XXIII Межрегиональная олимпиада школьников по математике и криптографии

Информация о порядке участия в олимпиаде

В соответствии с Положением о Межрегиональной олимпиаде школьников по математике и криптографии олимпиада проводится в два тура – отборочный (дистанционный) и заключительный (очный).

В отборочном туре могут принимать участие все желающие школьники 8-11 классов, а в заключительном (очном) туре – победители и призеры отборочного тура. Без прохождения отборочного тура в очном туре олимпиады имеют право участвовать победители и призеры аналогичной олимпиады прошлого года.

С соответствии с регламентом проведения олимпиады в 2013/14 году, школьники, не вошедшие в число победителей и призеров отборочного тура или вообще не проходившие его, могут участвовать в очном туре в статусе гостей, т.е. без права войти в список победителей и призеров очного тура для получения льгот при поступлении в вузы в 2014 году.

Отборочный тур проводится в дистанционной форме. Для участия в нем необходимо пройти регистрацию по адресу http://register.cryptolymp.ru и получить в период с 5 по 22 ноября условия задач.

Задание отборочного тура состоит из шести задач. Первые четыре из них составлены на основе задач олимпиады прошлых лет, к которым в приложении приводятся указания и ответы. После того, как Вы решите задачи отборочного тура, необходимо в срок с 17 до 22 ноября заполнить на сайте регистрации форму с ответами. Обращаем внимание, что сдача ответов происходит только один раз, сразу по всем задачам, которые Вы смогли решить. Поэтому советуем не торопиться, но и не откладывать сдачу заданий на последний день. На решение заданий, с учетом загруженности в школе, рекомендуется отвести 4-5 дней.

Итоги отборочного тура будут подведены 24 ноября. В случае успешного прохождения Вами этого тура появится возможность выбрать место участия в очном туре и распечатать анкету участника с уникальным номером (ее будет необходимо взять с собой на очный тур олимпиады).

XXIII Межрегиональная олимпиада школьников по математике и криптографии

Задачи отборочного тура для участников из 11 классов

Задача № 1

цифры	цвета
1	x
2	.
3	&
4	:
5	*
6	>
7	<
8	s
9	=
0	ж

Рис. 1

Ксюша вышивала крестиком. Внутри вышивки она скрыла послание Сереже. Для этого она представила русские буквы парами цифр в соответствии с их номерами в алфавите: А=01, Б=02, …, Я=33, а затем цифры – цветами (на рис. 1 представлены условные обозначения использованных цветов). Сначала она вышила само послание. При этом крестик, соответствующий цифре послания с номером k**,** она вышивала в позиции с номером k^2+ak+b. Позиции нумеруются слева направо, сверху вниз (например, левая верхняя клетка имеет номер 1, а клетка под ней – номер 51). Затем Ксюша стала заполнять оставшуюся часть картинки, но последние три строчки вышить не успела (рис.2). Прочитайте спрятанное послание.

Рис. 2

Ответ: До встречи в универе.

Задача № 2

При установке TCP/IP соединения между компьютерами **A** и **B** используется так называемая «процедура рукопожатия»: 1) **A** выбирает натуральное число x, не большее 5028, и передает **B** значение функции $F(x)$, а **B** отвечает **A** числом $F(x+1)$; 2) **B** выбирает натуральное число y, не большее 5028, и передает **A** число $F(y)$, при этом **A** отвечает **B** числом $F(y+1)$. Значение функции F равно остатку от деления на 5029 значения аргумента, возведенного в третью степень. Найдите сумму чисел x и y, если в сети последовательно наблюдались числа: 4258, 4385, 2243 и 2279. Примечание: число 5029 выбрано так, что значение аргумента определяется по значению функции F однозначно.

Ответ: 278.

Задача № 3

Вид	Кол-во
(**1*1***)	22
(1****0**)	25
(101*1*0*)	4
(1*1*10**)	10
(10***00*)	8
(101*100*)	2

Рис. 3

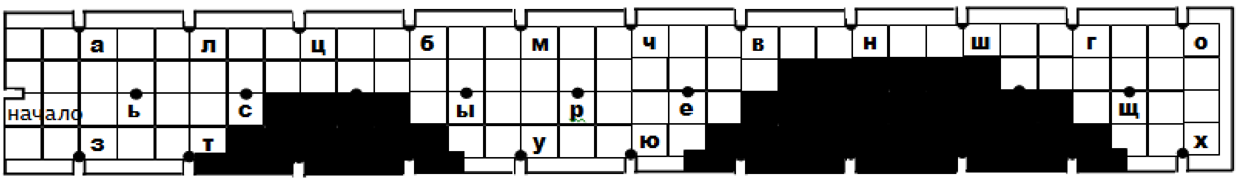
Номера гостиницы Криптохауз открываются магнитными карточками, на которых записаны ключевые последовательности из нулей и единиц длины 8. Чтобы карточка открыла номер класса «эконом» необходимо, чтобы на ней был записан ключ вида (10****0*), номер «стандарт» - ключ вида (**1*1***), «люкс» - (1****0**). На местах, помеченных символом «*», может быть любой из двух символов. Каждый из 182 работников

Криптохауза имеет ровно по 6 различных ключей и может использовать только их. Известно, что любой из существующих ключей изготовлен ровно в 21 экземплярах и находится в пользовании. Найдите минимальное число работников, открывающих номера класса «эконом», если получена информация о наличии ключей существующих типов (см. рис. 3).

Ответ: 88.

Задача № 4

При раскопках стоянки первобытных хакеров были обнаружены приспособления, предположительно использовавшиеся для шифрования паролей: частично поврежденная фигурная линейка и катушка с белой нитью, на которую нанесены одинаковые черные метки. Расстояния между последовательно идущими метками измерены в единицах деления найденной линейки и равны: 38.5; 144; 78.5; 63; 15.5; 101.5. Прочитайте пароль, зашифрованный хакерами.



Ответ: Мадрид.

Задача № 5

Подписью числа $x \in \mathbb{N}$ назовем число, равное остатку от деления x^d на 6031, где $d \in \mathbb{N}$ - некоторое фиксированное число. Известно, что подписью числа 15 является число 4273 и подписью числа 18 – число 4571. Найдите подпись числа 4050.

Ответ: 1892.

Задача № 6

Для связи абонентов A и B каналу связи передаются последовательности, состоящие из нулей и единиц. Для каждых четырех символов $a_1a_2a_3a_4$ последовательности, вычисляют *проверочную* последовательность $b_1b_2b_3$ по формулам:

$$b_1 = r_2(a_1 + a_3 + a_4), \qquad b_2 = r_2(a_1 + a_2 + a_3), \qquad b_3 = r_2(a_1 + a_2 + a_4),$$

где $r_2(x)$ – остаток от деления числа x на 2. В канале связи могут возникать помехи, приводящие к потере передаваемого символа. Абонент A по каналу передает набор $(b_1b_2b_3a_1a_2a_3a_4)$. Известно, что абонент B получил набор (111***1), где «*» - означает потерянный символ, т.е. на этом месте может находиться либо «0» либо «1». Найдите искомую последовательность $a_1a_2a_3a_4$.

Ответ: 1111.

Приложение. Примеры решения задач

Задача № 1

Ксюша вышивала крестиком. Внутри вышивки она скрыла послание Сереже. Для этого она представила русские буквы парами цифр в соответствии с их номерами в алфавите: А=01, Б=02, … , Я=33, а затем цифры – цветами (на рис. 1 представлены условные обозначения использованных цветов). Сначала она вышила само послание. При этом крестик, соответствующий цифре послания с номером k, она вышивала в позиции с номером $k^2 + ak + b$. Позиции нумеруются слева направо, сверху вниз (например, левая верхняя клетка имеет номер 1, а клетка под ней – номер 51). Затем Ксюша стала заполнять оставшуюся часть картинки, но последние две строчки вышить не успела (рис.2). Прочитайте спрятанное послание.

цифры	цвета
1	x
2	.
3	&
4	:
5	*
6	>
7	<
8	s
9	=
0	ж

Рис. 1

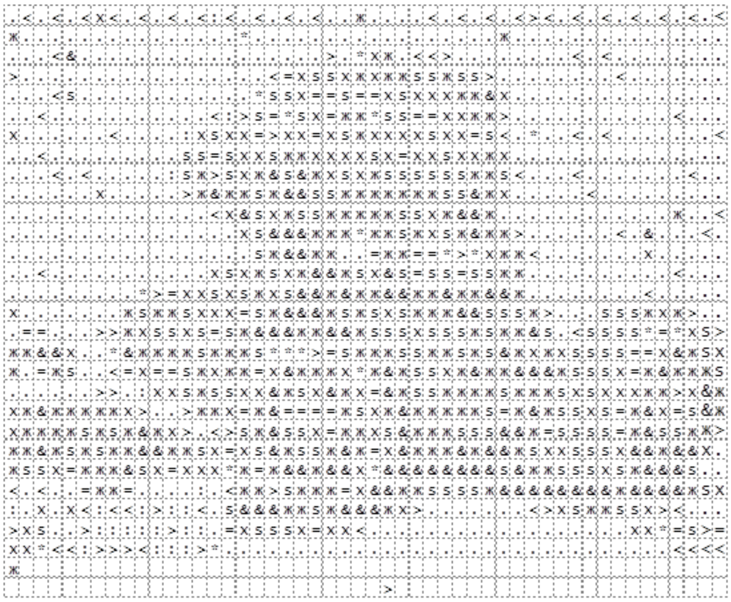


Рис. 2

Решение:

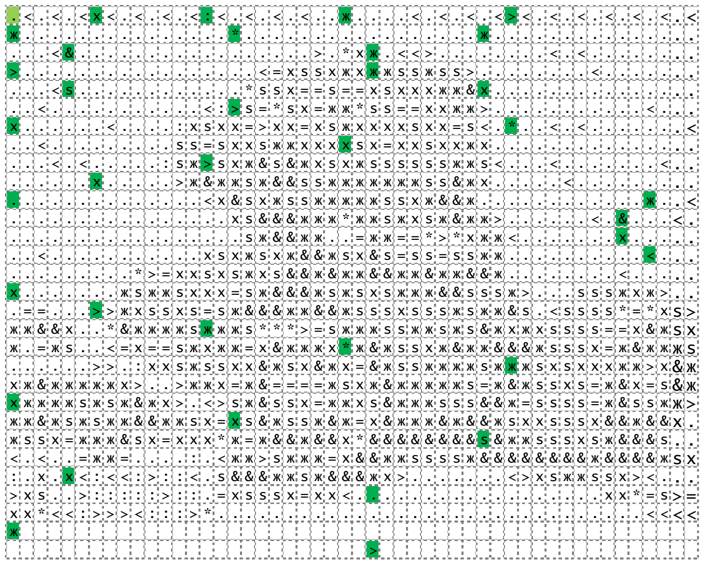
Рассмотрим расстояние между крестиком, соответствующим k-ому знаку послания, и крестиком, соответствующим (k+1)-му.

$$(k+1)^2 + a(k+1) + b - k^2 - ak - b = 2k + a + 1.$$

И рассмотрим последовательность расстояний между соседними знаками послания:

$$a+3, a+5, \ldots, a+2k+1, a+2k+3$$

Видно, что эта последовательность является арифметической прогрессией с шагом 2. Тогда посчитаем расстояние между двумя известными знаками послания – 76 крестиков. Для нахождения предыдущего символа послания необходимо отсчитать 74 крестиков назад, для пред-предыдущего еще 72 и так до начала первой строки (как показано на рисунке ниже).



Выпишем получившуюся последовательность символов:

.	x	:	ж	>	ж	*	ж	&	ж	>	ж	s	x	>	x	*	x	>	x	.	ж	&	x	<	x	>	ж	*	ж	x	x	s	x	.	ж	>
2	1	4	0	6	0	5	0	3	0	6	0	8	1	6	1	5	1	6	1	2	0	3	1	7	1	6	0	5	0	1	1	8	1	2	0	6
	М		Е		Д		В		Е		Ж		О		Н		О		К		В		П		О		Д		А		Р		К		Е	

Далее, начиная с конца, разобьем символы по парам и прочитаем сообщение: «МЕДВЕЖОНОК В ПОДАРКЕ». При этом первый символ является лишним.

Ответ: Медвежонок в подарке.

Задача № 2

При установке соединения между компьютерами **А** и **В** используется следующий вариант т.н. «процедуры рукопожатия»: 1) **А** выбирает натуральное число *x*, не большее 5250, и пересылает **В** значение функции $F(x)$, а затем **В** пересылает **А** число $F(x+1)$; 2) теперь **В** выбирает натуральное число *y*, не большее 5250, и пересылает **А** число $F(y)$, а **А** пересылает в ответ $F(y+1)$. При этом, $F(t) = r_{5251}(t^3)$, где $r_{5251}(t)$ - остаток от деления целого числа *t* на число 5251. Найдите числа *x* и *y*, если в сети последовательно наблюдались числа: 506, 519, 229 и 231. *Замечание*: известно, что в компьютерах **А** и **В** реализована процедура, решающая уравнение $r_{5251}(x^3) = a$, где *x* – неизвестное целое число, $0 \le x \le 5250$, и число 5251 выбрано так, что это уравнение имеет единственное решение.

Решение:

Исходя из условия задачи, составим систему уравнений в общем виде для z, где z - это либо x, либо y:

$$\begin{cases} r_N(z^3) = c_1, \\ r_N((z+1)^3) = c_2, \end{cases} \quad \begin{cases} r_N(z^3) = c_1, \\ r_N(z^3 + 3z^2 + 3z + 1) = c_2, \end{cases}$$

c_1, c_2, N - известны. Заметим, что

$$r_N(c_2 - c_1 + 2) = r_N(z^3 + 3z^2 + 3z + 1 - z^3 + 2) = r_N(3z^2 + 3z + 3),$$

$$r_N(c_2 + 2c_1 - 1) = r_N(z^3 + 3z^2 + 3z + 1 + 2z^3 - 1) = r_N(3z^3 + 3z^2 + 3z),$$

тогда получаем

$$r_N(z \cdot (c_2 - c_1 + 2)) = r_N(c_2 + 2c_1 - 1).$$

Для первой пары чисел 506, 519 получаем, что:

$$c_2 + 2c_1 - 1 = 1530;$$

$$c_2 - c_1 + 2 = 15;$$

тогда, исходя из этого, имеем: $x = \frac{1530}{15} = 102$. Для второй пары чисел 229, 231 получаем $y = 72$.

Ответ: $(x, y) = (102, 72)$.

Задача № 3

Табл. 1

Вид	Кол-во
(**1*1***)	21
(1****0**)	23
(101*1*0*)	4
(1*1*10**)	5
(10***00*)	4
(101*100*)	1

Номера гостиницы Криптохауз открываются магнитными карточками, на которых записаны ключевые последовательности из нулей и единиц длины 8. Чтобы карточка открыла номер класса «эконом» необходимо, чтобы на ней был записан ключ вида (10****0*), номер «стандарт» - ключ вида (**1*1***), «люкс» - (1****0**). На местах, помеченных символом «*», может быть любой из двух символов. Каждый из 174 работников Криптохауза имеет ровно по 9 различных ключей и может использовать только их. Известно, что любой из существующих ключей изготовлен ровно в 27 экземплярах и находится в пользовании. Найдите минимальное число работников, открывающих номера класса «эконом», если получена информация о наличии ключей существующих типов (см. табл. 1).

Решение:

Найдем общее число различных ключей. Для этого посчитаем количество всех используемых в гостинице ключей с учетом их повторений. Если *x* – общее число различных ключей, то количество всех используемых ключей с учетом их повторений равно 27*x*, поскольку каждый ключ изготовлен ровно в 27 экземплярах. В то же время, каждый из 174 работников имеет ровно по 9 различных ключей, а значит количество используемых в гостинице ключей с учетом их повторений равно 174·9 = 1566. Отсюда, 27*x*=1566 и *x*=58.

Теперь найдем количество ключей, открывающих номера класса «эконом». Ясно, что ключи имеющихся трех видов связаны диаграммой Эйлера (см. рис. 3). Пометим получившиеся 7 областей соответствующими числами. Так, например, области 7 соответствуют ключи, открывающие номера всех типов, области 1 – только номера класса «эконом» и т.д. В соответствии с данными задачи, составим таблицу количества ключей, находящихся в различных областях диаграммы (см. табл. 2).

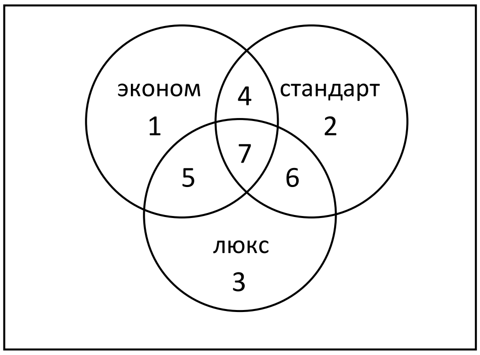


Рис. 3

Область	Кол-во
$4\cup7\cup6\cup2$	21
$5\cup7\cup6\cup3$	23
$4\cup7$	4
$6\cup7$	5
$5\cup7$	4
7	1

Табл. 2

Область	Кол-во

Из полученной таблицы легко найти количество ключей в каждой из областей 2,…,7, находя последовательно число элементов сначала в областях 4,5,6, а затем в 2,3. Чтобы найти число ключей в области 4 нужно из 4 элементов, находящихся в объединении 4∪7, вычесть число элементов, входящих в область 7. Отсюда получим, что области 4 ровно 3 различных ключа. Аналогично, в области 5 ровно 3 различных ключей и в области 6 ровно 4 различных ключей. Осталось найти число ключей, в областях 2 и 3. В области 2 ровно: 21-(3+1+4)=13 ключей. В области 3 ровно: 23-(3+1+4)=15 ключей. Полученные данные запишем в таблицу (см. табл. 3). И теперь, чтобы найти количество ключей, открывающих номера класса «эконом», нужно найти количество ключей, находящихся в области 1∪4∪5∪7. Для этого вычтем из общего числа различных ключей суммарное количество ключей, находящихся в других областях: 58 – (13+15+4) = 26. Итак, количество ключей, открывающих номера класса «эконом» равно 26.

2	13
3	15
4	3
6	4
5	3
7	1

Табл. 3

Найдем минимальное число работников, имеющих ключи, которые открывают номера класса «эконом». Покажем, что это число равно [27·26/9]=78, где [x] – наименьшее целое, больше либо равное x. Расположим данные ключи в таблицу размера 27 на 26, в столбцах которой будут экземпляры одного и того же ключа, и покроем ее элементы «девятками» - наборами, содержащими не более 9 различных ключей. В этих терминах задача переформулируется так: найти минимальное число «девяток», покрывающих построенную таблицу. Начнем покрывать ее с первой строки, ясно, что минимальное число «девяток» равно 2, т.к. 26=9·2+8, значит оставшееся число ключей в первой строке равно 8. Теперь выберем во второй строке 1 отличный от этих 8 ключей ключ (они образуют «девятку»), и покроем строку минимальным числом «девяток» (их ровно 2), тогда оставшееся число ключей во второй строке равно 7. Продолжим так далее данный процесс, выбирая в очередной строке подходящее число ключей для образования «девяток» с оставшимися ключами предыдущей строки, и разбивая затем строку на минимальное число «девяток». Отразим сказанное в следующей таблице:

<table>
<tr><td></td><td>1</td><td>2</td><td>…</td><td>26</td><td>Число «девяток»</td><td>остаток</td></tr>
<tr><td>1</td><td colspan="3">18</td><td>8</td><td>2</td><td>8</td></tr>
<tr><td>2</td><td>1</td><td colspan="2">18</td><td>7</td><td>3</td><td>7</td></tr>
<tr><td>3</td><td>2</td><td colspan="2">18</td><td>6</td><td>3</td><td>6</td></tr>
<tr><td>…</td><td colspan="4">…</td><td>…</td><td>…</td></tr>
<tr><td>9</td><td>8</td><td colspan="3">18</td><td>3</td><td>0</td></tr>
<tr><td>…</td><td colspan="4">…</td><td>..</td><td>…</td></tr>
<tr><td>27</td><td>8</td><td colspan="3">18</td><td>3</td><td>0</td></tr>
</table>

Как видно, каждые девять строк будет происходить повторение по наборам остатков. Всего таких повторений строк равно 27/9=3, а каждая такое повторение строк дает 8·3+2=26 «девяток». Итого 26·3=78 «девяток».

Ответ: 78.

Задача № 4

При раскопках стоянки первобытных хакеров были обнаружены приспособления, предположительно использовавшиеся для шифрования паролей: частично поврежденная фигурная линейка (см. рис. 4) и катушка с белой нитью, на которую нанесены одинаковые черные метки. Расстояния между последовательно идущими метками измерены в единицах деления найденной линейки и равны: 29.5; 24.5; 90; 29.5; 40; 32. Прочитайте пароль, зашифрованный хакерами

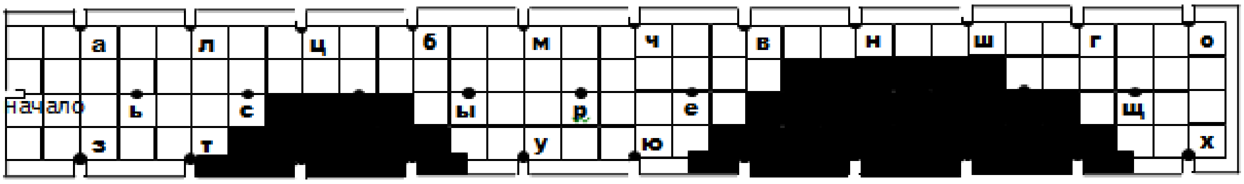


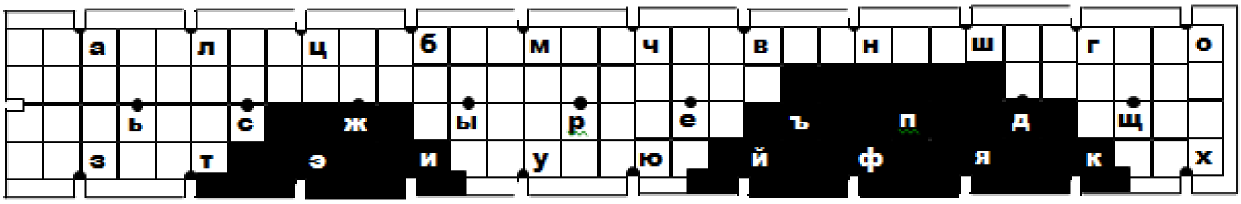
Рис. 4

Решение:

Рассмотрение оставшихся неповрежденными букв позволяет сделать предположение, что до порчи линейки на ней был изображен 32-буквенный русский алфавит (буква «ё» отсутствует). Анализ порядка следования букв в первой строке и букв, оставшихся во второй и третьей строках, позволяют восстановить утраченные символы (см. рис. 5).

Рассмотрение размеров и формы линейки позволяет сделать предположение о том, что шифрование осуществлялось по принципу «полоски Энея». Анализ величин

Рис. 5



расстояний между окрашенными точками на нити и на линейке позволяет предположить, что наматывание нити производилось так, что с оборотной стороны линейки нить ложилась вертикально, а с лицевой – диагонально. Возможны два варианта начала наматывания нити: от «а» к «з» или наоборот. Перебирая два варианта расшифрования, получаем ответ: БЕРЛИН.

Ответ: Берлин.