Условия и решения задач XXIV МЕЖРЕГИОНАЛЬНОЙ ОЛИМПИАДЫ ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

2014-2015 учебный год

Оглавление

9 классы 1
УСЛОВИЯ ЗАДАЧ (очный этап) 1
РЕШЕНИЯ ЗАДАЧ (очный этап) 2
10 классы 6
УСЛОВИЯ ЗАДАЧ (очный этап) 6
РЕШЕНИЯ ЗАДАЧ (очный этап) 7
11 классы 11
УСЛОВИЯ ЗАДАЧ (очный этап) 11
РЕШЕНИЯ ЗАДАЧ (очный этап) 12
9, 10, 11 классы 16
УСЛОВИЯ И ОТВЕТЫ (отборочный этап) 16

8-9 класс XXIV МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

(сайт олимпиады www.cryptolymp.ru) 30.11.2014

1 вариант

1. (12 баллов) Женя решила поделиться забавным палиндромом с Ксюшей. Но, чтобы никто о нем больше не узнал, Женя удалила пробелы между словами, перемешала буквы и получила вот что: **алжбанкнаабанжалкаан**. Помогите Ксюше прочитать палиндром (палиндром – текст, читающийся одинаково в обоих направлениях. Например: «А роза упала на лапу Азора»).

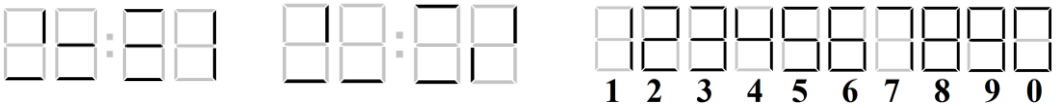
2. (15 баллов) Линия связи состоит из 4-х каналов, пронумерованных числами 1,2,3,4. Для передачи по линии сигнала на каждый канал подается свой импульс, величина которого может быть 7, 9 или 11 единиц. В каждом канале есть усилитель, который увеличивает поданный импульс в 3^{i-1} раз, где i - номер канала. На выходе линии формируется сигнал, который равен остатку от деления на 81 суммы полученных по каналам импульсов. Какие импульсы необходимо подать на каналы, чтобы получить сигнал величиной 6 единиц?

3. (12 баллов) Дана последовательность из 11 чисел $x_1, x_2, \ldots, x_{11}$. В ней каждое число x_i равно либо 0, либо 1. Из этой последовательности получили последовательность из 10 чисел $y_1, y_2, \ldots, y_{10}$ по формулам: $y_1 = x_1 \cdot x_2$, $y_2 = x_2 \cdot x_3, \ldots, y_{10} = x_{10} \cdot x_{11}$. Определите, какие из четырёх приведённых ниже последовательностей $y_1, y_2, \ldots, y_{10}$ могли быть получены указанным способом, а какие нет.

(I): 0011001100; (II): 0001111101; (III): 1000111000; (IV): 1100110110.

Ответ обоснуйте.

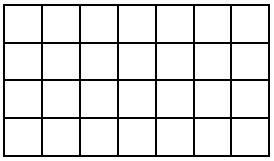
4. (15 баллов) Имеются сломанные электронные часы (они идут точно, но некоторые элементы табло перегорели). Показания часов в некоторый момент времени приведены на рисунке (а), а спустя ровно 1 час 8 минут – на рисунке (б). Определите время, которое на рисунке (а) показывали бы исправные часы. Отображение цифр на исправном табло показано на рисунке (в).



(а) **(б)** **(в)**

5. (24 балла) Для доступа на сайт Алиса вводит в строке браузера его имя. Затем это имя по сети отправляется на специальный DNS-сервер, который по имени сайта определяет его IP-адрес – набор из четырех целых чисел $x_1.x_2.x_3.x_4$, причем $0 < x_i < 255$, $i = 1,2,3,4$. Этот IP-адрес сервер отправляет Алисе. Чтобы защитить передаваемый адрес от подделки, сервер вместе с адресом передает число s, которое он вычисляет так: $s = r_{141}((h_4)^d)$, где d – секретное натуральное число, известное только Алисе и серверу, а $r_{141}(x)$ – остаток от деления числа x на 141; число h_4 находится последовательным применением правила $h_i = r_{141}(h_{i-1} \cdot x_i)$, где i принимает значения $1,2,3,4$, а $h_0 = 1$. Получив IP-адрес, Алиса также вычисляет s и, если оно совпадает с присланным сервером значением, Алиса признает этот IP-адрес подлинным. Злоумышленник узнал, что на запрос Алисы сервер ответил: 10.10.1.1 при $s = 115$. Он хочет от имени сервера отправить Алисе ложный (отличающийся от исходного) адрес вида 10.10.a.b и такое число s', чтобы этот адрес Алиса признала подлинным. Найдите хотя бы одну такую тройку a,b,s' с условием $s' \geq 1$.

6. (22 балла) Докажите, что *нельзя обойти* все клетки изображенной на рисунке фигуры, побывав в каждой ровно один раз. Начинать движение можно из любой клетки. Разрешается двигаться на *одну клетку* только вправо, влево, вверх или вниз. Движение по диагонали запрещено.



8-9 класс XXIV МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ
(сайт олимпиады www.cryptolymp.ru) **30.11.2014**

1 вариант

1. Женя решила поделиться забавным палиндромом с Ксюшей. Но, чтобы никто о нем больше не узнал, Женя удалила пробелы между словами, перемешала буквы и получила вот что: **алжбанкнаабанжалкаан**. Помогите Ксюше прочитать палиндром (палиндром – текст, читающийся одинаково в обоих направлениях. Например: «А роза упала на лапу Азора»).
Решение: Ответ: нажал кабан на баклажан

2. Линия связи состоит из 4-х каналов, пронумерованных числами 1,2,3,4. Для передачи по линии сигнала на каждый канал подается свой импульс, величина которого может быть 7, 9 или 11 единиц. В каждом канале есть усилитель, который увеличивает поданный импульс в 3^{i-1} раз, где i - номер канала. На выходе линии формируется сигнал, который равен остатку от деления на 81 суммы полученных по каналам импульсов. Какие импульсы необходимо подать на каналы, чтобы получить сигнал, величиной 6 единиц?
Решение:
Заметим, что числа 7, 9, 11, равные импульсам, которые передаются по каналам, дают разные и в точности все возможные остатки при делении на 3.
Пусть $a \in \mathbb{Z}$ - значение, равное сумме импульсов, переданных по четырем каналам. Тогда по условию $r_{81}(a) = 6$, где $r_{81}(a)$ – остаток от деления a на 81. Справедливо представление

$$a = a_1 + 3a_2 + 9a_3 + 27a_4,$$

где $a_i \in \{7, 9, 11\},\ i \in \{1, 2, 3, 4\}$. В то же время из условия задачи

$$a = 6 + 81q, \qquad q \in \mathbb{Z}.$$

Но тогда, нетрудно понять, что

$$r_3(a_1) = r_3(a) = r_3(6 + 81q) = r_3(6) = 0.$$

Откуда следует, что число a_1 может равняться только 9, поскольку только оно дает остаток 0 при делении на число 3. Получим

$$a - 9 = 3a_2 + 9a_3 + 27a_4 = -3 + 81q,$$
$$a_2 + 3a_3 + 9a_4 = -1 + 27q.$$

Аналогично предыдущим рассуждениям имеем:

$$r_3(a_2) = r_3(a_2 + 3a_3 + 9a_4) = r_3(-1 + 27q) = r_3(-1) = 2.$$

Отсюда находим, что $a_2 = 11$. Далее получим равенства:

$$3a_3 + 9a_4 = -1 + 27q - 11 = -12 + 27q,$$
$$a_3 + 3a_4 = -4 + 9q.$$

Также аналогично найдем

$$r_3(a_3) = r_3(a_3 + 3a_4) = r_3(-4 + 9q) = 2.$$

Следовательно, $a_3 = 11$. И, наконец, вычислим:

$$3a_4 = -4 + 9q - 11 = -15 + 9q,$$
$$a_4 = -5 + 3q.$$

Придем к равенствами

$$r_3(a_4) = r_3(-5 + 3q) = r_3(-5) = 1$$

и $a_4 = 7$. Таким образом, искомый набор импульсов на входе физической линии есть (9, 11, 11, 7).
Ответ: 9, 11, 11, 7.

3. Дана последовательность из 11 чисел $x_1, x_2, \ldots, x_{11}$. В ней каждое число x_i равно либо 0, либо 1. Из этой последовательности получили последовательность из 10 чисел $y_1, y_2, \ldots, y_{10}$ по формулам: $y_1 = x_1 \cdot x_2, y_2 = x_2 \cdot x_3, \ldots, y_{10} = x_{10} \cdot x_{11}$. Определите, какие из четырёх приведённых ниже последовательностей $y_1, y_2, \ldots, y_{10}$ могли быть получены указанным способом, а какие нет.
(I): 0011001100; (II): 0001111101; (III): 1000111000; (IV): 1100110110.
Ответ обоснуйте.

Решение: Для всевозможных последовательностей из четырех символов x_1, x_2, x_3, x_4 найдем им соответствующие последовательности y_1, y_2, y_3. Результаты приведены в таблице. Видим, что выходная последовательность y_i не может содержать фрагмент 101 (назовем его *запретом*).

x_1, x_2, x_3, x_4	y_1, y_2, y_3
0, 0, 0, 0	0, 0, 0
0, 0, 0, 1	0, 0, 0
0, 0, 1, 0	0, 0, 0
0, 0, 1, 1	0, 0, 1
0, 1, 0, 0	0, 0, 0
0, 1, 0, 1	0, 0, 0
0, 1, 1, 0	0, 1, 0
0, 1, 1, 1	0, 1, 1
1, 0, 0, 0	0, 0, 0
1, 0, 0, 1	0, 0, 0
1, 0, 1, 0	0, 0, 0
1, 0, 1, 1	0, 0, 1
1, 1, 0, 0	1, 0, 0
1, 1, 0, 1	1, 0, 0
1, 1, 1, 0	1, 1, 0
1, 1, 1, 1	1, 1, 1

Покажем теперь, что любая последовательность, не содержащая 101, может быть получена при некоторой входной последовательности x_i. Предположим, что последовательность $y_1,\dots,y_k$ нами уже получена с помощью некоторой последовательности $x_1,\dots,x_{k+1}, k>2.$ Покажем, что мы сможем тогда получить и последовательность $y_1,\dots,y_{k+1}$ (конечно, если она не содержит 101).

Если $y_{k+1}=0,$ то последовательность $y_1,\dots,y_k,0$ можно получить, добавив 0 к входной последовательности, из которой получена последовательность $y_1,\dots,y_k$. Если $y_{k+1}=1,$ то возможны три случая:

(1) последовательность $y_1,\dots,y_{k-2},0,0,1$

(2) последовательность $y_1,\dots,y_{k-2},0,1,1$

(3) последовательность $y_1,\dots,y_{k-2},1,1,1$

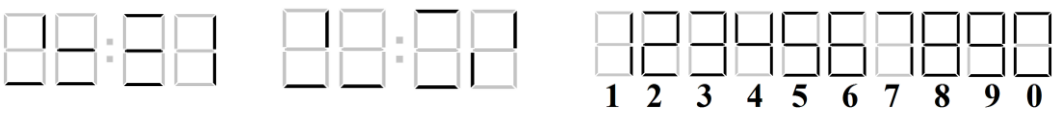
Случай (1). Если последовательность $y_1,\dots,y_{k-2},0,0$ получена с помощью входа $x_1,\dots,x_{k+1}$, то она же может быть получена и с помощью входа $x_1,\dots,x_{k-1},0,1$. Тогда требуемая последовательность $y_1,\dots,y_{k-2},0,0,1$ получается с помощью входа $x_1,\dots,x_{k-1},0,1,1$

Случай (2) Если последовательность $y_1,\dots,y_{k-2},0,1$ получена с помощью входа $x_1,\dots,x_{k+1}$, то $x_k=x_{k+1}=1$. Тогда требуемая последовательность $y_1,\dots,y_{k-2},0,1,1$ получается с помощью входа $x_1,\dots,x_{k-1},1,1,1$

Случай (3) рассматривается аналогично случаю (2).

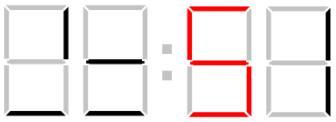
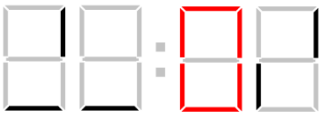
ОТВЕТ: запрет 101, не содержат запрета последовательности (I) и (III).

4. Имеются сломанные электронные часы (они идут точно, но некоторые элементы табло перегорели). Показания часов в некоторый момент времени приведены на рисунке (а), а спустя ровно 1 час 8 минут – на рисунке (б). Определите время, которое на рисунке (а) показывали бы исправные часы. Отображение цифр на исправном табло показано на рисунке (в).



(а) (б) (в)

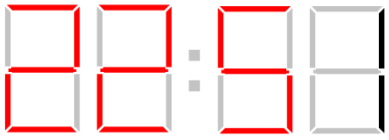
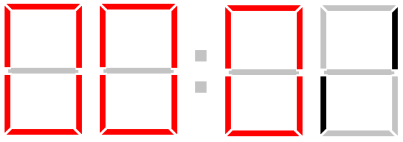
Решение: Так как на табло часы, то получаем ограничения на цифры на первой и третьейпозиции слева. Первая цифра это 0, 1 или 2. Третья цифра это 0, 1, 2, 3, 4, 5.
Рассмотрим третью слева позицию на часах. На рисунке а) подходят цифры 2,3,5. На рисунке б) подходят цифры 2,3,5,0. Получаем возможные пары:
(2,2) , (2,3) , (3,3) , (5,5) ,(5,0). Так как на рисунке а) горит средний горизонтальный элемент, а на рисунке б) не горит, то остается только пара (5,0).

а)  б) 

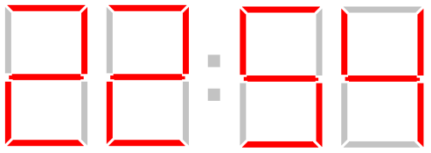
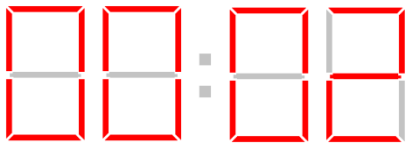
Теперь рассмотрим вторую слева позицию на часах. На рисунке а) подходят цифры: 2,3,5,6,8,9. На рисунке б) подходят цифры: 2,3,5,6,8,9,0. По условию сказано, что прошло ровно 1 час и 8 минут. Т.е, вторая позиция слева могла измениться либо на 1 либо на 2. Тогда подходят пары: (2,0) , (3,0) , (8,0) , (9,0). Так как в третьей слева цифре произошел переход через десяток, значит, во второй позиции цифры отличаются на 2. Тогда остаются пары: (2,0), (8,0).

Теперь рассмотрим первую слева позицию на часах, отвечающую за десятки часов.На рисунках обоих рисунках подходят цифры 0, 2. Возможные пары получаются: (0,0) , (2,2) , (2,0). Ни под одну эту пару не походит пара (8,0) из второй слева позиции часов.

Таким образом, получаем:

а)  б) 

Осталось определить последнюю пару цифр. На рисунке а) подходят: 0,1,3,4,7,8,9. На рисунке б): 2,8,0. С учетом разницы в 8 минут остаются пары: (0,8), (4,2). Пара (0,8) не подходит, так как должен бы гореть правый нижний элемент на рисунке б). Остается только пара (4,2).

а)  б) 

Ответ: 22:54

5. Для доступа на сайт Алиса вводит в строке браузера его имя. Затем это имя по сети отправляется на специальный DNS-сервер, который по имени сайта определяет его IP-адрес – набор из четырех целых чисел $x_1.x_2.x_3.x_4$, причем $0 < x_i < 255,\ i = 1,2,3,4.$ Этот IP-адрес сервер отправляет Алисе. Чтобы защитить передаваемый адрес от подделки, сервер вместе с адресом передает число s, которое он вычисляет так: $s = r_{141}((h_4)^d)$, где d – секретное натуральное число, известное только Алисе и серверу, а $r_{141}(x)$ – остаток от деления числа *x* на 141; число h_4 находится последовательным применением правила $h_i = r_{141}(h_{i-1} \cdot x_i)$, где i принимает значения $1,2,3,4,$ а $h_0 = 1$. Получив IP-адрес, Алиса также вычисляет *s* и, если оно совпадает с присланным сервером значением, Алиса признает этот IP-адрес подлинным. Злоумышленник узнал, что на запрос Алисы сервер ответил: 10.10.1.1 при $s = 115$. Он хочет от имени сервера отправить Алисе ложный (отличающийся от исходного) адрес вида 10.10.*a.b* и такое число *s′*, чтобы этот адрес Алиса признала подлинным. Найдите хотя бы одну такую тройку *a,b, s′* с условием $s' \geq 1.$

Решение:

Заметим, что факторизовывать число $N = 141$ и находить значение d нет необходимости – достаточно найти пару x_3', x_4' такую, что $x_3' \neq x_3,\ x_4' \neq x_4$ и описанное преобразование сжатия (в основе которого лежит итеративная функция h) от значений x_1, x_2, x_3', x_4' дает тоже значение h_4. То есть, попробуем найти коллизию сжимающего преобразования, тогда и значение s от IP-адресов $x_1.x_2.x_3.x_4$ и $x_1.x_2.x_3'.x_4'$ будет одинаковым.

Замечаем, что так как $x_3 = 1,\ x_4 = 1$, то $h_4 = r_N(h_2)$. Тогда при условии сохранения прежних компонент $x_1.x_2$, для искомого IP-адреса получаем, что необходимо найти такие x_3', x_4' и параметр h_3', которые удовлетворяют системе:

$\begin{cases} h_3' = r_N(h_2 \cdot x_3') \\ h_4 = r_N(h_3' \cdot x_4') \end{cases}$, из которой с учетом того, что $h_4 = r_N(h_2)$, следует, что $r_N(x_3' \cdot x_4') = 1$, то есть $x_3' \cdot x_4' = 1 + t \cdot N$, t - натуральное. Тогда при $t = 1$ имеем: $x_3' \cdot x_4' = 142 = 2 \cdot 5 \cdot 17$, откуда получаем следующий возможный вариант для пары (x_3', x_4'): (2, 71).

Ответ, возможный вариант: 10.10.2.71 с исходным значением s.

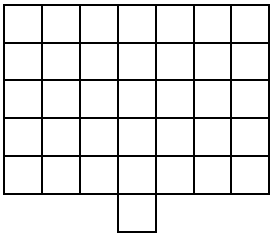
Замечание

Это не единственные ответы, так как могут быть получены ответы и при $t = 2$ и т.д.

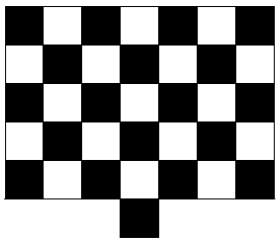
Дополнительная информация для проверки

p	q	$\varphi(N)$	d	h_1	h_2	h_3	h_4
3	47	$92 = 2^2 \cdot 23$	5	10	100	100	100

6. Докажите, что *нельзя обойти* все клетки изображенной на рисунке фигуры, побывав в каждой ровно один раз. Начинать движение можно из любой клетки. Разрешается двигаться на *одну клетку* только вправо, влево, вверх или вниз. Движение по диагонали запрещено.

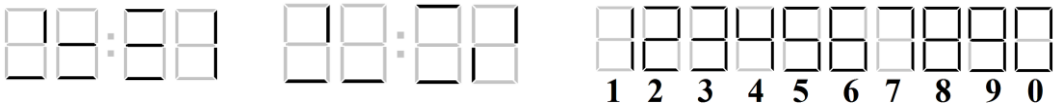


Решение: Раскрасим клетки как на рисунке. Делая один шаг, мы из черной клетки попадаем в белую и наоборот. Значит, если бы искомый обход был возможен, то клеток одного цвета было бы от силы на единицу больше, чем клеток другого цвета. Но черных клеток на две больше, чем белых. Поэтому обход невозможен.



1 вариант

1. (12 баллов) Имеются сломанные электронные часы (они идут точно, но некоторые элементы табло перегорели). Показания часов в некоторый момент времени приведены на рисунке (а), а спустя ровно 1 час 8 минут – на рисунке (б). Определите время, которое на рисунке (а) показывали бы исправные часы. Отображение цифр на исправном табло показано на рисунке (в).



(а) **(б)** **(в)**

2. (12 баллов) Женя решила поделиться забавным палиндромом с Ксюшей. Но, чтобы никто о нем больше не узнал, Женя удалила пробелы между словами, перемешала буквы и получила вот что: **колнёошакапеллашёланп**. Помогите Ксюше прочитать палиндром (палиндром – текст, читающийся одинаково в обоих направлениях. Например: «А роза упала на лапу Азора»).

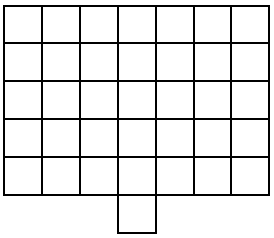
3. (12 баллов) Линия связи состоит из 4-х каналов, пронумерованных числами 1,2,3,4. Для передачи по линии сигнала на каждый канал подается свой импульс, величина которого может быть 7, 9 или 11 единиц. В каждом канале есть усилитель, который увеличивает поданный импульс в 3^{i-1} раз, где i - номер канала. На выходе линии формируется сигнал, который равен остатку от деления на 81 суммы полученных по каналам импульсов. Какие импульсы необходимо подать на каналы, чтобы получить сигнал величиной 6 единиц?

4. (24 балла) Из последовательности $x_1, x_2, \ldots, x_n, x_i \in \{0,1\}$ получена последовательность $y_1, y_2, \ldots, y_{n-1}$ по правилу: $y_i = x_i \cdot x_{i+1}, i = 1, \ldots, n-1$. Определите, какие из четырёх приведённых ниже последовательностей $y_1, y_2, \ldots, y_{10}$ могли быть получены указанным способом, а какие нет.

(I): 0011001100; (II): 0001111101; (III): 1000111000; (IV): 1100110110.

Сколько последовательностей $y_1, y_2, \ldots, y_6$ может быть получено (при выборе всевозможных $x_1, x_2, \ldots, x_7, x_i \in \{0,1\}$)? Ответ обоснуйте.

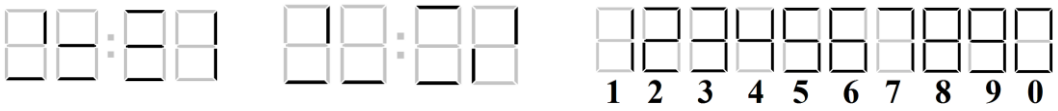
5. (16 баллов) Докажите, что *нельзя обойти* все клетки изображенной на рисунке фигуры, побывав в каждой ровно один раз. Начинать движение можно из любой клетки. Разрешается двигаться на *одну клетку* только вправо, влево, вверх или вниз. Движение по диагонали запрещено.



6. (24 балла) Для доступа на сайт Алиса вводит в строке браузера его имя. Затем это имя по сети отправляется на специальный DNS-сервер, который по имени сайта определяет его IP-адрес – набор из четырех целых чисел $x_1.x_2.x_3.x_4$, причем $0 < x_i < 255$, $i = 1,2,3,4$. Этот IP-адрес сервер отправляет Алисе. Чтобы защитить передаваемый адрес от подделки, сервер вместе с адресом передает число s, которое он вычисляет так: $s = r_{305}((h_4)^d)$, где d – секретное натуральное число, известное только Алисе и серверу, а $r_{305}(x)$ – остаток от деления числа x на 305; число h_4 находится последовательным применением правила $h_i = r_{305}((h_{i-1})^2 \cdot x_i)$, где i принимает значения $1,2,3,4$, а $h_0 = 1$. Получив IP-адрес, Алиса также вычисляет s и, если оно совпадает с присланным сервером значением, Алиса признает этот IP-адрес подлинным. Злоумышленник узнал, что на запрос Алисы сервер ответил: 10.11.1.1 при $s = 15$. Он хочет от имени сервера отправить Алисе ложный (отличающийся от исходного) адрес вида 10.11.*a.b* и такое число *s'*, чтобы этот адрес Алиса признала подлинным. Найдите хотя бы одну такую тройку *a,b, s'* с условием $s' \geq 1$.

1 вариант

1. Имеются сломанные электронные часы (они идут точно, но некоторые элементы табло перегорели). Показания часов в некоторый момент времени приведены на рисунке (а), а спустя ровно 1 час 8 минут – на рисунке (б). Определите время, которое на рисунке (а) показывали бы исправные часы. Отображение цифр на исправном табло показано на рисунке (в).



(а) **(б)** **(в)**

Решение: Так как на табло часы, то получаем ограничения на цифры на первой и третьейпозиции слева. Первая цифра это 0, 1 или 2. Третья цифра это 0, 1, 2, 3, 4, 5.

Рассмотрим третью слева позицию на часах. На рисунке а) подходят цифры 2,3,5. На рисунке б) подходят цифры 2,3,5,0. Получаем возможные пары:
(2,2) , (2,3) , (3,3) , (5,5) ,(5,0). Так как на рисунке а) горит средний горизонтальный элемент, а на рисунке б) не горит, то остается только пара (5,0).

Теперь рассмотрим вторую слева позицию на часах. На рисунке а) подходят цифры: 2,3,5,6,8,9. На рисунке б) подходят цифры: 2,3,5,6,8,9,0. По условию сказано, что прошло ровно 1 час и 8 минут. Т.е, вторая позиция слева могла измениться либо на 1 либо на 2. Тогда подходят пары: (2,0) , (3,0) , (8,0) , (9,0). Так как в третьей слева цифре произошел переход через десяток, значит, во второй позиции цифры отличаются на 2. Тогда остаются пары: (2,0), (8,0).
Теперь рассмотрим первую слева позицию на часах, отвечающую за десятки часов.На рисунках обоих рисунках подходят цифры 0, 2. Возможные пары получаются: (0,0) , (2,2) , (2,0). Ни под одну эту пару не походит пара (8,0) из второй слева позиции часов.
Таким образом, получаем:

Осталось определить последнюю пару цифр. На рисунке а) подходят: 0,1,3,4,7,8,9. На рисунке б): 2,8,0. С учетом разницы в 8 минут остаются пары: (0,8), (4,2). Пара (0,8) не подходит, так как должен бы гореть правый нижний элемент на рисунке б). Остается только пара (4,2).

Ответ: 22:54

2. Женя решила поделиться забавным палиндромом с Ксюшей. Но, чтобы никто о нем больше не узнал, Женя удалила пробелы между словами, перемешала буквы и получила вот что:

колнёошакапеллашёланп. Помогите Ксюше прочитать палиндром (палиндром – текст, читающийся одинаково в обоих направлениях. Например: «А роза упала на лапу Азора»).

Решение: Ответ: лёша на полке клопа нашёл

3. Линия связи состоит из 4-х каналов, пронумерованных числами 1,2,3,4. Для передачи по линии сигнала на каждый канал подается свой импульс, величина которого может быть 7, 9 или 11 единиц. В каждом канале есть усилитель, который увеличивает поданный импульс в 3^{i-1} раз, где i - номер канала. На выходе линии формируется сигнал, который равен остатку от деления на 81 суммы полученных по каналам импульсов. Какие импульсы необходимо подать на каналы, чтобы получить сигнал, величиной 6 единиц?

Решение: Заметим, что числа 7, 9, 11, равные импульсам, которые передаются по каналам, дают разные и в точности все возможные остатки при делении на 3.

Пусть $a \in \mathbb{Z}$ - значение, равное сумме импульсов, переданных по четырем каналам. Тогда по условию $r_{81}(a) = 6$, где $r_{81}(a)$ – остаток от деления a на 81. Справедливо представление

$$a = a_1 + 3a_2 + 9a_3 + 27a_4,$$

где $a_i \in \{7, 9, 11\},\ i \in \{1, 2, 3, 4\}$. В то же время из условия задачи

$$a = 6 + 81q, \qquad q \in \mathbb{Z}.$$

Но тогда, нетрудно понять, что

$$r_3(a_1) = r_3(a) = r_3(6 + 81q) = r_3(6) = 0.$$

Откуда следует, что число a_1 может равняться только 9, поскольку только оно дает остаток 0 при делении на число 3. Получим

$$a - 9 = 3a_2 + 9a_3 + 27a_4 = -3 + 81q,$$
$$a_2 + 3a_3 + 9a_4 = -1 + 27q.$$

Аналогично предыдущим рассуждениям имеем:

$$r_3(a_2) = r_3(a_2 + 3a_3 + 9a_4) = r_3(-1 + 27q) = r_3(-1) = 2.$$

Отсюда находим, что $a_2 = 11$. Далее получим равенства:

$$3a_3 + 9a_4 = -1 + 27q - 11 = -12 + 27q,$$
$$a_3 + 3a_4 = -4 + 9q.$$

Также аналогично найдем

$$r_3(a_3) = r_3(a_3 + 3a_4) = r_3(-4 + 9q) = 2.$$

Следовательно, $a_3 = 11$. И, наконец, вычислим:

$$3a_4 = -4 + 9q - 11 = -15 + 9q,$$
$$a_4 = -5 + 3q.$$

Придем к равенствами

$$r_3(a_4) = r_3(-5 + 3q) = r_3(-5) = 1$$

и $a_4 = 7$. Таким образом, искомый набор импульсов на входе физической линии есть (9, 11, 11, 7). **Ответ**: 9, 11, 11, 7.

4. Из последовательности $x_1, x_2, \ldots, x_n, x_i \in \{0,1\}$ получена последовательность $y_1, y_2, \ldots, y_{n-1}$ по правилу: $y_i = x_i \cdot x_{i+1}, i = 1, \ldots, n-1$. Определите, какие из четырёх приведённых ниже последовательностей $y_1, y_2, \ldots, y_{10}$ могли быть получены указанным способом, а какие нет.

(I): 0011001100; (II): 0001111101; (III): 1000111000; (IV): 1100110110.

Сколько последовательностей $y_1, y_2, \ldots, y_6$ может быть получено (при выборе всевозможных $x_1, x_2, \ldots, x_7, x_i \in \{0,1\}$)? Ответ обоснуйте.

Решение: Для всевозможных последовательностей из четырех символов x_1, x_2, x_3, x_4 найдем им соответствующие последовательности y_1, y_2, y_3. Результаты приведены в таблице. Видим, что выходная последовательность y_i не может содержать фрагмент 101 (назовем его *запретом*).

x_1, x_2, x_3, x_4	y_1, y_2, y_3
0, 0, 0, 0	0, 0, 0
0, 0, 0, 1	0, 0, 0
0, 0, 1, 0	0, 0, 0
0, 0, 1, 1	0, 0, 1
0, 1, 0, 0	0, 0, 0
0, 1, 0, 1	0, 0, 0
0, 1, 1, 0	0, 1, 0
0, 1, 1, 1	0, 1, 1
1, 0, 0, 0	0, 0, 0
1, 0, 0, 1	0, 0, 0
1, 0, 1, 0	0, 0, 0
1, 0, 1, 1	0, 0, 1
1, 1, 0, 0	1, 0, 0
1, 1, 0, 1	1, 0, 0
1, 1, 1, 0	1, 1, 0
1, 1, 1, 1	1, 1, 1

Покажем теперь, что любая последовательность, не содержащая 101, может быть получена при некоторой входной последовательности x_i. Предположим, что последовательность $y_1,...,y_k$ нами уже получена с помощью некоторой последовательности $x_1,...,x_{k+1}, k>2.$ Покажем, что мы сможем тогда получить и последовательность $y_1,...,y_{k+1}$ (конечно, если она не содержит 101).

Если $y_{k+1}=0,$ то последовательность $y_1,...,y_k,0$ можно получить, добавив 0 к входной последовательности, из которой получена последовательность $y_1,...,y_k$. Если $y_{k+1}=1,$ то возможны три случая:

(1) последовательность $y_1,...,y_{k-2},0,0,1$

(2) последовательность $y_1,...,y_{k-2},0,1,1$

(3) последовательность $y_1,...,y_{k-2},1,1,1$

Случай (1). Если последовательность $y_1,...,y_{k-2},0,0$ получена с помощью входа $x_1,...,x_{k+1}$, то она же может быть получена и с помощью входа $x_1,...,x_{k-1},0,1$. Тогда требуемая последовательность $y_1,...,y_{k-2},0,0,1$ получается с помощью входа $x_1,...,x_{k-1},0,1,1$

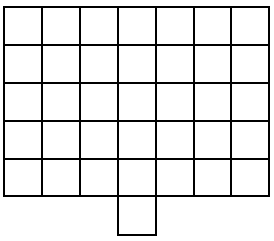
Случай (2) Если последовательность $y_1,...,y_{k-2},0,1$ получена с помощью входа $x_1,...,x_{k+1}$, то $x_k=x_{k+1}=1$. Тогда требуемая последовательность $y_1,...,y_{k-2},0,1,1$ получается с помощью входа $x_1,...,x_{k-1},1,1,1$

Случай (3) рассматривается аналогично случаю (2).

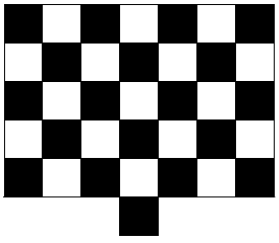
Подсчитаем число последовательностей длины 6, не содержащих отрезок 101. Для этого из общего числа последовательностей (64 шт) вычесть те, которые содержат 101 (27шт).

ОТВЕТ: запрет 101, не содержат запрета последовательности (I) и (III); количество 37.

5. Докажите, что *нельзя обойти* все клетки изображенной на рисунке фигуры, побывав в каждой ровно один раз. Начинать движение можно из любой клетки. Разрешается двигаться на *одну клетку* только вправо, влево, вверх или вниз. Движение по диагонали запрещено.



Решение: Раскрасим клетки как на рисунке. Делая один шаг, мы из черной клетки попадаем в белую и наоборот. Значит, если бы искомый обход был возможен, то клеток одного цвета было бы от силы на единицу больше, чем клеток другого цвета. Но черных клеток на две больше, чем белых. Поэтому обход невозможен.



6. Для доступа на сайт Алиса вводит в строке браузера его имя. Затем это имя по сети отправляется на специальный DNS-сервер, который по имени сайта определяет его IP-адрес – набор из четырех целых чисел $x_1.x_2.x_3.x_4$, причем $0 < x_i < 255,\ i = 1,2,3,4.$ Этот IP-адрес сервер отправляет Алисе. Чтобы защитить передаваемый адрес от подделки, сервер вместе с адресом передает число s, которое он вычисляет так: $s = r_{305}((h_4)^d)$, где d – секретное натуральное число, известное только Алисе и серверу, а $r_{305}(x)$ – остаток от деления числа x на 305; число h_4 находится последовательным применением правила $h_i = r_{305}((h_{i-1})^2 \cdot x_i)$, где i принимает значения $1,2,3,4$, а $h_0 = 1$. Получив IP-адрес, Алиса также вычисляет s и, если оно совпадает с присланным сервером значением, Алиса признает этот IP-адрес подлинным. Злоумышленник узнал, что на запрос Алисы сервер ответил: 10.11.1.1 при $s = 15$. Он хочет от имени сервера отправить Алисе ложный (отличающийся от исходного) адрес вида 10.11.*a.b* и такое число *s'*, чтобы этот адрес Алиса признала подлинным. Найдите хотя бы одну такую тройку *a,b, s'* с условием $s' \geq 1$.

Решение:

Заметим, что факторизовывать число $N = 305$ и находить значение d нет необходимости – достаточно найти пару x_3', x_4' такую, что $x_3' \neq x_3,\ x_4' \neq x_4$ и описанное преобразование сжатия (в основе которого лежит итеративная функция h) от значений x_1, x_2, x_3', x_4' дает тоже значение h_4. То есть, попробуем найти коллизию сжимающего преобразования, тогда и значение s от IP-адресов $x_1.x_2.x_3.x_4$ и $x_1.x_2.x_3'.x_4'$ будет одинаковым.

Замечаем, что так как $x_3 = 1,\ x_4 = 1$, то $h_4 = r_N((h_2)^4)$. Тогда при условии сохранения прежних компонент $x_1.x_2$, для искомого IP-адреса получаем, что необходимо найти такие x_3', x_4' и параметр h_3', которые удовлетворяют системе:

$\begin{cases} h_3' = r_N((h_2)^2 \cdot x_3') \\ h_4 = r_N((h_3')^2 \cdot x_4') \end{cases}, \begin{cases} h_3' = r_N((h_2)^2 \cdot x_3') \\ (h_2)^4 = r_N((h_3')^2 \cdot x_4') \end{cases}$, из которой следует, что $r_N((x_3')^2 \cdot x_4') = 1$, то есть $(x_3')^2 \cdot x_4' = 1 + t \cdot N$, t - натуральное. Тогда при $t = 1$ имеем: $(x_3')^2 \cdot x_4' = 306 = 2 \cdot 3^2 \cdot 17$, откуда получаем следующий возможный вариант для пары (x_3', x_4'): (3,34).

Ответ, возможный вариант: 10.11.3.34 с исходным значением s.

1. (16 баллов) Женя решила поделиться забавным *палиндромом* с Ксюшей (палиндром – текст, читающийся одинаково в обоих направлениях. Например: «А роза упала на лапу Азора»). Но чтобы никто о нем больше не узнал, Женя зашифровала его следующим образом: каждую букву палиндрома она заменила числом согласно таблице и в результате получила последовательность чисел $x_1, x_2, \ldots, x_{29}$. Затем она взяла последовательность целых чисел $y_1, y_2, \ldots, y_{29}$, полученных по правилу $y_i = i \cdot d$, где d - некоторое целое число, и вычислила новую последовательность $r_1, r_2, \ldots, r_{29}$, где r_i равно остатку от деления на 33 суммы $x_i + y_i$. В результате у неё получилось вот что: **11 30 1 11 7 15 31 5 13 23 21 5 31 12 3 26 26 14 11 27 31 4 11 9 15 0 4 14 9.** Помогите Ксюше прочитать палиндром.

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	Ь	Ы	Ь	Э	Ю	Я
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	32	33

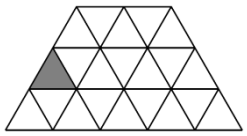
2. (18 баллов) Из последовательности $x_1, x_2, \ldots, x_n, x_i \in \{0,1\}$ получена последовательность $y_1, y_2, \ldots, y_{n-1}$ по правилу

$y_i = x_i \cdot x_{i+1}$, $i = 1, \ldots, n-1$. а) *Сколько* различных последовательностей $y_1, y_2, \ldots, y_6$ может быть получено (при выборе всевозможных $x_1, x_2, \ldots, x_7, x_i \in \{0,1\}$)?

б) *Какие* последовательности $y_1, y_2, \ldots, y_{n-1}$ *не могут* быть получены ни при каких $x_1, x_2, \ldots, x_n, x_i \in \{0,1\}$?

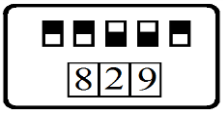
3. (16 баллов) Линия связи состоит из 4-х каналов, пронумерованных числами 1,2,3,4. Для передачи по линии сигнала на каждый канал подается свой импульс, величина которого может быть 7, 9, 11, 13 или 15 единиц. В каждом канале есть усилитель, который увеличивает поданный импульс в 5^{i-1} раз, где i - номер канала. На выходе линии формируется сигнал, который равен остатку от деления на 625 суммы полученных по каналам импульсов. Какие импульсы необходимо подать на каналы, чтобы получить сигнал величиной 57 единиц?

4. (16 баллов) В каждой треугольной ячейке (см. рис.) сидит по кузнечику. Одновременно все кузнечики перепрыгивают в какую-либо соседнюю по стороне ячейку (например, серая ячейка граничит по стороне с двумя ячейками). При этом в одной ячейке могут оказаться несколько кузнечиков. Каково *минимальное* количество ячеек, в которых не окажется *ни одного* кузнечика? Ответ обоснуйте.



5. (18 баллов) Для доступа на сайт Алиса вводит в строке браузера его имя. Затем это имя по сети отправляется на специальный DNS-сервер, который по имени сайта определяет его IP-адрес – набор из четырех целых чисел $x_1.x_2.x_3.x_4$, причем $0 < x_i < 255$, $i = 1,2,3,4$. Этот IP-адрес сервер отправляет Алисе. Чтобы защитить передаваемый адрес от подделки, сервер вместе с адресом передает число s, которое он вычисляет так: $s = r_{323}((h_4)^d)$, где d – секретное натуральное число, известное только Алисе и серверу, а $r_{323}(x)$ – остаток от деления числа x на 323; число h_4 находится последовательным применением правила $h_i = r_{323}((h_{i-1})^2 \cdot x_i)$, где i принимает значения $1,2,3,4$, а $h_0 = 123$. Получив IP-адрес, Алиса также вычисляет s и, если оно совпадает с присланным сервером значением, Алиса признает этот IP-адрес подлинным. Злоумышленник узнал, что на запрос Алисы сервер ответил: 192.168.2.5 при $s = 130$. Он хочет от имени сервера отправить Алисе ложный (отличающийся от исходного) адрес вида 192.168.*a.b* и такое число *s′*, чтобы этот адрес Алиса признала подлинным. Найдите хотя бы одну такую тройку *a,b, s′* с условием $s' \geq 1$.

6. (16 баллов) Для проведения расследования оперативным работникам необходимо попасть в игровой зал подпольного казино, который открывается с помощью электронных устройств А и В, расположенных в разных помещениях. Один из оперативников в промежуток времени с 6.00 до 7.15 может получить доступ к устройству А, а другой, в то же самое время, – к устройству В. До начала операции известно следующее. **1.** На лицевой панели каждого устройства имеется 5 тумблеров, принимающих положения «0» или «1», а также трёхразрядное десятичное табло (см. рис.). **2.** Каждому положению тумблеров соответствует своё ***уникальное для данного устройства*** трёхзначное число на табло. Соответствие положений тумблеров числам и сами числа неизвестны. **3.** Тумблеры можно установить в такие положения, что числа на табло обоих устройств совпадут. ***В этом и только в этом случае дверь в игровой зал откроется.*** **4.** Находясь в помещениях, оперативники смогут общаться, ***только*** пересылая друг другу по пневмопочте имеющийся в их распоряжении специальный блокнот на 1001 страницу. **5.** Страница блокнота (см. рис.) позволяет вписывать в отведенные 5 позиций цифры 0 или 1. Никакие другие манипуляции со страницами технически невозможны. **6.** Известно, что между переключением тумблеров и появлением соответствующего трёхзначного числа на табло проходит ровно 1 минута. В этот промежуток времени оперативник сможет отыскать в блокноте страницу по ее номеру, произвести на ней запись или прочитать ее



содержимое. Провести манипуляции с большим числом страниц за одну минуту технически невозможно.
7. Время пересылки блокнота по пневмопочте – 3 минуты. Как в отведенное время открыть дверь?

11 класс XXIV МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

(сайт олимпиады www.cryptolymp.ru) 30.11.2014

1 вариант

1. Женя решила поделиться забавным *палиндромом* с Ксюшей (палиндром – текст, читающийся одинаково в обоих направлениях. Например: «А роза упала на лапу Азора»). Но чтобы никто о нем больше не узнал, Женя зашифровала его следующим образом: каждую букву палиндрома она заменила числом согласно таблице и в результате получила последовательность чисел $x_1, x_2, \ldots, x_{29}$. Затем она взяла последовательность целых чисел $y_1, y_2, \ldots, y_{29}$, полученных по правилу $y_i = i \cdot d$, где d - некоторое целое число, и вычислила новую последовательность $r_1, r_2, \ldots, r_{29}$, где r_i равно остатку от деления на 33 суммы $x_i + y_i$. В результате у неё получилось вот что: **11 30 1 11 7 15 31 5 13 23 21 5 31 12 3 26 26 14 11 27 31 4 11 9 15 0 4 14 9.**

Помогите Ксюше прочитать палиндром.

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
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	32	33

Решение: Легко проверить, что $i-$ й член последовательности гамм равен $\gamma_i = id$.

Нам известны разности: $\gamma_n - \gamma_1, \gamma_{n-1} - \gamma_2 \ldots$

Если длина палиндрома четна, то найдем d из разности центральных символов шифрованного сообщения.

Если длина палиндрома нечетна, то найдем значение $2d$ из разности следующего и предыдущего символов шифрованного сообщения относительно центрального. Для нахождения d остается обратить 2 по модулю 33 ($2^{-1} \equiv 17 \pmod{33}$).

$d = 7$

ОТ: 4 16 13 16 5 6 15 15 16 19 10 20 6 13 30 13 6 20 10 19 16 15 15 6 5 16 13 16 4

ГАММА: 7 14 21 28 2 9 16 23 30 4 11 18 25 32 6 13 20 27 1 8 15 22 29 3 10 17 24 31 5

ШТ: 11 30 1 11 7 15 31 5 13 23 21 5 31 12 3 26 26 14 11 27 31 4 11 9 15 0 4 14 9

Ответ: **голоден носитель лет и сон не долог**

2. Из последовательности $x_1, x_2, \ldots, x_n, x_i \in \{0,1\}$ получена последовательность $y_1, y_2, \ldots, y_{n-1}$ по правилу

$$y_i = x_i \cdot x_{i+1},\ i = 1, \ldots, n-1.$$

а) *Сколько* различных последовательностей $y_1, y_2, \ldots, y_6$ может быть получено (при выборе всевозможных $x_1, x_2, \ldots, x_7, x_i \in \{0,1\}$)?

б) *Какие* последовательности $y_1, y_2, \ldots, y_{n-1}$ *не могут* быть получены ни при каких $x_1, x_2, \ldots, x_n, x_i \in \{0,1\}$?

Решение: Для всевозможных последовательностей из четырех символов x_1, x_2, x_3, x_4 найдем им соответствующие последовательности y_1, y_2, y_3. Результаты приведены в таблице. Видим, что выходная последовательность y_i не может содержать фрагмент 101 (назовем его *запретом*).

x_1, x_2, x_3, x_4	y_1, y_2, y_3

Покажем теперь, что любая последовательность, не содержащая 101, может быть получена при некоторой входной последовательности x_i. Предположим, что последовательность $y_1, \ldots, y_k$ нами уже получена с помощью некоторой последовательности $x_1, \ldots, x_{k+1}, k > 2$. Покажем, что мы сможем тогда получить и последовательность $y_1, \ldots, y_{k+1}$ (конечно, если она не содержит 101).

Если $y_{k+1} = 0$, то последовательность $y_1, \ldots, y_k, 0$ можно получить, добавив 0 к входной последовательности, из которой получена последовательность $y_1, \ldots, y_k$. Если $y_{k+1} = 1$, то возможны три случая:

(1) последовательность $y_1, \ldots, y_{k-2}, 0, 0, 1$

0, 0, 0, 0	0, 0, 0
0, 0, 0, 1	0, 0, 0
0, 0, 1, 0	0, 0, 0
0, 0, 1, 1	0, 0, 1
0, 1, 0, 0	0, 0, 0
0, 1, 0, 1	0, 0, 0
0, 1, 1, 0	0, 1, 0
0, 1, 1, 1	0, 1, 1
1, 0, 0, 0	0, 0, 0
1, 0, 0, 1	0, 0, 0
1, 0, 1, 0	0, 0, 0
1, 0, 1, 1	0, 0, 1
1, 1, 0, 0	1, 0, 0
1, 1, 0, 1	1, 0, 0
1, 1, 1, 0	1, 1, 0
1, 1, 1, 1	1, 1, 1

(2) последовательность $y_1,\dots,y_{k-2},0,1,1$

(3) последовательность $y_1,\dots,y_{k-2},1,1,1$

Случай (1). Если последовательность $y_1,\dots,y_{k-2},0,0$ получена с помощью входа $x_1,\dots,x_{k+1}$, то она же может быть получена и с помощью входа $x_1,\dots,x_{k-1},0,1$. Тогда требуемая последовательность $y_1,\dots,y_{k-2},0,0,1$ получается с помощью входа $x_1,\dots,x_{k-1},0,1,1$

Случай (2) Если последовательность $y_1,\dots,y_{k-2},0,1$ получена с помощью входа $x_1,\dots,x_{k+1}$, то $x_k = x_{k+1} = 1$. Тогда требуемая последовательность $y_1,\dots,y_{k-2},0,1,1$ получается с помощью входа $x_1,\dots,x_{k-1},1,1,1$

Случай (3) рассматривается аналогично случаю (2).

Подсчитаем число последовательностей длины 6, не содержащих отрезок 101. Для этого из общего числа последовательностей (64 шт) вычесть те, которые содержат 101 (27шт).

ОТВЕТ: запрет 101; количество 37

3. Линия связи состоит из 4-х каналов, пронумерованных числами 1,2,3,4. Для передачи по линии сигнала на каждый канал подается свой импульс, величина которого может быть 7, 9, 11, 13 или 15 единиц. В каждом канале есть усилитель, который увеличивает поданный импульс в 5^{i-1} раз, где i - номер канала. На выходе линии формируется сигнал, который равен остатку от деления на 625 суммы полученных по каналам импульсов. Какие импульсы необходимо подать на каналы, чтобы получить сигнал, величиной 57 единиц?

Решение: Заметим, что числа 7, 9, 11, 13, 15, равные импульсам, которые передаются по каналам, дают разные и в точности все возможные остатки при делении на 5.

Пусть $a \in \mathbb{Z}$ - значение, равное сумме импульсов, переданных по четырем каналам. Тогда по условию $r_{625}(a) = 57$, где $r_{625}(a)$ – остаток от деления a на 625. Справедливо представление

$$a = a_1 + 5a_2 + 25a_3 + 125a_4,$$

где $a_i \in \{7, 9, 11, 13, 15\},\ i \in \{1, 2, 3, 4\}$. В то же время из условия задачи

$$a = 57 + 625q, \qquad q \in \mathbb{Z}.$$

Но тогда, нетрудно понять, что

$$r_5(a_1) = r_5(a) = r_5(57 + 625q) = r_5(57) = 2.$$

Откуда следует, что число a_1 может равняться только 7, поскольку только оно дает остаток 2 при делении на число 5. Получим

$$a - 7 = 5a_2 + 25a_3 + 125a_4 = 50 + 625q,$$
$$a_2 + 5a_3 + 25a_4 = 10 + 125q.$$

Аналогично предыдущим рассуждениям имеем:

$$r_5(a_2) = r_5(a_2 + 5a_3 + 25a_4) = r_5(10 + 125q) = r_5(10) = 0.$$

Отсюда находим, что $a_2 = 15$. Далее получим равенства:

$$5a_3 + 25a_4 = 10 + 125q - 15 = -5 + 125q,$$
$$a_3 + 5a_4 = -1 + 25q.$$

Также аналогично найдем

$$r_5(a_3) = r_5(a_3 + 5a_4) = r_5(-1 + 25q) = 4.$$

Следовательно, $a_3 = 9$. И, наконец, вычислим:

$$5a_4 = -1 + 25q - 9 = -10 + 25q,$$
$$a_4 = -2 + 5q.$$

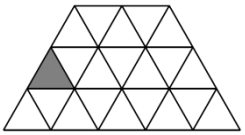
Придем к равенствами

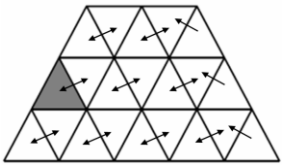
$$r_5(a_4) = r_5(-2 + 5q) = r_5(-2) = 3$$

и $a_4 = 13$. Таким образом, искомый набор импульсов на входе физической линии есть (7, 15, 9, 13).

Ответ: 7,15,9,13.

4. В каждой треугольной ячейке (см. рис.) сидит по кузнечику. Одновременно все кузнечики перепрыгивают в какую-либо соседнюю по стороне ячейку (например, серая ячейка граничит по стороне с двумя ячейками). При этом в одной ячейке могут оказаться несколько кузнечиков. Каково *минимальное* количество ячеек, в которых не окажется *ни одного* кузнечика? Ответ обоснуйте.





Решение: Заметим, что ячейки подразделяются на два типа: ячейки "острием вверх" (▲) и ячейки "острием вниз" (▼). Перепрыгивая, кузнечик попадает из ячейки (▲) в ячейку (▼) и наоборот. Ячеек типа (▲) на 3 больше, чем ячеек (▼). Поэтому, по крайней мере три ячейки окажутся пустыми. Чтобы обосновать, что ответ в задаче именно 3, укажем (см. рисунок) один из возможных способов перемещения кузнечиков, при котором освобождаются ровно 3 ячейки.

Ответ: 3

5. Для доступа на сайт Алиса вводит в строке браузера его имя. Затем это имя по сети отправляется на специальный DNS-сервер, который по имени сайта определяет его IP-адрес – набор из четырех целых чисел $x_1.x_2.x_3.x_4$, причем $0 < x_i < 255,\ i = 1,2,3,4.$ Этот IP-адрес сервер отправляет Алисе. Чтобы защитить передаваемый адрес от подделки, сервер вместе с адресом передает число s, которое он вычисляет так: $s = r_{323}((h_4)^d)$, где d – секретное натуральное число, известное только Алисе и серверу, а $r_{323}(x)$ – остаток от деления числа *x* на 323; число h_4 находится последовательным применением правила $h_i = r_{323}((h_{i-1})^2 \cdot x_i)$, где i принимает значения $1,2,3,4,$ а $h_0 = 123$. Получив IP-адрес, Алиса также вычисляет *s* и, если оно совпадает с присланным сервером значением, Алиса признает этот IP-адрес подлинным. Злоумышленник узнал, что на запрос Алисы сервер ответил: 192.168.2.5 при $s = 130$. Он хочет от имени сервера отправить Алисе ложный (отличающийся от исходного) адрес вида 192.168.*a.b* и такое число *s'*, чтобы этот адрес Алиса признала подлинным. Найдите хотя бы одну такую тройку *a,b, s'* с условием $s' \geq 1.$

Решение: Заметим, что факторизовывать число $N = 323$ и находить значение d нет необходимости – достаточно найти пару x_3', x_4' такую, что $x_3' \neq x_3,\ x_4' \neq x_4$ и описанное преобразование сжатия (в основе которого лежит итеративная функция h) от значений x_1, x_2, x_3', x_4' дает тоже значение h_4. То есть, попробуем найти коллизию сжимающего преобразования, тогда и значение s от IP-адресов $x_1.x_2.x_3.x_4$ и $x_1.x_2.x_3'.x_4'$ будет одинаковым. Замечаем, что так как

$$\begin{cases} h_1 = r_N((h_0)^2 \cdot x_1) \\ h_3 = r_N((h_1)^2 \cdot x_2) \\ h_3 = r_N((h_2)^2 \cdot x_3) \\ h_4 = r_N((h_3)^2 \cdot x_4) \end{cases}, \text{ то } h_4 = r_N((h_2)^4 \cdot (x_3)^2 \cdot x_4).$$

Тогда при условии сохранения прежних компонент $x_1.x_2$, для искомого IP-адреса получаем, что необходимо найти такие x_3', x_4' и параметр h_3', которые удовлетворяют системе:

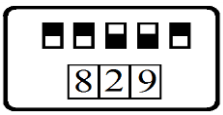
$$\begin{cases} h_3' = r_N((h_2)^2 \cdot x_3') \\ h_4 = r_N((h_3')^2 \cdot x_4') \end{cases}, \begin{cases} h_3' = r_N((h_2)^2 \cdot x_3') \\ r_N((h_2)^4 \cdot (x_3)^2 \cdot x_4) = r_N((h_3')^2 \cdot x_4') \end{cases}, \text{ из которой следует, что } (x_3')^2 \cdot x_4' = r_N((x_3)^2 \cdot x_4),$$

то есть $(x_3')^2 \cdot x_4' = (x_3)^2 \cdot x_4 + t \cdot N$, t - натуральное. Тогда при $t = 1$ имеем:

$(x_3')^2 \cdot x_4' = 20+323=343= 7^2 \cdot 7$, откуда получаем следующий возможный вариант для пары (x_3', x_4'): (7,7).

Ответ, возможный вариант: 192.168.7.7 с исходным значением s.

6. Для проведения расследования оперативным работникам необходимо попасть в игровой зал подпольного казино, который открывается с помощью электронных устройств А и В, расположенных в разных помещениях. Один из оперативников в промежуток времени с 6.00 до 7.15 может получить доступ к устройству А, а другой, в то же самое время, – к устройству В. До начала операции известно следующее. **1.** На лицевой панели каждого устройства имеется 5 тумблеров, принимающих положения «0» или «1», а также трёхразрядное десятичное табло (см. рис.). **2.** Каждому положению тумблеров соответствует своё ***уникальное для данного устройства*** трёхзначное число на табло. Соответствие положений тумблеров числам и сами числа неизвестны. **3.** Тумблеры можно установить в такие положения, что числа на табло обоих устройств совпадут. ***В этом и только в этом случае дверь в игровой зал откроется.*** **4.** Находясь в помещениях, оперативники смогут общаться, ***только*** пересылая друг другу по пневмопочте имеющийся в их распоряжении специальный блокнот на 1001 страницу. **5.** Страница блокнота (см. рис.) позволяет вписывать в отведенные 5 позиций цифры 0 или 1. Никакие другие манипуляции со страницами технически невозможны. **6.** Известно, что между переключением тумблеров и появлением соответствующего трёхзначного числа на табло проходит ровно 1 минута. В этот промежуток времени оперативник сможет отыскать в блокноте страницу по ее номеру, произвести на ней запись или прочитать ее содержимое. Провести манипуляции с большим числом страниц за одну минуту технически невозможно. **7.** Время пересылки блокнота по пневмопочте – 3 минуты. Как в отведенное время открыть дверь?



Примечание: Рисунки лишь поясняют условие задачи. Не следует думать, что страницу 23 надо заполнять именно так, и что такому положению тумблеров соответствует число 829.

Решение: Пусть, для определенности, блокнот сначала находится у оперативника, работающего с устройством А. За 33 минуты он перебирает все комбинации выключателей и записывает эти комбинации на страницах блокнота. Каждую комбинацию он пишет на странице с тем номером, который высветился на трехразрядном табло. То есть, если при положении тумблеров, скажем, 11010, высветилось на табло 755, то на странице 755 блокнота он и пишет 11010. Затем, заполненный блокнот оперативник А отправляет оперативнику В.

В итоге, в 6.36 оперативник В блокнот получает и начинает перебирать все 32 комбинации тумблеров у себя, при этом сверяясь с блокнотом, а именно: сначала выставляет комбинацию 00000; через минуту на табло загорается, скажем, 120. Он, затем, выставляет 00001 и проверяет заполнена ли страница 120 в блокноте и т.д. Как только заполненная страница, с некоторым номером **n**, найдется (а, по условию, она найдется обязательно), он вписывает ее содержимое на страницу с номером 1001, а тумблеры выставляет так, чтоб на табло горело это **n**. На это у оперативника В уйдет не более 34 минут.

Самое позднее в 7.13, оперативник А получает блокнот обратно. На странице 1001 записано положение тумблеров, при котором уже на табло его устройства загорится **n**. Ему остается открыть блокнот на странице 1001, прочитать ее содержимое и выставить тумблеры. Не позднее 7.15 на его табло тоже высветится **n**, и дверь откроется.

В заключении отметим, что общее время можно еще уменьшить. Действительно, 1) когда оперативники попали в помещения, тумблеры там уже в каком-то положении стояли, 2) оперативнику А достаточно вписать в блокнот лишь 31 комбинацию, т.к. если ни по одной из них оперативник В совпадений не найдет, то оставшаяся 32-ая будет искомой (страницу 1001 он оставит пустой).

9 КЛАСС

ВАРИАНТ 1.

1. Стёпа и Миша разработали следующую систему шифрования. Исходный текст, записанный без пробелов, разбивается последовательно на части по 10 букв. В каждой части буквы нумеруются слева направо от 1 до 10 и затем переставляются по правилу, которое задаётся таблицей 1. То есть, первая буква каждой части ставится на 5 место, вторая – на 7 место и т.д. Однажды Стёпа собрался отправить сообщение Мише. Он его зашифровал, а потом, для пущей надежности, зашифровал полученный текст еще раз. Подумал, и зашифровал его еще 75 раз. В результате Миша получил вот такое сообщение: «апятлрмаспчлнеааанув». В ответе укажите первое слово открытого текста (строчными буквами).

1	2	3	4	5	6	7	8	9	10
5	7	9	10	1	8	3	2	6	4

Ответ: ЛАМПА.

2. Для хранения пароля, записанного в 32-х буквенном алфавите ("е" отождествляется с "ё"), каждая его буква представляется порядковым номером -- парой цифр (т.е. А - 01, Б - 02 и т.д.). Получается последовательность цифр $y_1, y_2, \ldots$ Одновременно по правилу $x_{i+1} = r_{10}(ax_i + b), i \in \mathbb{N}$, вырабатывается последовательность десятичных цифр (x_i), минимальный период которой равен 10, где $r_{10}(x)$ – остаток от деления x на 10, a, b – натуральные числа. После чего по правилу $c_i = r_{10}(x_i + y_i)$ вычисляется последовательность (c_i), которая и сохраняется в памяти компьютера. Вася выбрал для пароля очень короткое слово, поэтому при вводе был вынужден повторить его дважды. Помогите ему восстановить забытый пароль, если сохраненная последовательность (c_i) имеет вид: 2 8 5 2 8 3 1 9 8 4 1 8 4 9 7 5. В ответе укажите полученный пароль строчными буквами (одно слово).
Ответ: яхта.

3. На соревнованиях беговых роботов было представлено некоторое количество механизмов. Роботов выпускали на одну и ту же дистанцию попарно. В протоколе фиксировались разности времен финиша победителя и побежденного в каждом из забегов. Все они оказались разными: 1 сек., 2 сек., 3 сек., 4 сек., 5 сек., 7 сек. Известно, что в ходе бегов каждый робот соревновался с каждым ровно один раз, и что каждый робот всегда бегал с одной и той же скоростью. В ответе укажите время в секундах самого медленного механизма, если лучшее время прохождения дистанции было равно 30 секундам.
Ответ: 37.

4. В таблицу, состоящую из n строк и m столбцов, записаны числа так, что сумма элементов в каждой строке равна 1520, а сумма элементов в каждом столбце равна 570. Найдите числа n и m, при которых выражение $7n-2m$ принимает наименьшее возможное натуральное значение. В ответе укажите значение $n+m$.
Ответ: 11.

5. Для зашифрования сообщения из 13 букв (сообщение написано без пробелов) на русском языке: 1) его преобразовали с помощью таблицы (рис. 1) в цепочку чисел $x_1, x_2, \dots, x_{13}$, 2) выбрали (секретное) натуральное число k_1 и дописали сумму к цепочке справа, 3) в расширенной цепочке $x_{14} = x_1 + x_2 + \cdots + x_{13} + k_1$ числа x_i заменили числами y_i по формулам: $y_i = 2x_i + x_{i+2} + (-1)^{\frac{i+1}{2}} k_1$, если i нечетное; $y_i = x_{i-1} + x_i + (-1)^{\frac{i}{2}} k_2$, если i четное, где k_2 еще одно (секретное) натуральное число и, наконец, 4) каждое y_i заменили его остатком от деления на 32. В результате получили вот что: 23, 4, 21, 7, 24, 2, 26, 28, 28, 4, 2, 16, 24, 10. В ответе укажите первое слово исходного сообщения (строчными буквами).
Ответ: нет.

6. Разблокировка коммуникатора осуществляется вводом 4-значного числового кода на сенсорном экране. На клавиатуре расстановка цифр после ввода кода меняется в зависимости от случайного простого числа k от 7 до 2017, и на месте цифры i отображается значение a_i, равное последней цифре числа ik. Пользователь вводит цифры из левой колонки левой рукой, а остальные правой. Восстановите код блокировки, если известно, что при наборе кода пользователь вводил цифры следующим образом:
при $a_3 = 3$ - правой, правой, левой, правой;
при $a_3 = 9$ - левой, левой, левой, левой;
при $a_3 = 1$ - правой, правой, правой, правой;
при $a_3 = 7$ - левой, правой, правой, правой.
В ответе укажите полученный код.

1	2	3
4	5	6
7	8	9
	0	

→

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9
	a_0	

Ответ: 3212.

10 КЛАСС

ВАРИАНТ 1.

1. Винтик и Шпунтик используют следующую систему шифрования. Исходный текст, записанный без пробелов, разбивается последовательно на части по 10 букв. В каждой части буквы нумеруются слева направо от 1 до 10 и затем переставляются по правилу, которое задаётся таблицей 1. То есть, первая буква каждой части ставится на 8 место, вторая – на 9 место и т.д. Однажды Винтик собрался отправить сообщение Шпунтик. Он его зашифровал, а потом, для пущей надежности, зашифровал полученный текст еще раз. Подумал, и зашифровал его еще 333 раза. В результате Шпунтик получил вот такое

сообщение:«авзодптмееарпазркоов». В ответе приведите последнее слово исходного текста (строчными буквами).

1	2	3	4	5	6	7	8	9	10
8	9	7	2	4	1	10	6	5	3

Ответ: зоопарк.

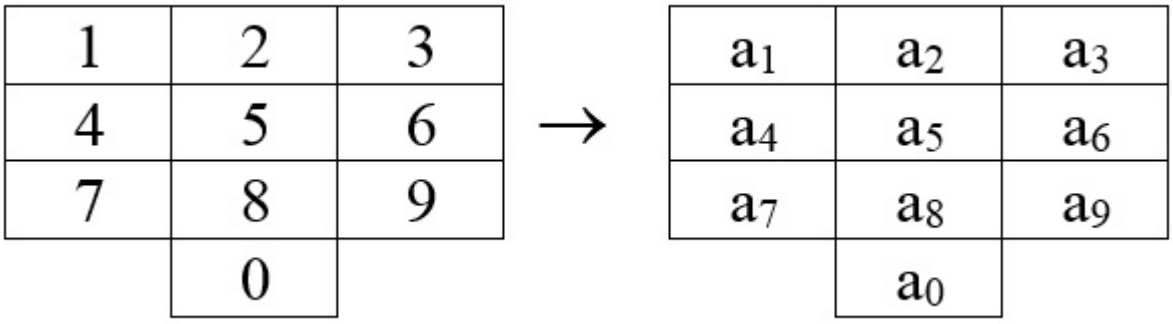
2. Для хранения пароля, записанного в 32-х буквенном алфавите ("ё" отождествляется с "е"), каждая его буква представляется порядковым номером – парой цифр (т.е. А - 01, Б - 02 и т.д.). Получается последовательность цифр $y_1, y_2, \ldots$ Одновременно по правилу $x_{i+1} = r_{10}(ax_i + b)$, вырабатывается последовательность десятичных цифр (x_i), минимальный период которой равен 10, где $r_{10}(x)$ – остаток от деления x на 10, a, b – натуральные числа. После чего по правилу $c_i = r_{10}(x_i + y_i)$ вычисляется последовательность (c_i), которая и сохраняется в памяти компьютера. Вася выбрал для пароля очень короткое слово, поэтому при вводе был вынужден повторить его дважды. Помогите ему восстановить забытый пароль, если сохраненная последовательность (c_i)имеет вид: 2 8 5 2 8 3 1 9 8 4 1 8 4 9 7 5. В ответе укажите полученный пароль строчными буквами (одно слово).
Ответ: яхта.

3. В таблицу, состоящую из n строк и m столбцов, записаны числа так, что сумма элементов в каждой строке равна 1248, а сумма элементов в каждом столбце равна 2184. Найдите числа n и m, при которых выражение $2n-3m$ принимает наименьшее возможное натуральное значение. В ответе укажите значение $n+m$.
Ответ: 11.

4. Для зашифрования сообщения из 13 букв (сообщение написано без пробелов) на русском языке: 1) его преобразовали с помощью таблицы (рис. 1) в цепочку чисел $x_1, x_2, \ldots, x_{13}$, 2) выбрали (секретное) натуральное число k_1 и дописали сумму к цепочке справа, 3) в расширенной цепочке $x_{14} = x_1 + x_2 + \cdots + x_{13} + k_1$ числа x_i заменили числами y_i по формулам: $y_i = 2x_i + x_{i+2} + (-1)^{\frac{i+1}{2}}\_1$, если i нечетное; $y_i = x_{i-1} + x_i + (-1)^{\frac{i}{2}}k_2$ если i четное, где k_2 еще одно (секретное) натуральное число и, наконец, 4) каждое y_i заменили его остатком от деления на 32. В результате получили вот что: 23, 4, 21, 7, 24, 2, 26, 28, 28, 4, 2, 16, 24, 10. В ответе укажите первое слово исходного сообщения (строчными буквами).
Ответ: нет.

5. Разблокировка коммуникатора осуществляется вводом 4-значного числового кода на сенсорном экране. На клавиатуре расстановка цифр после ввода кода меняется в зависимости от случайного простого числа k от 7 до 2017, и на месте цифры i отображается значение a_i, равное последней цифре числа ik. Пользователь вводит цифры из левой колонки левой рукой, а остальные правой. Восстановите код блокировки, если известно, что при наборе кода пользователь вводил цифры следующим образом:
при $a_3 =$ 3 - правой, правой, левой, правой;

при $a_3 = 9$ - левой, левой, левой, левой;
при $a_3 = 1$ - правой, правой, правой, правой;
при $a_3 = 7$ - левой, правой, правой, правой.
В ответе укажите полученный код.



Ответ: 3212

11 КЛАСС

ВАРИАНТ 1.

1. В таблицу, состоящую из n строк и m столбцов, записали числа (не обязательно целые) так, что сумма элементов в каждой строке равна 208, а сумма элементов в каждом столбце равна 468. После чего к таблице приписали k столбцов, сумма элементов в каждом из которых равна 260, и столбец, сумма элементов в котором равна 104. Получили таблицу, в которой сумма элементов в каждой строке равна 416. Найдите числа *n, m* и *k*, при которых выражение *3k-n-3m* принимает наименьшее возможное натуральное значение. В ответе укажите значение суммы таких *n, m* и *k (n+m+k).*
Ответ: 141

2. Незнайка и Кнопочка разработали следующую систему шифрования. Исходный текст, записанный без пробелов, разбивается на части по 16 букв. В каждой части буквы нумеруются слева направо от 1 до 16 и затем переставляются по правилу, которое задаётся таблицей 1. То есть, первая буква каждой части ставится на 15 место, вторая – на 6 место и т.д. Однажды Незнайка собрался отправить сообщение Кнопочке. Он его зашифровал, а потом, для пущей надежности, зашифровал полученный текст еще раз. Подумал, и зашифровал его еще 2013 раз. В результате Кнопочка получила вот такое сообщение: «тинаийпмтногмееокбпоучвлнлшеюуао». В ответе укажите последнее слово исходного текста (строчными буквами).

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

Таблица 1.

Ответ: палочку.

3. Для хранения пароля, записанного в 32-х буквенном алфавите ("и" отождествляется с "й"), каждая его буква представляется порядковым номером -- парой цифр (т.е. А - 01, Б

- 02 и т.д.). Получается последовательность цифр $y_1, y_2, \ldots$. Одновременно по правилу $x_{i+1} = r_{10}(ax_i + b), i \in \mathbb{N}$, вырабатывается последовательность десятичных цифр (x_i), минимальный период которой равен 10, где $r_{10}(x)$ – остаток от деления на 10, a, b – натуральные числа. После чего по правилу $c_i = r_{10}(x_i + y_i)$ вычисляется последовательность (c_i), которая и сохраняется в памяти компьютера. Вася выбрал для пароля очень короткое слово, поэтому при вводе был вынужден повторить его дважды. Помогите ему восстановить забытый пароль, если сохраненная последовательность (c_i) меет вид: 2 8 5 2 8 3 1 9 8 4 1 8 4 9 7 5. В ответе укажите полученный пароль строчными буквами (одно слово).
Ответ: яхта.

4. На соревнованиях беговых роботов было представлено некоторое количество механизмов. Роботов выпускали на одну и ту же дистанцию попарно. В протоколе фиксировались разности времен финиша победителя и побежденного в каждом из забегов. Все они оказались разными: 1 сек., 2 сек., 3 сек., 4 сек., 5 сек., 6 сек., 7 сек., 8 сек., 9 сек., 13 сек. Известно, что в ходе бегов каждый робот соревновался с каждым ровно один раз, и что каждый робот всегда бегал с одной и той же скоростью. Определите время самого медленного механизма, если лучшее время прохождения дистанции было равно 50 секундам.
Ответ: 63.

5. Для передачи по каналу трехбуквенного слова используется следующий способ. Каждой букве слова ставится в соответствие пара цифр по правилу: А – 00, Б – 01, В – 02,..., Я – 32. После чего полученная последовательность цифр $m_1, m_2, \ldots, m_6$. преобразуется по формуле:
$c_i = f(m_i, c_{\{i-1\}}), i \in \{1, \ldots, 6\}.$,
где $c_0 \in \{0, \ldots, 9\}$ – случайно выбранная цифра и $f(x, y) = r_{10}(x + 4y)$ – остаток от деления на 10 числа $x+4y$. Затем по каналу передается последовательность $c_0, c_1, \ldots, c_6$. Криптоше удалось перехватить $(c_0, c_2, c_4, c_6) = (1, 3, 7, 1)$, какое слово могло передаваться по каналу? В ответе укажите данное слово (строчными буквами).
Ответ: миф.

6. Для зашифрования сообщения из 13 букв (сообщение написано без пробелов) на русском языке: 1) его преобразовали с помощью таблицы (рис. 1) в цепочку чисел $x_1, x_2, \ldots, x_{13}$, 2) выбрали (секретное) натуральное число k_1 и дописали сумму к цепочке справа, 3) в расширенной цепочке $x_{14} = x_1 + x_2 + \cdots + x_{13} + k_1$ числа x_i заменили числами y_i по формулам: $y_i = 2x_i + x_{i+2} + (-1)^{\frac{i+1}{2}} k_1$, если i нечетное; $y_i = x_{i-1} + x_i + (-1)^{\frac{i}{2}} k_2$ если i четное, где k_2 еще одно (секретное) натуральное число и, наконец, 4) каждое y_i заменили его остатком от деления на 32. В результате получили вот что: 23, 4, 21, 7, 24, 2, 26, 28, 28, 4, 2, 16, 24, 10. В ответе укажите первое слово исходного сообщения (строчными буквами).
Ответ: нет.