

Доступ к серверу

Автор задачи: Даниил Орешников, разработчики: Константин Бац и Даниил Орешников

Будем решать задачу с помощью хешей. Поскольку хеши будут вести себя некорректно по какому-то стандартному модулю, когда значения элементов вычисляются по модулю 139, возьмем хеш по модулю 139. Разумеется, одного хеша по модулю 139 не хватит, поэтому будем использовать несколько (достаточно пяти-шести) хешей с разными простыми по одному модулю для сравнения строк.

Для решения первой подгруппы можно просто перебрать позицию вхождения кода в массив и с помощью хешей проверить, что вхождение удовлетворяет условию. Для этого зафиксируем позицию старта l , тогда $b_{l:l+q}$ — это ключ, а $b_{l+q:l+q+m}$ — это зашифрованный код. Поскольку мы считаем хеши по модулю 139, достаточно проверить, что хеш i -го блока зашифрованного кода равен сумме хеша i -го блока кода и хеша ключа, что можно сделать за $\mathcal{O}(1)$. Получаем решение за $\mathcal{O}(n \cdot \frac{m}{q})$.

Вторая подгруппа была упрощением полного решения без необходимости считать хеши. Заметим, что если разбить код на блоки длины q , которое в данной подгруппе равно 1, то разностный массив хешей блоков (а в данном случае — просто соседних элементов) будет совпадать с разностным массивом тех же блоков в зашифрованном коде. Действительно, к каждому блоку было прибавлено одно и то же значение, и в разностном массиве они сократятся.

Соответственно, задача свелась к поиску разностного массива $\text{diff}(a)$ в разностном массиве $\text{diff}(b)$ и проверке, что соответствующее вхождение в b отличается от a прибавлением предшествующего вхождению элемента b (ключа). Первое можно реализовать за $\mathcal{O}(n+m)$ с помощью алгоритма КМП (префикс-функции), после чего для каждого вхождения проверить предшествующий элемент.

Если $a_i = 0$, то на самом деле требуется найти $\frac{m}{q} + 1$ вхождение ключа в b подряд. Вернемся к решению с хешами и упорядочим блоки длины q из массива b так, чтобы подряд шли «соседние» блоки. Иными словами, выпишем подряд все блоки, начинающиеся в индексах с остатком 0 по модулю q , затем с остатком 1, и так далее. В таком массиве достаточно найти $\frac{m}{q} + 1$ блок подряд с одинаковыми хешами и имеющими одинаковый остаток индекса начала по модулю q . Это можно сделать просто жадным проходом по массиву за $\mathcal{O}(n)$.

В предпоследней группе очередное упрощение полного решения. Теперь требуется найти два блока длины q в b такие, что хеш второго равен хешу первого плюс хеш a . Аналогично, решается выписыванием всех рядом стоящих блоков подряд и проверкой разности соседних.

Для полного решения воспользуемся и хешами, и разностным массивом. Выпишем все блоки длины q подряд, и на массиве хешей этих блоков построим разностный массив. Как и во второй подгруппе, с помощью КМП можно найти все вхождения $\text{diff}(a)$ в полученный $\text{diff}(\text{blocks}(b))$. Для каждого вхождения остается проверить, что разность между соответствующими блоками действительно соответствует предшествующему блоку, который должен быть ключом.