11 класс XXX Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии

1 вариант

1. Найдите наибольшее пятизначное число, которое в 51 раз больше квадрата суммы своих цифр. Решение обоснуйте.

Решение: Обозначим $\boldsymbol{x}$ – искомое число, $\boldsymbol{s}$ – сумма его цифр. Тогда $\boldsymbol{x} = \mathbf{3} \cdot \mathbf{17} \cdot \boldsymbol{s}^2$. 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: $\boldsymbol{s} = \mathbf{9}$, $\boldsymbol{s} = \mathbf{18}$, $\boldsymbol{s} = \mathbf{27}$, $\boldsymbol{s} = \mathbf{36}$, $\boldsymbol{s} = \mathbf{45}$. Для каждого $\boldsymbol{s}$, соответственно, находим: $\boldsymbol{x} = \mathbf{4131}$, $\boldsymbol{x} = \mathbf{16524}$, $\boldsymbol{x} = \mathbf{37179}$, $\boldsymbol{x} = \mathbf{66096}$, $\boldsymbol{x} = \mathbf{103275}$. Первое и последнее – не пятизначные, у четвертого сумма цифр не равна 36. Подходящие: $\boldsymbol{x} = \mathbf{16524}$, $\boldsymbol{x} = \mathbf{37179}$.

Ответ: 37179.

2. На координатной прямой отмечены 9 точек с координатами $2; 25; 7; -3; 12; 19; -5; 8; 9$. Найдите координату точки, сумма расстояний от которой до указанных 9 точек минимальна. Ответ обоснуйте.

Решение: Расположим числа в порядке возрастания: −5; −3; 2; 7; **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**.**

3. Ключом шифрсистемы служит таблица 4×4, в каждую ячейку которой записана одна из цифр 0, 1, 2. При этом должны делиться на 3 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?

1	1	2	2
2	1	1	2
0	0	1	2
0	1	2	0

Решение: 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.

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 **ЯГКЫНИ**. Найдите исходное слово, если известно, что при зашифровании на этом ключе буква **Ъ** переходит в букву **Ь**, а буква **П** – в **Е**.

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

Решение: 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,

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

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.

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: **ЖЯЮЦКР**. Найдите исходное слово, если известно, что оно начинается на букву **В**.

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

Решение: 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.

6. Устройство принимает на вход и выдает на выход наборы из n битов (причем $n \geq 4$). Поданный на вход набор $\boldsymbol{x} = (x_1, \dots, x_n)$ преобразуется в выходной набор $h(\boldsymbol{x}) = (x_1 \oplus x_{n-1}, x_2 \oplus x_n, x_2 \oplus x_3, x_3 \oplus x_4, \dots, x_{n-2} \oplus x_{n-1}, x_1 \oplus x_n)$, где $\oplus$ – стандартная операция сложения битов: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Подав теперь этот набор $h(\boldsymbol{x})$ на вход, получим на выходе набор $h(h(\boldsymbol{x})) = h^{(2)}(\boldsymbol{x})$, который вновь подадим на вход и получим $h^{(3)}(\boldsymbol{x})$ и т.д. Докажите, что если все наборы $\boldsymbol{x}$, $h(\boldsymbol{x})$, $h^{(2)}(\boldsymbol{x})$, … , $h^{(k)}(\boldsymbol{x})$ оказались различными, то $k \leq 2^{n-1} - 1$.

Решение:

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 $\boldsymbol{x}$, $h(\boldsymbol{x})$, $h^{(2)}(\boldsymbol{x})$, … , $h^{(k)}(\boldsymbol{x})$ (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 $k \leq 2^{n-1}$. Для получения оценки $k \leq 2^{n-1} - 1$ рассмотрим отдельно случай когда среди векторов последовательности (1) нет нулевого вектора (0,0, … ,0) и когда он есть. Если в последовательности (1) нет вектора (0,0, … ,0), то она содержит не более $1 + (2^{n-1} - 1) = 2^{n-1}$ векторов и $k \leq 2^{n-1} - 1$. Пусть теперь последовательность (1) содержит вектор (0,0, … ,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 $k \leq 2^{n-1} - 1$.

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

$\boldsymbol{a} = (0,0,1,0,1, \dots ,0,1,1)$ 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 $k \leq 2^{n-1} - 1$.