XXXI
Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии

УСЛОВИЯ И РЕШЕНИЯ

Москва 2022

Приводимые задания предлагались в трех возрастных категориях (9, 10, 11 классы) по два равноценных по сложности варианта в 9 и 10 классах и по два равноценных по сложности варианта в каждом из трех групп часовых поясов (ЗАПАД, СИБИРЬ, ВОСТОК) для участников 11 класса. Тематика отдельных задач в разных классах пересекается, при этом младшим классам предлагались более легкие варианты заданий.

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

9 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Решите уравнение $p^4 + q^2 = n^2$, где p и q – простые числа, а n –натуральное число.

2. Дана последовательность $a_1, b_1, a_2, b_2, \dots, a_k, b_k$, состоящая из 0 и 1. Пусть N – количество чисел i от 1 до k таких, что $a_i = 0$ и $b_i = 1$. Докажите, что число последовательностей указанного вида, для которых N нечетно, находится по формуле $2^{2k-1} - 2^{k-1}$.

3. Петя использует для работы в интернете пароли из шести символов. Опасаясь злоумышленников, он решил в каждом пароле изменить порядок следования символов, используя для этого одно и то же *правило*, которое записал в книжечку. Правило могло выглядеть, например, так: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 1 & 2 \end{pmatrix}$. То есть первый символ ставится на третье место,

второй – на шестое и так далее. В своем пароле для почты **qwerty** Петя переставил буквы по правилу из книжечки, а затем, для большей надежности переставил буквы по этому же правилу еще раз. (Если использовать правило как в примере, то из **qwerty** после первой перестановки получится **tyqerw**, а после второй – **rwtqey**). Какие из нижеследующих комбинаций могли быть получены двойной перестановкой букв в пароле **qwerty** (используя, возможно, другие правила указанного вида):

а)

yetrqw	eyrtqw	yrwteq	rewqyt	qwtyre	tywreq

б) Петя потерял книжечку! Он помнит, что первоначально пароль был **qwerty**, но правило, по которому были в нем дважды переставлены буквы, не помнит. За какое наименьшее число попыток можно с гарантией подобрать утерянный пароль?

4. Знаками открытого и шифрованного текстов являются пары целых от 0 до 31. Для зашифрования используется секретный ключ k (целое число от 0 до 31), заданная таблично функция h, а также функция $g(c,d)$, которая паре целых чисел (c,d) ставит в соответствие пару $(d, c+h(d+k))$ (причем если число $d+k$ или $d+h(d+k)$ превышает 31, то их заменяют остатком от деления на 32). Знак шифрованного текста (b_1,b_2) получается из знака открытого текста (a_1,a_2) путем 128-кратного применения функции g:

$$(b_1,b_2)=g^{128}(a_1,a_2)=g\left(\dots g\left(g(a_1,a_2)\right)\right).$$

Известно, что знак открытого текста $(21,0)$ преобразовался в знак зашифрованного текста $(15,25)$, знак $(7,3)$ преобразовался в $(29,5)$, $(0,17)$ – в $(25,4)$ и, наконец, $(5,21)$ – в $(22,9)$. Найдите ключ k.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$h(i)$	9	1	30	4	24	12	8	23	18	7	16	15	21	26	10	17	19	22	13	28	14	11	2	29	3	6	27	0	5	25	31	20

5. Подписью битового сообщения $(a_1,\dots,a_4)$ является любой битовый набор $(x_1,\dots,x_8)$, который удовлетворяет соотношениям

$a_1=b_1\oplus b_3\oplus b_4$, $b_1=x_1x_8\oplus x_2x_7\oplus x_3x_8\oplus x_4x_6\oplus x_5x_8\oplus x_6x_7\oplus x_7x_8$,
$a_2=b_2\oplus b_3\oplus b_4$, $b_2=x_1x_7\oplus x_2x_6\oplus x_3x_7\oplus x_4x_8\oplus x_5x_7\oplus x_6x_7\oplus x_6x_8$,
$a_3=b_1\oplus b_2\oplus b_3$, $b_3=x_1x_6\oplus x_2x_8\oplus x_3x_6\oplus x_4x_7\oplus x_5x_6\oplus x_6x_8\oplus x_7$,
$a_4=b_1\oplus b_2\oplus b_4$, $b_4=x_1x_6\oplus x_2x_6\oplus x_3x_7\oplus x_4x_8\oplus x_5x_7\oplus x_6x_7\oplus x_7x_8$.

Здесь $\oplus$ – стандартная операция сложения битов: $0\oplus 0=1\oplus 1=0$, $0\oplus 1=1\oplus 0=1$.

Найдите какую-нибудь подпись для сообщения (0,1,1,1).

6. На вход устройства подается лента с записанными на ней нулями и единицами:

Лента	**1** 0 0 **1** 0 0 0 1 **1** 0 1 1 1 1 0 0 0 1 1 0 0 0 0 1 1 0 1 0 1 1 0 1 0 0 1 1 0 1 1 0…
Позиции	μ_1 μ_2 μ_3 ⇨

За один такт устройство считывает с ленты с позиций μ_1,μ_2,μ_3 (на первом такте $\mu_1=1$) три значения x,y,z. Если $x+y+z\geq 2$, то устройство на новой ленте печатает 1, иначе – 0. Затем устройство сдвигается на одну позицию вправо, и процедура повторяется. Найдите разности $d_1=\mu_2-\mu_1$ и $d_2=\mu_3-\mu_2$, если известно, что $d_1+d_2\leq 10$, а на новой ленте было напечатано следующее: 1 0 0 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 0 1…

(для примера на рисунке изображен случай $d_1=3, d_2=5$).

РЕШЕНИЯ ЗАДАЧ

Задача 1

Перепишем исходное равенство: $p^4=(n-q)(n+q)$. Учитывая, что $(n-q)<(n+q)$ и что p – простое число, возможны следующие случаи:

1) $\begin{cases} n-q=1 \\ n+q=p^4 \end{cases}$

2) $\begin{cases} n-q=p \\ n+q=p^3 \end{cases}$

В случае 1): вычтем из второго уравнения первое. Получим равенство

$2q=p^4-1$

Это равносильно

$2q = (p-1)(p+1)(p^2+1)$

Так как q простое число, то это возможно только при $p-1=1$. Непосредственной проверкой убеждаемся, что $p=2$ не подходит.

В случае 2): вычтем из второго уравнения первое. Получим равенство

$2q = p^3 - p$

Это равносильно

$2q = (p-1)p(p+1)$

Так как q простое число, то это возможно только при $p-1=1$.

Отсюда найдём $p=2, q=3, n=5$..

ОТВЕТ: $p=2, q=3, n=5$.

Задача 2

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

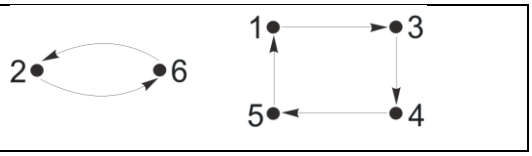
$$a_1, b_1, a_2, b_2, \ldots, a_{k-1}, b_{k-1}, \qquad (2)$$

в которых количество $i = 1,2,\ldots k-1$, 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 $i = 1,2,\ldots k-1$, 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 3

Приведенное в условии правило перестановки букв, или *перестановку*, будем обозначать греческой буквой σ. Перестановку σ 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:

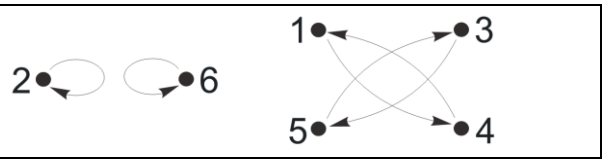
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 1 & 2 \end{pmatrix}$.	

Видно, что если бы мы перестановку σ 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 σ 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 σ, показывая, что в ней один цикл длины 4 и один цикл длины 2.

Посмотрим теперь более детально на то, что произойдет, если по правилу σ переставить буквы еще раз. Так 1 при первом применении правила σ 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* σ, выглядит так:

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

Заметим, что после повторной перестановки 2 и 6 вернутся 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 yeqwrt 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 дины 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	tywreq

б) 270.

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

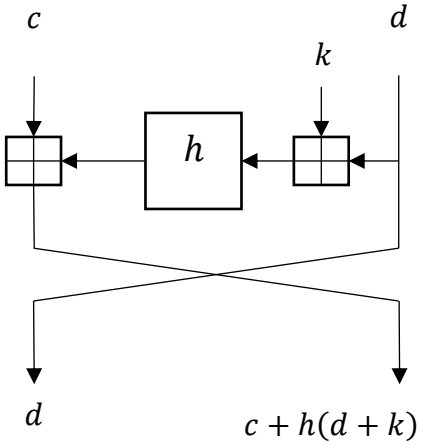
$(15,25) = g^{128}(21,0)$,

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

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

Сначала надо решить СЛУ и определить значения $(b_1, \dots, b_4)$ – в нашем случае $(b_1, \dots, b_4)$) = (1, 0, 0, 0). После в квадратичной системе от переменных $x_1, \dots, x_8$ зафиксируем значения переменных x_6, x_7, x_8 произвольным образом и решим полученную СЛУ относительно оставшихся переменных. В случае, если получится несовместная СЛУ как, например, при $x_6 = 1, x_7 = 0, x_8 = 1$, то необходимо зафиксировать значения переменных x_6, x_7, x_8 другим образом. Например, при фиксации $x_6 = 1, x_7 = 0, x_8 = 0$ имеем два решения $x_1 = 0, x_2 = 0, x_4 = 1, x_3 = x_5$

Задача 6

Число возможных вариантов d_1 и d_2 : $9 + 8 + \dots + 1 = 45$, можно для каждого варианта проверять, что соответствие входных и выходных символов, а можно предложить более быстрый способ, заключающийся в нахождении сначала d_1 (максимум 9 вариантов), а затем d_2. Для этого достаточно заметить следующее.

Если рассмотреть систему уравнений, соответствующую выходным знакам на расстоянии d_1 вида 1 ... 1 в произвольном такте работы μ_1:

$$x_{\mu_1} + x_{\mu_1+d_1} + x_{\mu_1+d_1+d_2} \le 1,$$
$$x_{\mu_1+d_1} + x_{\mu_1+2d_1} + x_{\mu_1+2d_1+d_2} \le 1,$$

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

Это позволяет отбраковать опробуемый вариант d_1. Устанавливаем, что $d_1 = 4$.

Аналогично, если рассмотреть систему уравнений, соответствующую выходным знакам на расстоянии d_2 вида $0 \dots 0$ в произвольном такте работы μ_1 :

$$x_{\mu_1} + x_{\mu_1+d_1} + x_{\mu_1+d_1+d_2} \le 1,$$
$$x_{\mu_1+d_2} + x_{\mu_1+d_1+d_2} + x_{\mu_1+d_1+2d_2} \le 1,$$

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: $d_1 = 4, d_2 = 6$.

10 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Решите уравнение $p^4 + q^2 = n^2$, где p и q – простые числа, а n –натуральное число.

2. Дана последовательность $a_1, b_1, a_2, b_2, \dots, a_k, b_k$, состоящая из 0 и 1. Пусть N – количество чисел i от 1 до k таких, что $a_i = 0$ и $b_i = 1$. Докажите, что число последовательностей указанного вида, для которых N нечетно, находится по формуле $2^{2k-1} - 2^{k-1}$.

3. Петя использует для работы в интернете пароли из шести символов. Опасаясь злоумышленников, он решил в каждом пароле изменить порядок следования символов, используя для этого одно и то же *правило*, которое записал в книжечку. Правило могло выглядеть, например, так: $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 6 & 4 & 5 & 1 & 2\end{pmatrix}$. То есть первый символ ставится на третье место, второй – на шестое и так далее. В своем пароле для почты **qwerty** Петя переставил буквы по правилу из книжечки, а затем, для большей надежности переставил буквы по этому же правилу еще раз. (Если использовать правило как в примере, то из **qwerty** после первой перестановки получится **tyqerw**, а после второй – **rwtqey**). Какие из нижеследующих комбинаций могли быть получены двойной перестановкой букв в пароле **qwerty** (используя, возможно, другие правила указанного вида):

а)

yetrqw	eyrtqw	yrwteq	rewqyt	qwtyre	tywreq

б) Петя потерял книжечку! Он помнит, что первоначально пароль был **qwerty**, но правило, по которому были в нем дважды переставлены буквы, не помнит. За какое наименьшее число попыток можно с гарантией подобрать утерянный пароль?

4. Знаками открытого и шифрованного текстов являются пары целых от 0 до 31. Для зашифрования используется секретный ключ k (целое число от 0 до 31), заданная таблично функция h, а также функция $g(c,d)$, которая паре целых чисел (c,d) ставит в соответствие пару $(d, c + h(d+k))$ (причем если число $d+k$ или $d + h(d+k)$ превышает 31, то их заменяют остатком от деления на 32). Знак шифрованного текста (b_1, b_2) получается из знака открытого текста (a_1, a_2) путем 128-кратного применения функции g:

$$(b_1, b_2) = g^{128}(a_1, a_2) = g\Big(\dots g\big(g(a_1, a_2)\big)\Big).$$

Известно, что знак открытого текста $(21,0)$ преобразовался в знак зашифрованного текста $(15,25)$, знак $(7,3)$ преобразовался в $(29,5)$, $(0,17)$ – в $(25,4)$ и, наконец, $(5,21)$ – в $(22,9)$. Найдите ключ k.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$h(i)$	9	1	30	4	24	12	8	23	18	7	16	15	21	26	10	17	19	22	13	28	14	11	2	29	3	6	27	0	5	25	31	20

5. Подписью битового сообщения $(a_1, \dots, a_4)$ является любой битовый набор $(x_1, \dots, x_8)$, который удовлетворяет соотношениям

$a_1 = b_1 \oplus b_3 \oplus b_4$, $b_1 = x_1x_8 \oplus x_2x_7 \oplus x_3x_8 \oplus x_4x_6 \oplus x_5x_8 \oplus x_6x_7 \oplus x_7x_8$,
$a_2 = b_2 \oplus b_3 \oplus b_4$, $b_2 = x_1x_7 \oplus x_2x_6 \oplus x_3x_7 \oplus x_4x_8 \oplus x_5x_7 \oplus x_6x_7 \oplus x_6x_8$,
$a_3 = b_1 \oplus b_2 \oplus b_3$, $b_3 = x_1x_6 \oplus x_2x_8 \oplus x_3x_6 \oplus x_4x_7 \oplus x_5x_6 \oplus x_6x_8 \oplus x_7$,
$a_4 = b_1 \oplus b_2 \oplus b_4$, $b_4 = x_1x_6 \oplus x_2x_6 \oplus x_3x_7 \oplus x_4x_8 \oplus x_5x_7 \oplus x_6x_7 \oplus x_7x_8$.

Здесь $\oplus$ – стандартная операция сложения битов: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$.

Найдите какую-нибудь подпись для сообщения (0,1,1,1).

6. На вход устройства подается лента с записанными на ней нулями и единицами:

Лента	**1**00**1**0001**1**0111100011000011010110100110110…
Позиции	μ_1 μ_2 μ_3 ⟹

За один такт устройство считывает с ленты с позиций μ_1, μ_2, μ_3 (на первом такте $\mu_1 = 1$) три значения x, y, z. Если $x + y + z \geq 2$, то устройство на новой ленте печатает 1, иначе – 0. Затем устройство сдвигается на одну позицию вправо, и процедура повторяется. Найдите разности

$d_1 = \mu_2 - \mu_1$ и $d_2 = \mu_3 - \mu_2$, если известно, что $d_1 + d_2 \le 10$, а на новой ленте было напечатано следующее: 1 0 0 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 0 1… (для примера на рисунке изображен случай $d_1 = 3, d_2 = 5$).

РЕШЕНИЯ ЗАДАЧ

Задача 1

Перепишем исходное равенство: $p^4 = (n-q)(n+q)$. Учитывая, что $(n-q) < (n+q)$ и что p – простое число, возможны следующие случаи:

3) $\begin{cases} n-q=1 \\ n+q=p^4 \end{cases}$

4) $\begin{cases} n-q=p \\ n+q=p^3 \end{cases}$

В случае 1): вычтем из второго уравнения первое. Получим равенство

$2q = p^4 - 1$

Это равносильно

$2q = (p-1)(p+1)(p^2+1)$

Так как q простое число, то это возможно только при $p - 1 = 1$. Непосредственной проверкой убеждаемся, что $p = 2$ не подходит.

В случае 2): вычтем из второго уравнения первое. Получим равенство

$2q = p^3 - p$

Это равносильно

$2q = (p-1)p(p+1)$

Так как q простое число, то это возможно только при $p - 1 = 1$.

Отсюда найдём $p = 2, q = 3, n = 5$..

ОТВЕТ: $p = 2, q = 3, n = 5$.

Задача 2

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

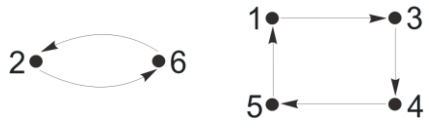
$$a_1, b_1, a_2, b_2, \ldots, a_{k-1}, b_{k-1}, \qquad (2)$$

в которых количество $i = 1,2,\ldots k-1$, 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 $i = 1,2,\ldots k-1$, 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 3

Приведенное в условии правило перестановки букв, или *перестановку*, будем обозначать греческой буквой σ. Перестановку σ 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:

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 1 & 2 \end{pmatrix}$.	

Видно, что если бы мы перестановку σ 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

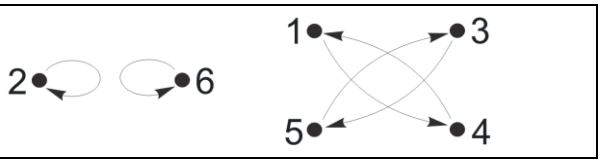
по циклу. Поэтому перестановка σ может символически быть записана в виде *произведения циклов*:

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

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

Посмотрим теперь более детально на то, что произойдет, если по правилу σ переставить буквы еще раз. Так 1 при первом применении правила σ 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 $\sigma\big(\sigma(1)\big) = 4$ или же $\sigma^2(1) = 4$. Поэтому правило двойной перестановки букв, представляющее собой *квадрат перестановки* σ, выглядит так:

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



Заметим, что после повторной перестановки 2 и 6 вернутся 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 `yeqwrt` 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 дины 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.

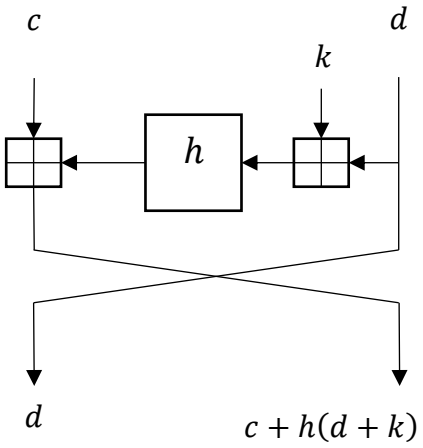
ОТВЕТ: а) Полученные двойной перестановкой комбинации выделены цветом.

yetrqw	eyrtqw	yrwteq	rewqyt	qwtyre	tywreq

б) 270.

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

Сначала надо решить СЛУ и определить значения $(b_1, \dots, b_4)$ – в нашем случае $(b_1, \dots, b_4)) = (1, 0, 0, 0)$. После в квадратичной системе от переменных $x_1, \dots, x_8$ зафиксируем значения переменных x_6, x_7, x_8 произвольным образом и решим полученную СЛУ относительно оставшихся переменных. В случае, если получится несовместная СЛУ как, например, при $x_6 = 1, x_7 = 0, x_8 = 1$, то необходимо зафиксировать значения переменных x_6, x_7, x_8 другим образом. Например, при фиксации $x_6 = 1, x_7 = 0, x_8 = 0$ имеем два решения $x_1 = 0, x_2 = 0, x_4 = 1, x_3 = x_5$

Задача 6

Число возможных вариантов d_1 и d_2 : $9 + 8 + \dots + 1 = 45$, можно для каждого варианта проверять, что соответствие входных и выходных символов, а можно предложить более

быстрый способ, заключающийся в нахождении сначала d_1 (максимум 9 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 μ_1:

$$x_{\mu_1} + x_{\mu_1+d_1} + x_{\mu_1+d_1+d_2} \le 1,$$
$$x_{\mu_1+d_1} + x_{\mu_1+2d_1} + x_{\mu_1+2d_1+d_2} \le 1,$$

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

Это позволяет отбраковать опробуемый вариант d_1. Устанавливаем, что $d_1 = 4$.

Аналогично, если рассмотреть систему уравнений, соответствующую выходным знакам на расстоянии d_2 вида $0 \dots 0$ в произвольном такте работы μ_1 :

$$x_{\mu_1} + x_{\mu_1+d_1} + x_{\mu_1+d_1+d_2} \le 1,$$
$$x_{\mu_1+d_2} + x_{\mu_1+d_1+d_2} + x_{\mu_1+d_1+2d_2} \le 1,$$

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: $d_1 = 4, d_2 = 6$.

11 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Дана последовательность $a_1, b_1, a_2, b_2, \dots, a_k, b_k$, состоящая из 0 и 1. Пусть N – количество чисел i от 1 до k таких, что $a_i = 0$ и $b_i = 1$. Докажите, что число последовательностей указанного вида, для которых N нечетно, находится по формуле $2^{2k-1} - 2^{k-1}$.

2. Петя использует для работы в интернете пароли из шести символов. Опасаясь злоумышленников, он решил в каждом пароле изменить порядок следования символов, используя для этого одно и то же *правило*, которое записал в книжечку. Правило могло выглядеть, например, так: $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 6 & 4 & 5 & 1 & 2\end{pmatrix}$. То есть первый символ ставится на третье место, второй – на шестое и так далее. В своем пароле для почты **qwerty** Петя переставил буквы по правилу из книжечки, а затем, для большей надежности переставил буквы по этому же правилу еще раз. (Если использовать правило как в примере, то из **qwerty** после первой перестановки получится **tyqerw**, а после второй – **rwtqey**). Какие из нижеследующих комбинаций могли быть получены двойной перестановкой букв в пароле **qwerty** (используя, возможно, другие правила указанного вида):

а)

yetrqw	eyrtqw	yrwteq	rewqyt	qwtyre	tywreq

б) Петя потерял книжечку! Он помнит, что первоначально пароль был **qwerty**, но правило, по которому были в нем дважды переставлены буквы, не помнит. За какое наименьшее число попыток можно с гарантией подобрать утерянный пароль?

3. На вход устройства подается лента с записанными на ней нулями и единицами:

Лента	**1** 0 0 **1** 0 0 0 1 **1** 0 1 1 1 1 0 0 0 1 1 0 0 0 0 1 1 0 1 0 1 1 0 1 0 0 1 1 0 1 1 0…
Позиции	μ_1 μ_2 μ_3 ⇒

За один такт устройство считывает с ленты с позиций μ_1, μ_2, μ_3 (на первом такте $\mu_1 = 1$) три значения x, y, z. Если $x + y + z \ge 2$, то устройство на новой ленте печатает 1, иначе – 0. Затем устройство сдвигается на одну позицию вправо, и процедура повторяется. Найдите разности $d_1 = \mu_2 - \mu_1$ и $d_2 = \mu_3 - \mu_2$, если известно, что $d_1 + d_2 \le 10$, а на новой ленте было напечатано следующее: 0 0 0 1 0 0 0 0 1 0 1 1 1 1 1 1 0 0 0 1 1 1 0 1 0 1 1 1 0 1 1 0 1 0 1 0 1 0 0 1… (для примера на рисунке изображен случай $d_1 = 3, d_2 = 5$).

4. Знаками открытого и шифрованного текстов являются пары целых от 0 до 31. Для зашифрования используется секретный ключ k (целое число от 0 до 31), заданная таблично функция h, а также функция $g(c, d)$, которая паре целых чисел (c, d) ставит в соответствие пару $(d, c + h(d + k))$ (причем если число $d + k$ или $d + h(d + k)$ превышает 31, то их

заменяют остатком от деления на 32). Знак шифрованного текста (b_1, b_2) получается из знака открытого текста (a_1, a_2) путем 128-кратного применения функции g:

$$(b_1, b_2) = g^{128}(a_1, a_2) = g\left(\dots g\big(g(a_1, a_2)\big)\right).$$

Известно, что знак открытого текста $(21,0)$ преобразовался в знак зашифрованного текста $(15,25)$, знак $(7,3)$ преобразовался в $(29,5)$, $(0,17)$ – в $(25,4)$ и, наконец, $(5,21)$ – в $(22,9)$. Найдите ключ k.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$h(i)$	9	1	30	4	24	12	8	23	18	7	16	15	21	26	10	17	19	22	13	28	14	11	2	29	3	6	27	0	5	25	31	20

5. В Криптоландии используется алфавит, состоящий из четырёх латинских букв a, b, c, d. Любая последовательность букв алфавита будет *словом* криптоландского языка при выполнении единственного ограничения: если в последовательности есть хоть одна буква "a", то тогда в ней обязательно должны встретиться две буквы "a" подряд.

Например, последовательности $baacda,\ aabb,\ ddd$ являются словами, а последовательности $bcadda,\ abba$ – не являются. Найдите число слов длины 8 в криптоландском языке.

6. Подписью битового сообщения $(a_1, \dots, a_5)$ является любой битовый набор $(x_1, \dots, x_{10})$, который удовлетворяет соотношениям

$a_1 = b_3 \oplus b_4 \oplus b_5$, $b_1 = x_1x_9 \oplus x_2x_{10} \oplus x_3x_8 \oplus x_4x_9 \oplus x_5x_9 \oplus x_6x_8 \oplus x_7x_8 \oplus x_9x_{10}$,

$a_2 = b_2 \oplus b_4 \oplus b_5$, $b_2 = x_1x_8 \oplus x_2x_9 \oplus x_3x_{10} \oplus x_4x_8 \oplus x_5x_{10} \oplus x_6x_{10} \oplus x_7x_8 \oplus x_8x_9$,

$a_3 = b_2 \oplus b_3 \oplus b_5$, $b_3 = x_1x_9 \oplus x_2x_{10} \oplus x_3x_8 \oplus x_4x_7 \oplus x_5x_8 \oplus x_6x_8 \oplus x_7x_8 \oplus x_8x_9 \oplus x_{10}$,

$a_4 = b_1 \oplus b_2 \oplus b_3$, $b_4 = x_1x_7 \oplus x_2x_{10} \oplus x_3x_{10} \oplus x_4x_7 \oplus x_5x_7 \oplus x_6x_{10} \oplus x_7x_{10} \oplus x_9x_{10}$,

$a_5 = b_1 \oplus b_3 \oplus b_5$, $b_5 = x_1x_8 \oplus x_2x_7 \oplus x_3x_7 \oplus x_4x_9 \oplus x_5x_9 \oplus x_6x_8 \oplus x_7x_8 \oplus x_8x_{10} \oplus x_9$.

Здесь $\oplus$ – стандартная операция сложения битов: $0 \oplus 0 = 1 \oplus 1 = 0,\ 0 \oplus 1 = 1 \oplus 0 = 1$. Найдите какую-нибудь подпись для сообщения (0,1,0,0,0).

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

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

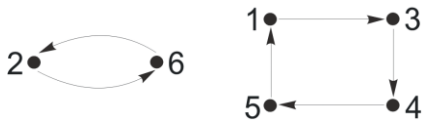
в которых количество $i = 1,2,\dots k-1$, таких, что $a_i = 0$ и $b_i = 1$ четно (в этом случае пара (a_k, b_k) может быть только $(0,1)$) плюс количество последовательностей вида (2) в которых количество чисел $i = 1,2,\dots k-1$, таких, что $a_i = 0$ и $b_i = 1$ нечетно, умноженному на 3 (так как пара (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 σ. Перестановку σ 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:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 1 & 2 \end{pmatrix}.$$

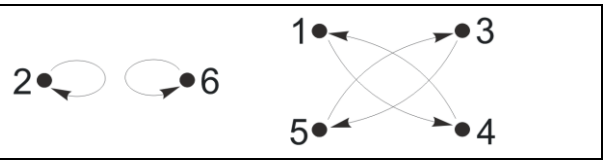


Видно, что если бы мы перестановку σ применяли многократно, то буквы на 2-й и 6-й позициях постоянно менялись бы местами, а буквы на позициях 1, 3, 4, 5 переставлялись бы по циклу. Поэтому перестановка σ может символически быть записана в виде *произведения циклов*:

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

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

Посмотрим теперь более детально на то, что произойдет, если по правилу σ переставить буквы еще раз. Так 1 при первом применении правила σ 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* σ, выглядит так:

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

Заметим, что после повторной перестановки 2 и 6 вернутся 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 `yeqwrt` 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 дины 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	tywreq

б) 270.

Задача 3

Число возможных вариантов d_1 и d_2: $10 + 9 + \cdots + 1 = 55$, 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 $1 \ldots 1$ в произвольном такте работы μ_1:

$$x_{\mu_1} + x_{\mu_1+d_1} - x_{\mu_1+d_1+d_2} \geq 1,$$
$$x_{\mu_1+d_1} + x_{\mu_1+2d_1} - x_{\mu_1+2d_1+d_2} \geq 1,$$

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 $0 \ldots 1$ в произвольном такте работы μ_1:

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

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: $d_1 = 2, d_2 = 6$.

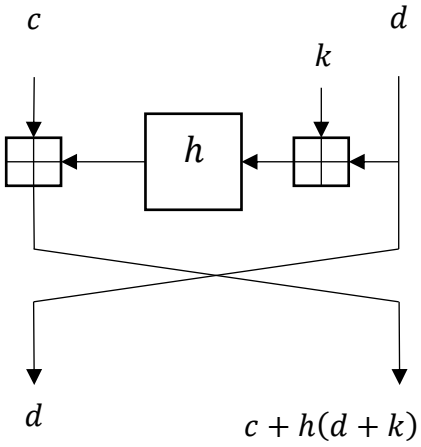
Задача 4

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 $1, 2, \dots, \left\lfloor \frac{k+1}{2} \right\rfloor$ букв "a". Тогда общее число последовательностей второго типа будет равно:

$$k \cdot (m-1)^{k-1} + \binom{k-1}{2}(m-1)^{k-2} + \cdots + \binom{k+1-t}{t}(m-1)^{k-t} + \cdots + \binom{k+1-\left\lfloor \frac{k+1}{2} \right\rfloor}{\left\lfloor \frac{k+1}{2} \right\rfloor}(m-1)^{k-\left\lfloor \frac{k+1}{2} \right\rfloor} = \sum_{t=1}^{\left\lfloor \frac{k+1}{2} \right\rfloor} \binom{k+1-t}{t}(m-1)^{k-t}$$

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

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

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.

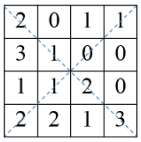
ОТБОРОЧНЫЙ ЭТАП

9 КЛАСС

1. Найдите наибольшее четырёхзначное число, которое в 207 раз больше суммы своих цифр.

2. На координатной прямой отмечены 5 точек с координатами 3; 9; −7; 29; 8. Найдите координату точки, сумма расстояний от которой до указанных 5 точек минимальна.

3. Ключом шифрсистемы служит таблица 4×4, в каждую ячейку которой записана одна из цифр 0, 1, 2 и 3. При этом должны делиться на 4 сумма цифр в каждой строке, сумма цифр в каждом столбце, а также суммы цифр на каждой из двух диагоналей, отмеченных пунктиром. На рисунке приведен один из возможных вариантов ключа. Сколько существует всего различных ключей?



4. На границе Криптоландии установлена пропускная система, имеющая 17 входов и 17 выходов (входы перед границей, выходы – уже в Криптоландии). Входы и выходы занумерованы независимо друг от друга числами от 1 до 17, причем в неизвестном для посетителей Криптоландии порядке. От каждого входа проложен один «прямой» туннель к одному из выходов, причем от разных входов – к разным выходам. От каждого выхода проложен один «обратный» туннель ко входу с тем же номером, что у этого выхода. Посетитель сам выбирает один из входов. Войдя в него, он попадает в лифт, в котором есть 2 кнопки: зеленая – «ехать», красная – «выходить». Система работает следующим образом. Посетитель, находясь в лифте около входа, нажимает зеленую кнопку, лифт по прямому туннелю доставляет его к соответствующему выходу. Находясь в лифте около выхода, посетитель может: 1) нажать зеленую кнопку, и тогда лифт по обратному туннелю доставит его ко входу с тем же номером; 2) нажать красную кнопку, и тогда выход откроется, но только если его номер совпадает с номером того входа, через который посетитель вошел первоначально. В противном случае (при несовпадении номеров) посетитель будет удалён за пределы Криптоландии и сможет воспользоваться правом посещения только через год. Алиса решила провести каникулы в Криптоландии. При этом ей стала известна схема прямых туннелей системы пропуска:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4	15	16	5	9	13	8	14	11	2	1	7	3	12	10	6

Здесь верхнее число является номером входа, а стоящее под ним число – номером того выхода, к которому ведет прямой туннель. За какое минимальное число поездок по туннелям Алиса сможет гарантированно попасть в Криптоландию?

5. Для зашифрования осмысленного слова его буквы заменили числами $x_1, x_2, \dots, x_n$ по таблице. Затем выбирали четные натуральные числа p и q и для каждого числа x_i из соотношений $x_i = y_i + pz_i$, $z_i = y_i + qx_i$ нашли целые числа y_i и z_i. Потом по формулам $z_i' = r_{32}(z_i), i = 1, \dots, n$ получили числа $z_1', \dots, z_n'$ (где $r\_32(a)$ – остаток от деления числа a на 32), которые вновь заменили буквами согласно таблице. В результате получили вот что: **ЩЙИФБА**. Найдите исходное слово, если известно, что оно начинается на букву **Е**, и запишите его буквами в ВЕРХНЕМ регистре, то есть если у Вас получился ответ олимпиада, то его следует записать, как **ОЛИМПИАДА.**

А	Б	В	Г	Д	Е Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

6. Алиса и Боб играют в "угадай число". Чтобы никто им не помешал, они играют по следующим правилам. Алиса загадывает некоторое число $c \in \{0, \dots, 122\}$, вычисляет $m_a = r_{123}(c^7)$, где $r_{123}(a)$ – остаток от деления числа a на 123, и отправляет m_a Бобу. Боб, зная как получено m_a, пытается получить c, затем вычисляет $m_b = r_{123}(c^{29})$ и отправляет m_b Алисе. Алиса в

свою очередь проверяет и говорит, то ли число получил Боб. Узнайте, какое число загадала Алиса, если Боб угадал его и $m_a = 25$, а $m_b = 31$.

10 КЛАСС

1. Найдите наибольшее четырёхзначное число, которое в 207 раз больше суммы своих цифр.

2. На координатной прямой отмечены 5 точек с координатами 3; 9; -7; 29; 8. Найдите координату точки, сумма расстояний от которой до указанных 5 точек минимальна.

3. Ключом шифрсистемы служит таблица 4×4, в каждую ячейку которой записана одна из цифр 0, 1, 2 и 3. При этом должны делиться на 4 сумма цифр в каждой строке, сумма цифр в каждом столбце, а также суммы цифр на каждой из двух диагоналей, отмеченных пунктиром. На рисунке приведен один из возможных вариантов ключа. Сколько существует всего различных ключей?

2	0	1	1
3	1	0	0
1	1	2	0
2	2	1	3

4. На границе Криптоландии установлена пропускная система, имеющая 17 входов и 17 выходов (входы перед границей, выходы – уже в Криптоландии). Входы и выходы занумерованы независимо друг от друга числами от 1 до 17, причем в неизвестном для посетителей Криптоландии порядке. От каждого входа проложен один «прямой» туннель к одному из выходов, причем от разных входов – к разным выходам. От каждого выхода проложен один «обратный» туннель ко входу с тем же номером, что у этого выхода. Посетитель сам выбирает один из входов. Войдя в него, он попадает в лифт, в котором есть 2 кнопки: зеленая – «ехать», красная – «выходить». Система работает следующим образом. Посетитель, находясь в лифте около входа, нажимает зеленую кнопку, лифт по прямому туннелю доставляет его к соответствующему выходу. Находясь в лифте около выхода, посетитель может: 1) нажать зеленую кнопку, и тогда лифт по обратному туннелю доставит его ко входу с тем же номером; 2) нажать красную кнопку, и тогда выход откроется, но только если его номер совпадает с номером того входа, через который посетитель вошел первоначально. В противном случае (при несовпадении номеров) посетитель будет удалён за пределы Криптоландии и сможет воспользоваться правом посещения только через год. Алиса решила провести каникулы в Криптоландии. При этом ей стала известна схема прямых туннелей системы пропуска:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4	15	16	5	9	13	8	14	11	2	1	7	3	12	10	6

Здесь верхнее число является номером входа, а стоящее под ним число – номером того выхода, к которому ведет прямой туннель. За какое минимальное число поездок по туннелям Алиса сможет гарантированно попасть в Криптоландию?

5. Для зашифрования осмысленного слова его буквы заменили числами $x_1, x_2, \dots, x_n$ по таблице. Затем выбирали четные натуральные числа p и q и для каждого числа x_i из соотношений $x_i = y_i + pz_i$, $z_i = y_i + qx_i$ нашли целые числа y_i и z_i. Потом по формулам $z'_i = r_{32}(z_i), i = 1, \dots, n$ получили числа $z'_1, \dots, z'_n$ (где $r\_32(a)$ – остаток от деления числа a на 32), которые вновь заменили буквами согласно таблице. В результате получили вот что: **ЩЙИФБА**. Найдите исходное слово, если известно, что оно начинается на букву **Е**, и запишите его буквами в ВЕРХНЕМ регистре, то есть если у Вас получился ответ олимпиада, то его следует записать, как **ОЛИМПИАДА.**

А	Б	В	Г	Д	Е Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

6. Алиса и Боб играют в "угадай число". Чтобы никто им не помешал, они играют по следующим правилам. Алиса загадывает некоторое число $c \in \{0, \dots, 122\}$, вычисляет $m_a = r_{123}(c^7)$, где $r_{123}(a)$ – остаток от деления числа a на 123, и отправляет m_a Бобу. Боб, зная как получено m_a, пытается получить c, затем вычисляет $m_b = r_{123}(c^{29})$ и отправляет m_b Алисе. Алиса в

свою очередь проверяет и говорит, то ли число получил Боб. Узнайте, какое число загадала Алиса, если Боб угадал его и $m_a = 25$, а $m_b = 31$.

11 КЛАСС

1. Найдите наибольшее пятизначное число, которое в 138 раз больше квадрата суммы своих цифр.

2. На координатной прямой отмечены 9 точек с координатами 3; 21; −7; 10; 12; 29; −5; −8; 9. Найдите координату точки, сумма расстояний от которой до указанных 9 точек минимальна.

3. Ключом шифрсистемы служит таблица 4×4, в каждую ячейку которой записана одна из цифр 0, 1, 2 и 3. При этом должны делиться на 4 сумма цифр в каждой строке, сумма цифр в каждом столбце, а также суммы цифр на каждой из двух диагоналей, отмеченных пунктиром. На рисунке приведен один из возможных вариантов ключа. Сколько существует всего различных ключей?

2	0	1	1
3	1	0	0
1	1	2	0
2	2	1	3

4. Целое число $s \in \{0, \dots, 30\}$ может быть преобразовано следующим образом. Пусть, например, $s = 9$. Представим его в двоичной системе счисления *пятизначным* числом: $s = 9 = 01001_2$. Теперь выберем какое-нибудь целое число $c \geq 0$ и сдвинем получившуюся строку 01001 циклически на c позиций влево. Например, при $c = 1$ получится строка 10010, представляющая собой двоичную запись числа 18. Значит, сдвигом на одну позицию из числа 9 получается число 18; будем это записывать так: $9 \lll 1 = 18$. (Если 01001 сдвинуть влево на две позиции, то получится 00101, то есть $9 \lll 2 = 5$.) Итак, $s \lll c$ – это число, получившееся сдвигом числа s на c позиций влево.

Для зашифрования осмысленного слова выбирается секретный ключ – набор из 64 чисел $k_1, \dots, k_{32} \in \{0, \dots, 30\}$ и $c_1, \dots, c_{32} \in \{0,1,2,3\}$. Затем с каждой буквой слова (по отдельности) проделывается следующее. Букву заменяют числом a по таблице и последовательно вычисляют $a_1 = (a + k_1) \lll c_1,\ a_2 = (a_1 + k_2) \lll c_2, \dots, a_{32} = (a_{31} + k_{32}) \lll c_{32}$. Исходную букву затем заменяют на букву, соответствующую числу a_{32}. (Если в процессе вычислений получается число, превышающее 30, то оно заменяется остатком от деления на 31. Так, сумму $20 + 17$ сдедует заменить на 6.)

В результате зашифрования получился набор букв **СХОАГ**. Найдите исходное слово, если известно, что при зашифровании на этом ключе буква **Д** переходит в букву **Е**, а буква **Ю** – в **Ф**, и запишите его буквами в ВЕРХНЕМ регистре, то есть если у Вас получился ответ **олимпиада**, то его следует записать, как **ОЛИМПИАДА**.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

5. Для зашифрования осмысленного слова его буквы заменили числами $x_1, x_2, \dots, x_n$ по таблице. Затем выбирали четные натуральные числа p и q и для каждого числа x_i из соотношений $x_i = y_i + pz_i$, $z_i = y_i + qx_i$ нашли целые числа y_i и z_i. Потом по формулам $z_i' = r_{32}(z_i), i = 1, \dots, n$ получили числа $z_1', \dots, z_n'$ (где $r\_32(a)$ – остаток от деления числа a на 32), которые вновь заменили буквами согласно таблице. В результате получили вот что: **ОАЭШЯЪ**. Найдите исходное слово, если известно, что оно начинается на букву **К**, и запишите его буквами в ВЕРХНЕМ регистре, то есть если у Вас получился ответ олимпиада, то его следует записать, как **ОЛИМПИАДА.**

А	Б	В	Г	Д	Е Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

6. Алиса и Боб играют в "угадай число". Чтобы никто им не помешал, они играют по следующим правилам. Алиса загадывает некоторое число $c \in \{0, \dots, 122\}$, вычисляет $m_a = r_{123}(c^7)$, где $r_{123}(a)$ – остаток от деления числа a на 123, и отправляет m_a Бобу. Боб, зная как получено m_a, пытается получить c, затем вычисляет $m_b = r_{123}(c^{29})$ и отправляет m_b Алисе. Алиса в

свою очередь проверяет и говорит, то ли число получил Боб. Узнайте, какое число загадала Алиса, если Боб угадал его и $m_a = 25$, а $m_b = 31$.

ОТВЕТЫ

9 КЛАСС

1) 5589.
2) 8.
3) 16384.
4) 60.
5) ЕХИДНА.
6) 4.

10 КЛАСС

1) 5589.
2) 8.
3) 16384.
4) 60.
5) ЕХИДНА.
6) 4.

11 КЛАСС

1) 44712.
2) 9.
3) 16384.
4) ТВЕРЬ.
5) КАЗИНО.
6) 4.