РЕШЕНИЯ ЗАДАЧ

Задача 1

Обозначим $\boldsymbol{x}$ – искомое число, $\boldsymbol{s}$ – сумма его цифр. Тогда $\boldsymbol{x = 3 \cdot 17 \cdot s^2}$. Следовательно, $\boldsymbol{x}$ делится нацело на 3. По признаку делимости на 3, число $\boldsymbol{s}$ делится на 3. Но тогда $\boldsymbol{x}$ делится на 9. По признаку делимости на 9, $\boldsymbol{s}$ делится на 9. Так как искомое число пятизначное, то для $\boldsymbol{s}$ возможны 5 вариантов: $\boldsymbol{s = 9, s = 18, s = 27, s = 36, s = 45}$. Для каждого $\boldsymbol{s}$, соответственно, находим: $\boldsymbol{x = 4131, x = 16524, x = 37179, x = 66096, x = 103275}$. Первое и последнее – не пятизначные, у четвертого сумма цифр не равна 36. Подходящие: $\boldsymbol{x = 16524, x = 37179}$.

ОТВЕТ: 37179.

Задача 2

Расположим числа в порядке возрастания: $-5; -3; 2; 7; \boldsymbol{8}; 9; 12; 19; 25$. Покажем, что выделенное среднее число **8** является искомым. Обозначим $s(y)$ - сумма расстояний от числа y до остальных чисел. Рассмотрим число $y = 8 + x$. Если $x \in (0; 1)$, то сумма расстояний от y до первых четырех чисел увеличится на $4x$, а до последних четырех –

уменьшится на $4x$ (по сравнению с числом 8), и при этом до самого числа 8 расстояние равно x, то есть $s(y) = s(8) + x$. Если $x = 1$, то есть $y = 9$, то сумма расстояний от y до всех чисел будет равна $s + 1$. Рассуждая аналогично при $x \in (1; +\infty)$, получим вывод: минимальное значение $s(y)$ достигается при $y = 8$. При отрицательных значениях x рассуждения ничем не отличаются.

ОТВЕТ: 8.

Задача 3

Указанную в условии таблицу 4×4, можно построить следующим образом: положим элементы верхнего левого угла размеров 3×3, произвольным образом, после чего заметим, что все оставшиеся элементы определяются однозначно из линейных (по модулю 3) соотношений для строк и столбцов (при этом элемент в правом нижнем углу будет равен сумме по модулю 3 всех остальных элементов квадрата). Плюс к этому имеем два линейных соотношения для элементов диагоналей. Таким образом, общее число независимого выбора переменных $a_{i,j}, i, j = 1,2,3$ равно 7. Следовательно, общее число ключей равно $3^7 = 2187$.

ОТВЕТ: 2187.

Задача 4

Покажем, что $(s \lll c) = r_{31}(s \cdot 2^c)$ (*)

Заметим, что достаточно доказать для $c = 1$.

Пусть $s = (s_4 s_3 s_2 s_1 s_0)_2$. Если $s_4 = 0$, то равенство (*) очевидно.

Если $s_4 = 1$, то $s = 16 + 2^3 \cdot s_3 + 2^2 \cdot s_2 + 2 \cdot s_1 + s_0$.

Тогда $r_{31}(s \cdot 2) = 2^4 \cdot s_3 + 2^3 \cdot s_2 + 2^2 \cdot s_1 + 2 \cdot s_0 + 1 = (s \lll c)$, и равенство (*) доказано.

Следовательно,

$a_1 = \big((a + k_1) \lll c_1\big) = r_{31}\big((a + k_1) \cdot 2^{c_1}\big) = r_{31}(a \cdot 2^{c_1} + k_1 \cdot 2^{c_1})$ (1)

То есть, на одном шаге шифрования - линейное преобразование числа a по правилу (1). Так как композиция линейных преобразований есть линейное преобразование, то $a_{32} = (a \cdot x + k)$, где x и k – неизвестные.

Воспользуемся тем, что на этом ключе буква **Ъ** переходит в букву **Ь**, а буква **П** – в **Е**:

$27 = (25 \cdot x + k)$, $5 = (14 \cdot x + k)$ (по модулю 31).

Вычитая из первого равенства второе, получим: $22 = 11 \cdot x$. Отсюда $x = 2$. Тогда $27 = (25 \cdot 2 + k)$ (по модулю 31) и, следовательно, $k = 8$. Окончательно получили:

$a_{32} = (a \cdot 2 + 8)$. Тогда $a = 2^{-1}(a_{32} - 8) = 16 \cdot a_{32} + 27$ (можно было сразу решать уравнение $a = (a_{32} \cdot x + k)$). Последовательно подставляя буквы шифрованного текста ЯГКЫНИ получим исходное слово МОСКВА.

ОТВЕТ: МОСКВА.

Задача 5

Рассмотрим произвольную букву открытого и шифрованного текстов. Для соответствующих им (по таблице) чисел x и z' выполняются равенства $x = y + pz$ и $z = y + qx$, при некотором y, p и q. При этом по условию $z' = r_{32}(z)$. Используя свойство сравнений по модулю целого числа, получим: $x - z' = pz' - qx (mod\ 32)$ или $x(1 + q) = z'(1 + p) (mod\ 32)$.

Для дальнейшего решения будем пользоваться следующим свойством: если наибольший общий делитель чисел a и n равен 1, то сравнение $x = y (mod\ n)$ равносильно $ax = ay (mod\ n)$. Используя условие задачи для первой буквы открытого и шифрованного текста, получим равенство $2(1 + q) = 6(1 + p) (mod\ 32)$.

Заметим, что сравнение $6t = 2 (mod\ 32)$ имеет 2 решения по модулю 32: $t = 11 (mod\ 32)$, $t = 27 (mod\ 32)$. Тогда получим, что $11 \cdot (1 + q) = (1 + p) (mod\ 32)$ или $27 \cdot (1 + q) =$

$(1+p)(mod\ 32)$ для каждого t. Таким образом, $x = 11z'(mod\ 32)$ или $x = 27z'(mod\ 32)$ соответственно.

Остается воспользоваться полученными соотношениями для остальных букв. Осмысленное слово получается только при втором варианте. А значит, исходное слово **ВЕКТОР**.

ОТВЕТ: ВЕКТОР.

Задача 6

Заметим, что для всех $\boldsymbol{x}$ вектор $h(\boldsymbol{x})$ содержит четное число единиц, так как

$$(x_1 \oplus x_{n-1}) \oplus (x_2 \oplus x_n) \oplus (x_2 \oplus x_3) \oplus (x_3 \oplus x_4) \oplus \dots, \oplus (x_{n-2} \oplus x_{n-1}) \oplus (x_1 \oplus x_n) = 0.$$

Значит в рассматриваемой последовательности $\boldsymbol{x}, h(\boldsymbol{x}), h^{(2)}(\boldsymbol{x}), \dots, h^{(k)}(\boldsymbol{x})$ (1)

все векторы, начиная со второго, имеют четное количество единиц. Количество всех векторов, имеющих четное количество единиц, равно 2^{n-1}. Поэтому претендентом на самое большое количество различных векторов является последовательность (1), начинающаяся с вектора, содержащего нечетное количество единиц и продолжающаяся всеми векторами с четным количеством единиц. Количество векторов в такой последовательности будет $1 + 2^{n-1}$ Таким образом $k \le 2^{n-1}$. Для получения оценки $k \le 2^{n-1} - 1$ рассмотрим отдельно случай когда среди векторов последовательности (1) нет нулевого вектора $(0,0,\dots,0)$ и когда он есть. Если в последовательности (1) нет вектора $(0,0,\dots,0)$, то она содержит не более $1 + (2^{n-1} - 1) = 2^{n-1}$ векторов и $k \le 2^{n-1} - 1$. Пусть теперь последовательность (1) содержит вектор $(0,0,\dots,0)$. Рассмотрим два случая.

1) Если n - нечетное число, то $h(0,0,\dots,0) = h(1,1,\dots,1) = (0,0,\dots,0)$ и других векторов, переходящих в нулевой нет. При этом не существует векторов $\boldsymbol{z}$ таких, что $h(\boldsymbol{z}) = (1,1,\dots,1)$ Таким образом в этом случае последовательность (1) содержит максимум два вектора и $k \le 2^{n-1} - 1$.

2) Если n - четное число, то $h(0,0,\dots,0) = h(1,1,\dots,1) = (0,0,\dots,0)$ и найдутся два вектора

$$\boldsymbol{a} = (0,0,1,0,1,\dots,0,1,1) \text{ и } \boldsymbol{b} = (1,1,0,1,0,1,\dots,0,1,0,0)$$

содержащие четное число единиц такие, что $h(\boldsymbol{a}) = h(\boldsymbol{b}) = (1,1,\dots,1)$. Последовательность (1) не может содержать одновременно векторы $\boldsymbol{a}$ и $\boldsymbol{b}$, поэтому в этом случае она содержит не более $1 + (2^{n-1} - 1) = 2^{n-1}$ векторов и $k \le 2^{n-1} - 1$.