粘贴过来的。工科人怎么可能会从零开始呢？他们没有这个能力。

**问题背景**

我们先介绍问题背景。小工产生了一个哈希对 (H\_1, H\_2, X)，这些哈希对符合下面的三个条件。

* 存在 R\_1 是 H\_1 的原像
* 存在 R\_2 是 H\_2 的原像
* R\_1 = R\_2 XOR X

小工希望向小理证明：它的这个哈希对 (H\_1, H\_2, X) 符合上述的条件；但是小工不希望告诉小理 R\_1 和 R\_2 是什么。

换句话说，我们需要两个性质：

* 小理相信小工产生的哈希对符合上面的三个条件。
* 小理不知道 R\_1 和 R\_2。

**解决问题的方法：零知识非交互式零知识证明**

本题考虑一种方法 -- 非交互式零知识证明（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, zkSNARK）。这种证明方法在著名的区块链货币 Zcash 里面有充分应用，他可以实现完全匿名的区块链货币交易。未来，这种技术还会用于实现支持保密智能合约的区块链系统。

zkSNARK 是这样工作的：小工知道有一个算法 F(H\_1, H\_2, X, R\_1, R\_2) 能够快速验证这个哈希对是否满足条件。他根据这个算法产生几个数字，而这几个数字就蕴含着证明哈希对满足条件的神秘力量，但是却能够隐藏 R\_1 和 R\_2。我们记这些数字为一个证明 v。

如果小工告诉小理 (H\_1, H\_2, X, v)，当小理对 v 和其他参数进行某些计算之后，小理就能够相信小工提供的 (H\_1, H\_2, X) 满足条件。在这个过程里面，R\_1 和 R\_2 没有泄露给小理。

**回到这个问题**

上述描述的过程里面，小理验证这个证明是否有效，需要一个校验密钥，这个密钥我们称为 vk。我们在压缩包 vkandproofs.zip 里面提供了这个文件。 我们产生了 40 个有效的证明和 40 个无效的证明。它们就混在这 80 个证明文件里面。

你现在需要补全这个 github repo 里面缺少的验证算法，然后利用这个验证算法来找出哪些证明是有效的。

如果第 i 个证明是有效的，那么我们记 b\_i = 1，否则记 b\_i = 0。flag 的格式为 flag{b\_1 b\_2 ... b\_80}。

例如 flag 可能是 flag{11010101010101010101010101010101....1010101}

**有关的代码**

<https://github.com/weikengchen/lightning_circuit>

**Hint**

