Проверка блокчейна РУЧ

Ограничение времени 1 секунда

64Mb Ограничение памяти

Ввод стандартный ввод или

input.txt

стандартный вывод или Вывод

Блокчейн (blockchain) переводится как «цепочка

output.txt

блоков». Это способ хранения данных, защищённый от подделки, используемый, в частности, криптовалютой биткоин.

Блокчейн действительно представляет собой последовательность блоков. Каждый блок представляет собой некоторую полезную информацию (в частности, в случае биткоина это список транзакций за определённый период времени кто кому когда сколько денег передал), снабжённую случайным числом и некоторыми служебными данными, в том числе **хэшем** — числом, которое по определённой формуле зависит от остальной части блока и хэша предыдущего блока.

Хэш должен быть меньше определённого числа. При этом формула, по которой вычисляется хэш, устроена так, что невозможно получить достаточно маленький хэш иначе, чем перебирая различные значения случайного числа. Поэтому если злоумышленник решит подделать блокчейн (и, допустим, вставить в его середину блок с записью о том, что все люди передают ему все свои деньги), то ему придётся подобрать новое случайное число в новое поддельном блоке и всех последующих (ведь хэш каждого следующего блока зависит от хэша предыдущего), что потребует невозможно больших вычислительных мощностей.

атак. Напишите программу, которая проводит проверку

правильности хэшей в модельном блокчейне с

Поэтому блокчейн в целом защищён от подобных

простой хэш-функцией. Блок b_n с номером n включает полезную

информацию m_n, представленную натуральным

числом, r_n — случайное число от 0 до 255 и h_n — хеш (целое число от 0 до 255). У каждого блока хэш вычисляется по формуле $h_n = 37 \times (m_n + r_n + h_{n-1})$ (по модулю 256), при вычислении хэша начального блока h_0 вместо хэша предыдущего блока берётся ноль. При этом каждый блок представлен одним числом b_n

хэш h_n был меньше 100. Формат ввода На первой строке вводится натуральное число N —

 $= h_n + r_n \times 256 + m_n \times 256^2$. При этом требуется, чтобы

Формат вывода

Далее следуют N чисел b_n, каждое на отдельной

Следует вывести номер первого блока, у которого неправильный хэш (не меньше 100 или не совпадает с вычисленным по указанной в условии формуле), или

номера от 0 до N-1.

Нумерация блоков идёт с нуля, т. е. они имеют

-1, если все хэши в блокчейне правильные.

количество блоков.

строке.

Пример 1	
Ввод	Вывод
5 6122802 14406496 15230209	-1

1839958 5214020

2541121 1758741		
Пример 2		
Ввод	Вывод	
5	3	
1865535		
13479687		
16689153		