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.**

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

Помогите Ксюше прочитать палиндром.

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

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

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
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 $y_1, \ldots, y_k$ 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 $y_1, \ldots, y_{k-2}, 0, 0, 1$

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

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

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

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

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:

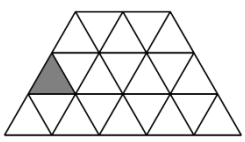
$$5a_4 = -1 + 25q - 9 = -10 + 25q,$$
$$a_4 = -2 + 5q.$$

Придем к равенствами

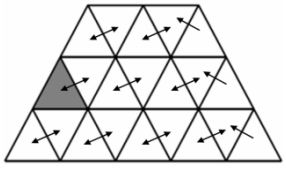
$$r_5(a_4) = r_5(-2 + 5q) = r_5(-2) = 3$$

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 специальныйDNS-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 отIP-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:

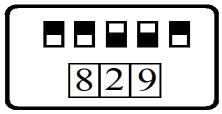
$$\begin{cases} h_3' = r_N((h_2)^2 \cdot x_3') \\ h_4 = r_N((h_3')^2 \cdot x_4') \end{cases}, \begin{cases} h_3' = r_N((h_2)^2 \cdot x_3') \\ r_N((h_2)^4 \cdot (x_3)^2 \cdot x_4) = r_N((h_3')^2 \cdot x_4') \end{cases}, \text{ из которой следует, что } (x_3')^2 \cdot x_4' = r_N((x_3)^2 \cdot x_4),$$

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 A и B, расположенных в разных помещениях. Один из оперативников в промежуток времени с 6.00 до 7.15 может получить доступ к устройству A, а другой, в то же самое время, – к устройству B. 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 A. 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 00001и 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).