

## РЕШЕНИЯ ЗАДАЧ

### Задача 1

Применим метод математической индукции по параметру  $k$ . При  $k = 1$  формула очевидна. Допустим формула верна для значения  $k - 1$ . Искомое число равно числу последовательностей

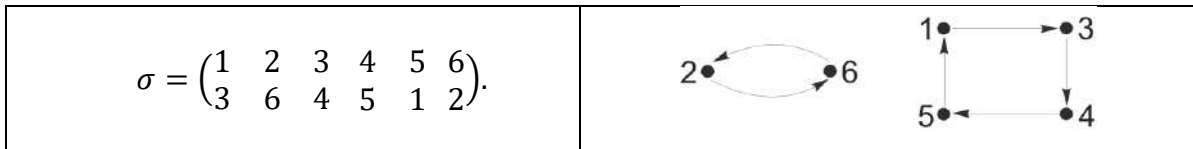
$$a_1, b_1, a_2, b_2, \dots, a_{k-1}, b_{k-1}, \quad (2)$$

в которых количество  $i = 1, 2, \dots, k - 1$ , таких, что  $a_i = 0$  и  $b_i = 1$  четно (в этом случае пара  $(a_k, b_k)$  может быть только  $(0, 1)$ ) плюс количество последовательностей вида (2) в которых количество чисел  $i = 1, 2, \dots, k - 1$ , таких, что  $a_i = 0$  и  $b_i = 1$  нечетно, умноженному на 3 (так как пара  $(a_k, b_k)$  может быть любой из пар  $(0, 0)$ ,  $(1, 0)$ ,  $(1, 1)$ ). В итоге по предположению индукции нужное число последовательностей будет удовлетворять равенству

$$(2^{2(k-1)} - (2^{2(k-1)-1} - 2^{k-2})) + 3(2^{2(k-1)-1} - 2^{k-2}) = 2^{2k-1} - 2^{k-1}.$$

### Задача 2

Приведенное в условии правило перестановки букв, или *перестановку*, будем обозначать греческой буквой  $\sigma$ . Перестановку  $\sigma$  можно интерпретировать как отображение множества цифр  $\{1, 2, 3, 4, 5, 6\}$  в себя. Например, тот факт, что первая буква перешла на третье место, можно записать как  $\sigma(1) = 3$ , а также изобразить стрелочкой из 1 в 3:



Видно, что если бы мы перестановку  $\sigma$  применяли многократно, то буквы на 2-й и 6-й позициях постоянно менялись бы местами, а буквы на позициях 1, 3, 4, 5 переставлялись бы по циклу. Поэтому перестановка  $\sigma$  может символически быть записана в виде *произведения циклов*:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 1 & 2 \end{pmatrix} = (1345)(26) = 4 * 2.$$

Запись  $4 * 2$  отражает *цикловую структуру* перестановки  $\sigma$ , показывая, что в ней один цикл длины 4 и один цикл длины 2.

Посмотрим теперь более детально на то, что произойдет, если по правилу  $\sigma$  переставить буквы еще раз. Так 1 при первом применении правила  $\sigma$  перешла в 3:  $\sigma(1) = 3$ , а при повторном применении 3 перешла в 4:  $\sigma(3) = 4$ . Значит, в результате двойной перестановки 1 переходит в 4. Будем это записывать как  $\sigma(\sigma(1)) = 4$  или же  $\sigma^2(1) = 4$ . Поэтому правило двойной перестановки букв, представляющее собой *квадрат перестановки*  $\sigma$ , выглядит так:

$\begin{aligned} \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 1 & 3 & 6 \end{pmatrix} = \\ &= (14)(13)(2)(6) = 2 * 2 * 1 * 1. \end{aligned}$	
--	--

Заметим, что после повторной перестановки 2 и 6 вернуться на свои места, то есть цикл  $(2, 6)$  распадется на два тривиальных цикла  $(2)$  и  $(6)$ , а цикл  $(1345)$  превратится в два цикла  $(1, 4)$  и  $(3, 5)$ . Таким образом, при повторном применении перестановки циклы четной длины  $2n$  распадаются на два цикла, длины  $n$  каждый. Несложно проверить, что при этом циклы нечетной длины сохраняются. Справедливо утверждение.

**Утверждение.** *Перестановка представляет собой полный квадрат в том и только том случае, когда в ее представлении в виде произведения непересекающихся циклов имеется сколько и каких угодно циклов нечетной длины, в то время как циклов одной и той же четной длины должно быть четное число.*

Рассмотрим первую комбинацию `ueqwrt` из пункта а). Она получена из `qwerty` перестановкой  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 6 & 1 \end{pmatrix} = (1324561)$ , которая представляет собой цикл длины 6. Поскольку циклов четной длины здесь нечетное количество (всего один), то, согласно утверждению, такая комбинация двойной перестановкой букв получиться не могла. Аналогично исследуются и остальные комбинации в пункте а).

Проведем подсчет общего числа перестановок, являющихся полными квадратами. Их цикловые структуры могут быть следующие:

- $1 * 1 * 1 * 1 * 1 * 1$ . Это перестановка, оставляющая все на своих местах (тождественная перестановка). Она единственна.
- $1 * 5$ . Мы должны выбрать 5 элементов из шести, чтобы составить цикл длины 5. Это можно сделать 6-ю способами. Из пяти элементов цикл длины 5 можно организовать  $(5 - 1)!$  способами (действительно, организуем цикл из пяти элементов  $a_1, a_2, a_3, a_4, a_5$ ; элемент  $a_1$  может перейти в любой из четырех (т.к. в себя нельзя), элемент  $a_2$  переходит в один из оставшихся трех и т.д. В итоге получаем  $4 \cdot 3 \cdot 2 \cdot 1$  способов). Таким образом, здесь  $6 \cdot 4! = 144$  перестановок.
- $2 * 2 * 1 * 1$ . Выбрать два элемента из шести для первого цикла длины 2 можно  $C_6^2$  способами. Для второго цикла длины 2 есть  $C_4^2$  способа. Итого  $C_6^2 \cdot C_4^2 = 90$ . От порядка следования циклов результат не зависит, поэтому 90 еще следует разделить на два. Всего 45 перестановок с такой структурой.
- $3 * 3$ . Здесь мы 6 элементов десятью способами ( $\frac{1}{2}C_6^3 = 10$ ) разбиваем на две тройки и из каждой тройки получаем по 2 цикла. Всего 40 перестановок.
- $3 * 1 * 1 * 1$ . Здесь мы двадцатью способами ( $C_6^3 = 20$ ) выбираем тройку и из каждой тройки получаем по 2 цикла. Всего 40 перестановок.

В итоге, имеется  $1 + 144 + 45 + 40 + 40 = 270$  перестановок длины 6, представляющих собой полный квадрат.

**ОТВЕТ:** а) Полученные двойной перестановкой комбинации выделены цветом.

yetrqw	eyrtqw	yrwteq	rewqyt	qwtyre	lywreq
--------	--------	--------	--------	--------	--------

б) 270.

### Задача 3

Число возможных вариантов  $d_1$  и  $d_2$ :  $10 + 9 + \dots + 1 = 55$ , можно для каждого варианта проверять, что соответствие входных и выходных символов, а можно предложить более быстрый способ, заключающийся в нахождении сначала  $d_1$  (максимум 10 вариантов), а затем  $d_2$ . Для этого достаточно заметить следующее.

Если рассмотреть систему уравнений, соответствующую выходным знакам на расстоянии  $d_1$  вида  $1 \dots 1$  в произвольном такте работы  $\mu_1$ :

$$\begin{aligned}x_{\mu_1} + x_{\mu_1+d_1} - x_{\mu_1+d_1+d_2} &\geq 1, \\x_{\mu_1+d_1} + x_{\mu_1+2d_1} - x_{\mu_1+2d_1+d_2} &\geq 1,\end{aligned}$$

то если  $x_{\mu_1+d_1} = 0$ , то  $x_{\mu_1} = 1, x_{\mu_1+2d_1} = 1$ .

Это позволяет отбраковать опробуемый вариант  $d_1$ . Устанавливаем, что  $d_1 = 2$ .

Аналогично, если рассмотреть систему уравнений, соответствующую выходным знакам на расстоянии  $d_2$  вида  $0 \dots 1$  в произвольном такте работы  $\mu_1$ :

$$\begin{aligned}x_{\mu_1} + x_{\mu_1+d_1} - x_{\mu_1+d_1+d_2} &\leq 0, \\x_{\mu_1+d_2} + x_{\mu_1+d_1+d_2} - x_{\mu_1+d_1+2d_2} &\geq 1,\end{aligned}$$

тогда если  $x_{\mu_1+d_1+d_2} = 0$ , то  $x_{\mu_1+d_1} = 0, x_{\mu_1+d_1+2d_2} = 0$ .

Это позволяет отбраковать опробуемый вариант  $d_2$  (с учётом найденного ранее  $d_1 = 2$ ).

Находим  $d_2 = 6$ .

**ОТВЕТ:**  $d_1 = 2, d_2 = 6$ .

### Задача 4

Необходимо заметить, что из равенств

$$(b_1, b_2) = g^{128}(a_1, a_2),$$

$$(b'_1, b'_2) = g^{128}(a'_1, a'_2),$$

$$(a'_1, a'_2) = g(a_1, a_2)$$

следует равенство

$$(b'_1, b'_2) = g(b_1, b_2).$$

Необходимым условием выполнения равенств  $(a'_1, a'_2) = g(a_1, a_2)$ ,  $(b'_1, b'_2) = g(b_1, b_2)$  являются равенства  $a'_1 = a_2, b'_1 = b_2$ . Среди приведенных в задаче пар знаков открытого и шифрованного текстов есть знаки, удовлетворяющие этому условию: одна пара (21,0), (0,17) и вторая пара (29,5), (5,21). То есть

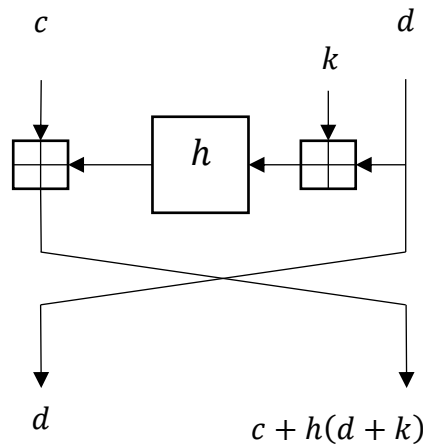
$$(15,25) = g^{128}(21,0),$$

$$(25,4) = g^{128}(0,17).$$

Из условия задачи возможность найти ключ – воспользоваться равенствами

$$(0,17) = g(21,0), (25,4) = g(15,25).$$

Убедимся, что при этих условиях оба равенства дают одинаковое значение ключа  $k$ .



**ОТВЕТ:** 19.

### Задача 5

Множество всех последовательностей длины  $k$  состоит из  $m^k$  последовательностей. Это множество разбивается на три непересекающихся между собой подмножества:

1. Последовательностей, не содержащих  $a$ .
2. Последовательностей, содержащих  $a$ , но не содержащих двух подряд идущих таких букв.
3. Последовательностей, содержащих  $a$ , в которых встречаются две подряд идущие такие буквы.

Чтобы решить задачу, нужно найти число последовательностей во втором подмножестве и вычесть его из числа  $m^k$ .

В свою очередь, множество последовательностей второго типа можно разбить на непересекающиеся подмножества, в которые входят последовательности, содержащие  $1, 2, \dots, \lfloor \frac{k+1}{2} \rfloor$  букв " $a$ ". Тогда общее число последовательностей второго типа будет равно:

$$\begin{aligned}
 & k \cdot (m-1)^{k-1} + \binom{k-1}{2} (m-1)^{k-2} + \dots + \binom{k+1-t}{t} (m-1)^{k-t} + \dots \\
 & + \binom{k+1 - \lfloor \frac{k+1}{2} \rfloor}{\lfloor \frac{k+1}{2} \rfloor} (m-1)^{k - \lfloor \frac{k+1}{2} \rfloor} = \\
 & = \sum_{t=1}^{\lfloor \frac{k+1}{2} \rfloor} \binom{k+1-t}{t} (m-1)^{k-t}
 \end{aligned}$$

поскольку число последовательностей длины  $k$ , содержащих ровно  $t$  отдельно стоящих букв " $a$ ", равно

$$\binom{k+1-t}{t} (m-1)^{k-t}$$

а максимально возможное число букв " $a$ " в такой последовательности, равно

$$\lfloor \frac{k+1}{2} \rfloor$$

**ОТВЕТ:** 27466.

### Задача 6

Сначала надо решить СЛУ и определить значения  $(b_1, \dots, b_5)$ . После в квадратичной системе от переменных  $x_1, \dots, x_{10}$  зафиксируем значения переменных  $x_7, x_8, x_9, x_{10}$  произвольным образом и решим полученную СЛУ относительно оставшихся переменных. В случае, если получится несовместная СЛУ, то необходимо зафиксировать значения переменных  $x_7, x_8, x_9, x_{10}$  другим образом.