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:

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

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. 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 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 $d_1 = 3, d_2 = 5$).