XXII Межрегиональная олимпиада школьников по математике и криптографии

Олимпиада проводилась в два тура. Первый тур прошел в дистанци - онной форме на интернет-сайте www.cryptolymp.ru. Второй тур проводился в очной форме на базе ИКСИ Академии ФСБ России, АлтГТУ (г. Барнаул), БТИ (г. Бийск), ДФГУ (г. Владивосток), ДГТУ (г. Ростов-на-Дону), МарГТУ (г. Йошкар-Ола), ННГУ (г. Нижний Новгород), НГУЭУ (г. Новосибирск), ИГУ (г. Иркутск), ОТИ (г. Озёрск), ОмГУ (г. Омск), ПГУ (г. Пенза), СамГУ (г. Самара), СПбГПУ (г. С.-Петербург), ГУАП (г. С.-Петербург), СибГАУ (г. Красноярск), СибГУТИ (г. Новосибирск), СФУ (г. Красноярск), ТГУ (г. Томск), ТУСУР (г. Томск), УрФУ (г. Екатеринбург), БГТУ (г. Белгород), ДВФУ (г. Владивосток), ВолГУ (г. Волгоград), КНИТУ-КАИ (г. Казань), Калининградский пограничный институт, КубГТУ (г. Краснодар), филиал БашГУ (г. Нефтекамск), ОТИ МИФИ (г. Озерск), Академия ФСО России (г. Орел), ПНИПУ (г. Пермь), ПГЛУ (г. Пятигорск), РГРТУ (г. Рязань), СГТУ (г. Саратов), ЮФУ (г. Таганрог).

Проверка работ проводилась централизовано по единым критериям. Всего дипломами I, II, III степени награждены 238 участников. Задания олимпиады были подготовлены для каждой возрастной категории (8-9, 10 и 11 классы) в нескольких равноценных вариантах. В сборнике приводятся условия и решения одной из задач каждого типа.

Межрегиональная олимпиада школьников по математике и криптографии включена в Перечень олимпиад школьников на 2012/2013 учебный год (Приказ Минобрнауки России от 14.11.2012 № 916), что дает право предоставлять льготы победителям и призерам при поступлении в государственные и муниципальные учреждения высшего профессионального образования (Приказ Минобрнауки России от 22.10.2007 № 285). Решения о льготах принимаются вузами самостоятельно и должны быть объявлены к 1 июня 2013 года.

УСЛОВИЯ И РЕШЕНИЯ ЗАДАЧ

Задача 1 (8-9, 10 классы)

Известно, что десятизначное число $A = 2013x2013y$ делится нацело на 121. Найдите все возможные пары цифр (x,y). Решение обоснуйте.

Решение

Заметим, что $121 = 11 \cdot 11$. Используя признак делимости на 11 (знакопеременная сумма цифр числа должна делиться на 11) получаем, что число A делится на 11 только при условии $x = y$. Действительно, знакопеременная сумма цифр числа A равна:

$$y + 1 + 2 + 3 + 0 - (3 + 0 + x + 1 + 2) = y - x.$$

Но y и x являются цифрами, следовательно $|y - x| < 11$, поэтому делимость возможна тогда и только тогда, когда $x = y$. Отсюда, число A имеет вид $2013x(10^5 + 1)$. Непосредственной проверкой можно убедиться, что $10^5 + 1$ делится на 11, но не делится на 121. Следовательно, на 11 должно делиться число $2013x$. Используя признак делимости на 11, находим, что $x = 0$, а значит и $y = 0$.

Ответ: (0,0).

Задача 2 (8-9, 10 классы)

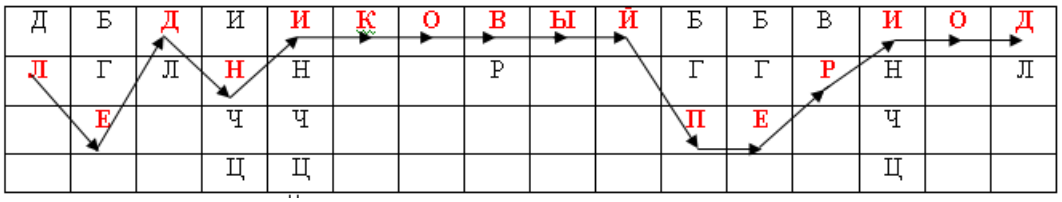
При передаче сообщения по факсу произошел сбой. В результате на листе было напечатано

Восстановите текст (ответ обоснуйте). Известно, что исходный шрифт выглядел так

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.

Решение

Сопоставим каждому изображенному символу возможные соответствующие ему буквы алфавита и затем попробуем, выбирая по одной букве из каждого столбца, прочитать исходное сообщение:



Ответ: ЛЕДНИКОВЫЙ ПЕРИОД.

Комментарий

Решение предложенной задачи основывается на используемом в криптографии ***методе бесключевого чтения***, при котором открытый текст находится без предварительного определения ключа. К этому методу также прибегают, например, в случае, когда сообщение передается по каналу связи с помехами, при этом известны виды происходящих искажений $\{\gamma_1, \dots, \gamma_k\}$.

полученные буквы / искажения	t_1	t_2	…	t_n
γ_1	s_{11}	s_{12}		s_{1n}
γ_2	s_{21}	s_{22}	…	s_{2n}
⋮	⋮	⋮	⋮	⋮
γ_k	s_{k1}	s_{k2}	…	s_{kn}

В таком случае этот метод сводится к так называемому ***чтению в колонках***, или по-другому, ***зигзагообразному чтению***. Для восстановления исходного сообщения каждой полученной искаженной букве t_i ставится в соответствие набор возможных ее истинных значений $\{s_{1i}, \dots, s_{ki}\}$ в зависимости от возможных искажений, после чего становится возможным применение зигзагообразного чтения для нахождения осмысленного текста.

Задача 3 (8-9 класс)

Для записи текста используются только заглавные буквы, пробелы, точки и запятые – всего различных 36 символов. При зашифровании каждый символ заменили числом от 0 до 35, в соответствии с порядком в «расширенном» алфавите. Затем полученную последовательность чисел разбили на пары, а каждую пару заменили по правилу: пару (a_1, a_2) заменили на пару $\left(r_{36}(a_1 n),\ r_{36}(a_1 k + a_2 m)\right)$, где $r_{36}(x)$ – остаток от деления числа x

на 36, а n, k и m – заранее выбранные целые числа от 0 до 35. Найдите все наборы чисел n, k и m, при которых разные пары переходят в разные (это необходимо для возможности расшифрования текста). Сформулируйте правило расшифрования для случая $n = k = m = 17$. Решение обоснуйте.

Решение

Условие задачи равносильно тому, что при «правильно» выбранных n, k и m система уравнений

$$\begin{cases} r_{36}(a_1 n) = y_1, \\ r_{36}(a_1 k + a_2 m) = y_2, \end{cases}$$

имеет единственное решение (a_1, a_2) при любой паре (y_1, y_2). В этом случае разные пары (a_1, a_2) будут переходить в разные (y_1, y_2), иначе получим противоречие с единственностью решения такой системы при некоторой паре (y_1, y_2). Обратно, если разные пары (a_1, a_2) переходят в разные пары (y_1, y_2), то при любой паре (y_1, y_2) такая система либо имеет единственное решение, либо не имеет решений. Однако в то же время количество различных пар (a_1, a_2) равно 36^2, а значит количество соответствующих им различных пар (y_1, y_2) по крайней мере 36^2, но ясно, что их число не превосходит 36^2, а стало быть оно в точности равно 36^2. Отсюда следует, что для любой пары (y_1, y_2) рассматриваемая система имеет решение и при том только одно.

Можно показать, что уравнение $r_{36}(a_1 n) = y_1$ имеет единственное решение a_1 при любом y_1 тогда и только тогда, когда n и 36 взаимнопросты. Следовательно, если n и 36 взаимнопросты, то из данного уравнения значение a_1 находится однозначно и тогда второе уравнение системы примет вид: $r_{36}(a_2 m) = r_{36}(y_2 - a_1 k)$.

Аналогично, оно имеет единственное решение относительно a_2 при любом y_2 тогда и только тогда, когда m и 36 взаимнопросты, при этом значение параметра k на это свойство никак не влияет. Таким образом, однозначное расшифрование возможно при выборе взаимнопростых с 36

числах $n,\ m$ и произвольном k.

Пусть теперь $n = k = m = 17$. Тогда для нахождения (a_1, a_2) нужно решить систему уравнений:

$$\begin{cases} r_{36}(17a_1) = y_1, \\ r_{36}\big(17(a_1 + a_2)\big) = y_2. \end{cases}$$

Легко видеть, что $r_{36}(17 \cdot 17) = 1$. Отсюда легко проверить, что $a_1 = r_{36}(17y_1)$ и $a_2 = r_{36}(17y_2 - 17y_1)$.

Ответ: $a_1 = r_{36}(17y_1)$, $a_2 = r_{36}(17y_2 - 17y_1)$.

Комментарий

В простейших исторических системах шифрования процесс зашифрования осуществлялся над каждой буквой в отдельности. То есть при зашифровании каждая буква исходного текста переходит в букву или символ шифрованного текста. Такие системы шифрования называются ***поточными***. Если же преобразование зашифрования применяется сразу к блоку, состоящему из 2-х, 3-х или более букв, то такое шифрование называется ***блочным***. Одним из исторических примеров блочного шифра является так называемый ***шифр Хилла***. В самой простой интерпретации этот шифр переводит пару букв открытого текста в пару букв шифрованного текста того же алфавита. Такой шифр называют ***биграммным шифром Хилла***, именно он и рассматривался в предложенной задаче.

В общем случае правило зашифрования пары букв (a_1, a_2) таким шифром выглядит следующим образом:

$$(y_1, y_2) = \big(r_t(a_1 \cdot u_{11} + a_2 \cdot u_{21}), r_t(a_1 \cdot\ u_{12} + a_2 \cdot\ u_{22})\big),$$

где u_{ij} целые числа от 0 до $t - 1$, t количество букв в алфавите, а $r_t(z) -$ остаток от деления числа z на t. При этом можно показать, что данное преобразование допускает однозначное расшифрование тогда и только тогда, когда числа t и $u_{11}u_{22} - u_{12}u_{21}$ взаимнопросты.

Задача 4 (8-9, 10, 11 классы)

При раскопках стоянки древних хакеров археологами были обнаружены следующие предметы, вероятно, использовавшиеся для шифрования информации: линейка (см. рис. 1), и катушка с белой нитью, на которую были нанесены черные метки. Расстояния между последовательными метками, измеренные в единицах деления линейки, равны 74.5, 85, 90, 90, 86, 18. Прочитайте сообщение, зашифрованное хакерами.

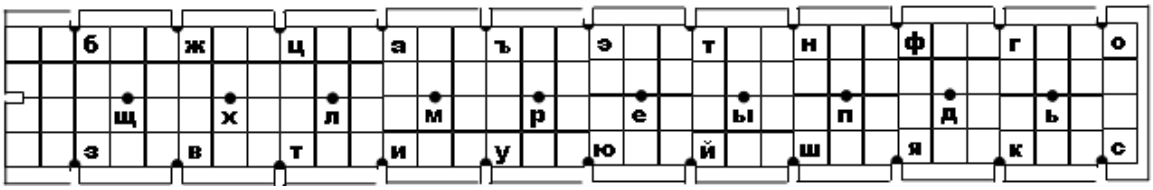
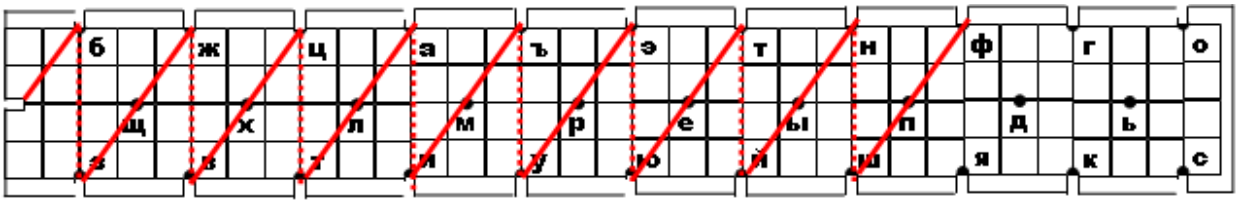


Рис. 1

Решение

Анализ линейки на рис. 1 позволяет догадаться о способе наматывания нити для осуществления шифрования. Наматывание нити производилось так, что с оборотной стороны линейки нить ложилась вертикально, а с лицевой – диагонально. В этом случае возможны два варианта наматывания нити: от «б» к «з» или наоборот.



Перебором двух вариантов устанавливаем, что наматывание нити осуществлялось по вертикали сверху вниз, по диагонали – снизу вверх, а скрытым текстом являлось слово «фишинг».

Ответ: фишинг.

Комментарий

Идея способа шифрования в представленной задаче взята из истории криптографии. Со времен Спарты одним из известных на тот период времени

приспособлением для шифрования информации являлась ***табличка Энея,*** реализующей шифр замены. Данная табличка представляла собой линейку с прорезями по бокам и имеющая отверстия, количество которых равнялось количеству букв алфавита. Каждое отверстие помечалось своей буквой, а расположение букв алфавита на линейки было произвольным. При шифровании нить протягивалась через прорезь, а затем через отверстие, соответствующее первой букве шифруемого текста, при этом на нити завязывался узелок в месте прохождения её через отверстие; затем нить возвращалась в прорезь и аналогично зашифровывалась вторая буква текста и т. д. После окончания шифрования нить извлекалась и передавалась получателю сообщения. Таким образом, каждая буква заменялась расстоянием от начала нити до соответствующего узелка. Ключом такого шифра являлся порядок расположения букв на линейке. Изобретение этого устройства приписывается Энею Тактику, полководцу IV века до н. э., одному из самых ранних греческих авторов, который писал об искусстве ведения военных действий. Единственным из сохранившихся на настоящий момент времени его трудов является работа «О перенесении осады». Так же Энеем был создан ***книжный шифр***, при котором скрытие информации осуществлялось с помощью малозаметных пометок в тексте книги или документа, например, игольных дырок, проставленных рядом с буквами, которые в своей совокупности образовывали секретное сообщение. Данный способ сокрытия информации относится к стеганографии.

Задача 5 (10, 11 класс)

При установке TCP/IP соединения между компьютерами **A** и **B** используется так называемая «процедура рукопожатия»: 1) **A** выбирает натуральное число x, не большее 5988, и передает **B** значение функции $F(x)$, а **B** отвечает **A** числом $F(x+1)$; 2) **B** выбирает натуральное число y, не большее 5988, и передает **A** число $F(y)$, при этом **A** отвечает **B** числом $F(y+1)$. Значение функции F равно остатку от деления на 5989 значения аргумента, возведенного в третью степень. Найдите числа x и y, если в сети

последовательно наблюдались числа: 1369,1421, 2795 и 2804. Число 5989 выбрано так, что значение аргумента определяется по значению функции F однозначно.

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: $c_2 - c_1 + 2 = 54$, $c_2 + 2c_1 - 1 = 4158$; тогда $x = \frac{4158}{54} = 77$. Для второй пары чисел: $c_2 - c_1 + 2 = 11$, $c_2 + 2c_1 - 1 = 8393$; тогда $y = \frac{8393}{11} = 763$.

Ответ: $(x, y) = (77, 763)$

Комментарий

Протокол TCP (Transmission Control Protocol) является одним из самых распространенных сетевых протоколов, задачей которого является гарантированная доставка данных от стороны **A** к стороне **B**. Передаваемые протоколом *TCP* данные разбиваются на составные части, которые принято называть ***сегментами***. Непосредственно перед передачей сегментов между сторонами **A** и **B** происходит обмен специальными сообщениями, позволяющими “подготовить” обе стороны к приему-передаче данных, то есть “установить соединение”. Эта процедура получила название ***протокола тройного рукопожатия*** (Three-Way Handshake). При этом вначале сторона **A** формирует сегмент, в специальном поле SEQ которого заносится

случайным образом выбранное 32-битное число x. Данный сегмент передается стороне **B**. Затем сторона **B** должна подтвердить получение этого сообщения от **A**, для чего она формирует сегмент, в специальное поле ACK которого записывает число $x+1$, а в поле SEQ этого же сегменте заносит свое случайным образом выбранное 32-битное число y. Для подтверждения получения сообщения от **B**, **A** отвечает передачей сегмента, поле ACK которого содержит $y+1$, после чего устанавливается соединение между **A** и **B**. Далее происходит передача информационных данных, причем для каждого очередного передаваемого сегмента значение в поле SEQ увеличивается на число, равное количеству передаваемых байтов информации. Таким образом, данное поле позволяет **B** определить потери каких-либо данных в процессе передачи и перезапросить их.

При разработке протокола TCP не затрагивались вопросы безопасности. Например, при установлении соединения по протоколу TCP можно легко перехватить числа x, y и $x+1, y+1$. Данное обстоятельство позволяет нарушителю подменить некоторые истинные сегменты (передаваемые от **A** к **B**) на свои с правильными значениями поля SEQ, которые будут приняты **B** за истинные. В представленной задаче предлагается защита против такого действия: числа $x, y, x+1, y+1$ передаются в преобразованном виде: все эти числа возводятся в куб и от них берутся остатки от деления на некоторое известное число N ($N = p \cdot q$, где p, q - простые числа, не известные противнику). Фактически это преобразование описывает процесс шифрования информации (в данном случае чисел) с помощью так называемой ***криптосистемы RSA***. Напомним, что в такой системе ключ зашифрования e и ключ расшифрования d – различны, хотя и взаимосвязаны между собой. Ключ расшифрования при этом хранится в секрете. Для зашифрования сообщения $x \in \{0, ..., N-1\}$ его необходимо возвести в степень e (в задаче $e = 3$) и взять остаток от деления на N, а для расшифрования – получившееся число возвести в степень d и также взять

остаток от деления на N. Стойкость криптосистемы RSA базируется на сложной задаче дискретной математики: разложении некоторого числа N на простые множители p,q (***задача факторизации***). При правильном выборе параметров p,q и e такие криптосистемы считаются надежными и широко распространены на практике. В данном случае, несмотря на незнание чисел p,q, найти неизвестные x,y становится вполне возможным, исходя из возникающей при $e=3$ слабости предложенной модификации процедуры тройного рукопожатия.

Задача 6 (11 класс)

Докажите, что из любых пяти различных натуральных чисел всегда можно выбрать три различных числа так, что их сумма будет делиться на три. Докажите, что из любых двадцати пяти различных натуральных чисел всегда можно выбрать девять различных чисел так, что их сумма будет делиться на девять.

Решение

Решим сначала первую часть задачи. Пусть $a_1, a_2, a_3, a_4, a_5 -$ различные пять натуральных чисел и $r_1, r_2, r_3, r_4, r_5,\ r_i \in \{0,1,2\} -$ их остатки от деления на 3 соответственно. Возможны следующие два случая: а) среди чисел r_1, r_2, r_3, r_4, r_5 есть хотя бы три одинаковых, тогда сумма этих трех чисел делится на три; б) среди чисел r_1, r_2, r_3, r_4, r_5 нет трех одинаковых, а значит, найдутся три различных числа, имеющие остатки 0, 1 и 2 и тогда их сумма делится на три.

Докажем теперь второе утверждение задачи. Пусть $a_1, \dots, a_{25}$ −любые двадцать пять натуральных чисел. Будем считать, что они упорядочены по возрастанию. Сгруппируем их последовательно по 5 штук: a_1, a_2, a_3, a_4, a_5; $a_6, a_7, a_8, a_9, a_{10}$; … ; $a_{21}, a_{22}, a_{23}, a_{24}, a_{25}$. В каждой пятерке по первой части задачи найдется три различных числа, сумма которых делится на три, выпишем их: $v_1, v_2, v_3,\ w_1, w_2, w_3, \dots,\ z_1, z_2, z_3$. Рассмотрим пять различных натуральных чисел $\overline{v} = \frac{1}{3}(v_1 + v_2 + v_3),\ \overline{w} = \frac{1}{3}(w_1 + w_2 + w_3),$

… , $\bar{z} = \frac{1}{3}(z_1 + z_2 + z_3)$. Среди этих пяти чисел по доказанной первой части задачи найдутся три различных числа, пусть a, b, c, сумма которых делится на три. Каждое из чисел a, b, c есть $\frac{1}{3}$ от суммы трех некоторых различных чисел из набора $a_1, \dots, a_{25}$, тогда $a + b + c$ есть $\frac{1}{3}$ от суммы некоторых девяти различных чисел из этого же набора. Отсюда из свойств делимости целых чисел следует, что сумма этих девяти чисел делится на 9.

Задача 7 (8-9, 11 классы)

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 176 работников Криптохауза имеет ровно по 5 различных ключей и может использовать только их. Известно, что любой из существующих ключей изготовлен ровно в 16 экземплярах и находится в пользовании. Найдите минимальное число работников, открывающих номера класса «эконом», если получена информация о наличии ключей существующих типов (см. табл. 1).

Табл. 1

Вид	Кол-во
(**1*1***)	22
(1****0**)	28
(101*1*0*)	6
(1*1*10**)	10
(10***00*)	4
(101*100*)	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 $16x$, поскольку каждый ключ изготовлен ровно в 16 экземплярах. В то же время, каждый из 176 работников имеет ровно по 5 различных ключей, а значит количество используемых в гостинице ключей с учетом их повторений равно 176·5 =

880. Отсюда, 16x=880 и x=55.

Теперь найдем количество ключей, открывающих номера класса «эконом». Ясно, что ключи имеющихся трех видов связаны так называемой ***диаграммой Эйлера*** (см. рис. 2). 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.

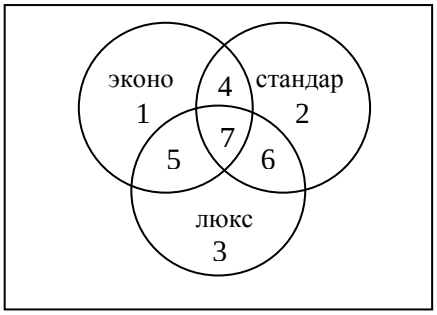


Рис. 2

В соответствии с условием задачи, составим таблицу количества ключей, находящихся в различных областях диаграммы (табл. 2).

Табл. 2

Область	4∪7∪6∪2	5∪7∪6∪3	4∪7	6∪7	5∪7	7
Количество	22	28	6	10	4	1

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. Эти данные запишем в таблицу (табл. 3).

Табл. 3

Область	2	3	4	5	6	7
Количество	7	15	5	3	9	1

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: 55 – (7+9+15) = 24. Итак, количество ключей, открывающих только номера класса «эконом» равно 24.

Найдем минимальное число работников, имеющих ключи, которые открывают номера класса «эконом». Покажем, что это число равно [16·24/5]=77, где [*x*] – наименьшее целое, больше либо равное *x*. Расположим данные ключи в табл. 4 размера 16 на 24, в столбцах которой будут экземпляры одного и того же ключа, и покроем ее элементы «пятерками» - наборами, содержащими не более 5 различных ключей.

Табл. 4

	1	2	…	24	Число «пятерок»	остаток
1	20			4	4	**4**
2	1	20		3	5	**3**
3	2	20		2	5	**2**
4	3	20		1	5	**1**
5	4	20			5	**0**
…	…				…	…
16	**20**			**4**	**4**	**4**

В этих терминах задача переформулируется так: найти минимальное число «пятерок», покрывающих построенную таблицу. Начнем покрывать ее с первой строки. Ясно, что минимальное число «пятерок» равно 4, т.к. 24=5·4+4, значит оставшееся число ключей в первой строке равно 4. Теперь выберем во второй строке один отличный от этих 4-х ключей ключ (они образуют «пятерку»), и покроем строку минимальным числом «пятерок» (их ровно четыре), тогда оставшееся число ключей во второй строке равно 3. Продолжим данный процесс, выбирая в очередной строке подходящее число ключей для образования «пятерки» с оставшимися ключами предыдущей строки, и разбивая затем строку на минимальное число «пятерок».

Как видно, набор остатков в каждых последовательно идущих пяти строках будет одинаковым. Всего таких повторений - 3, т.к. 16=5·3+1, а каждое такое повторение строк дает 5·4+4=24 «пятерок». Итого всего «пятерок», приходящихся на 15 строк, будет 24·3=72. Таким образом, остается одна строка (последняя), которая даст 4 «пятерки», и в остатке еще 4 ключа, которые покроет еще одна «пятерка». Отсюда, общее их количество равно 72+4+1=77.

Ответ: 77.

Комментарий

Математическая идея, лежащая в основе данной задачи, основывается на известной в комбинаторике ***формуле «включения-исключения».*** Пусть $n(X)$ - количество элементов множества X, тогда справедлива формула:

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap B) - n(C \cap B) + n(A \cap B \cap C).$$

Если теперь A – множество ключей, открывающих номера класса «эконом», B – класса «стандарт» и C – класса «люкс», то ясно, что в задаче требовалось найти $n(A)$, при этом все остальные величины в формуле были известны, а значение $n(A \cup B \cup C)$ легко вычислялось. В самой задаче идет речь о ***системе контроля и управления доступом***. Базовым элементом такой системы является ***идентификатор***, который хранит код, служащий для подтверждения подлинности пользователя (его ***идентификации***) и предоставлении ему определенных прав (***авторизации***). В качестве идентификатора может выступать код, вводимый на клавиатуре, отдельные биометрические параметры человека: отпечаток пальца, рисунок сетчатки или радужной оболочки глаза, трехмерное изображение лица, рисунок кровеносной системы человека. Идентификатором также может быть «таблетка», используемая в домофонах, бесконтактная (proximity) карта, брелок, или карта с магнитной полосой. Принципиально более высокий уровень защищенности дают интеллектуальные пластиковые карты или просто ***смарт-карты*** (SmartCard), в которых код хранится в специальной области памяти, доступ к которой защищен паролем владелеца карты. В отличие от большинства перечисленных носителей информации, смарт-карты помимо энергонезависимой оперативной памяти содержат микропроцессор, способный выполнять криптографические преобразования информации, что позволяет, смарт-картам самостоятельно проверять правильность ввода пароля на доступ к ключевой информации.

Задача 8 (8-9, 10 классы)

В картинке, вышитой «крестиком», Ксюша скрыла послание Сереже (см. рис. 3). Буквы она заменила парами цифр в соответствии с алфавитным порядком: А=01, Б=02, …, Я=33. Затем Ксюша выбрала простое число p. Для цифры послания с номером k крестик нужного цвета вышивался в клетке с номером pk. Нужный цвет определялся по рис. 4, а клетки в схеме нумеруются слева направо снизу вверх (например, левая нижняя клетка имеет номер 1, а клетка над ней - 51). Затем Ксюша завершила оставшуюся часть картинки. Прочитайте скрытое послание.

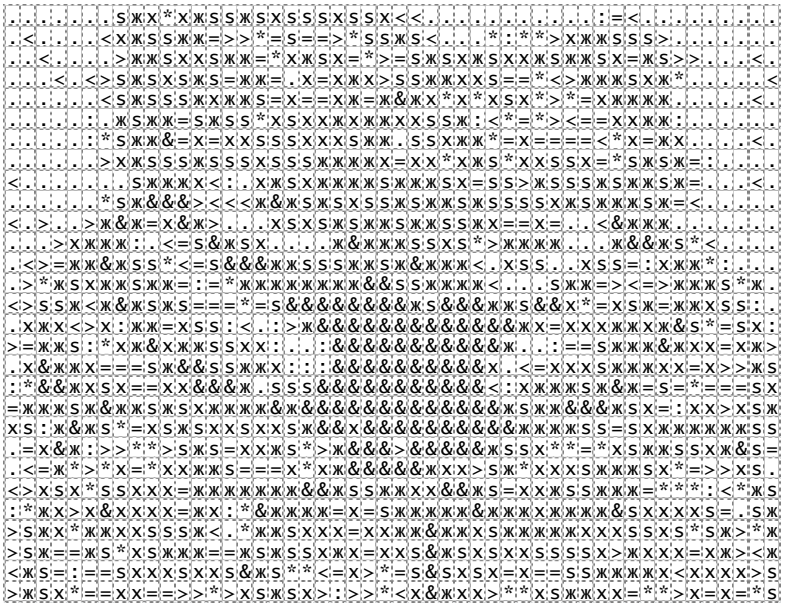


Рис. 3

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

Рис. 4

Решение

Так как буквы русского алфавита представлены их номерами алфавита, то первый символ послания может быть только «ж», «х», «.» или «&». Рассмотрим позиции с простым номером в первой строке, в которых записаны именно эти символы: 2, 29, 37 и 47. Значит, данные числа могут являться кандидатами на выбранное Ксюшей число p, поскольку на этих местах могут находиться цифры послания с номером $k = 1$. Начинаем выбирать клетки картинки, двигаясь по строкам слева направо снизу вверх с шагом, равным p. Как только на нечетном месте встречается неподходящий символ (т.е. отличный от «ж», «х», «.», «&»), делаем вывод, что p выбрано не верно (см. табл. 5).

Табл. 5

2	х	ж	=																										
	1	0	9																										
	И		?																										
29	ж	s	s																										
	0	8	8																										
	Ж		?																										
37	ж	>	ж	>	ж	=	х	*	ж	*	s																		
	0	6	0	6	0	9	1	5	0	5	8																		
	Е		Е		З		Н		Д		?																		
47	х	<	ж	х	х	s	х	>	х	&	&	ж	х	:	ж	>	ж	*	ж	&	ж	>	ж	s	ж	х	.	ж	ж	х
	1	7	0	1	1	8	1	6	1	3	3	0	1	4	0	6	0	5	0	3	0	6	0	8	0	1	2	0	0	1
	П		А		Р		О		Л		Ь		М		Е		Д		В		Е		Ж		А		Т		А	

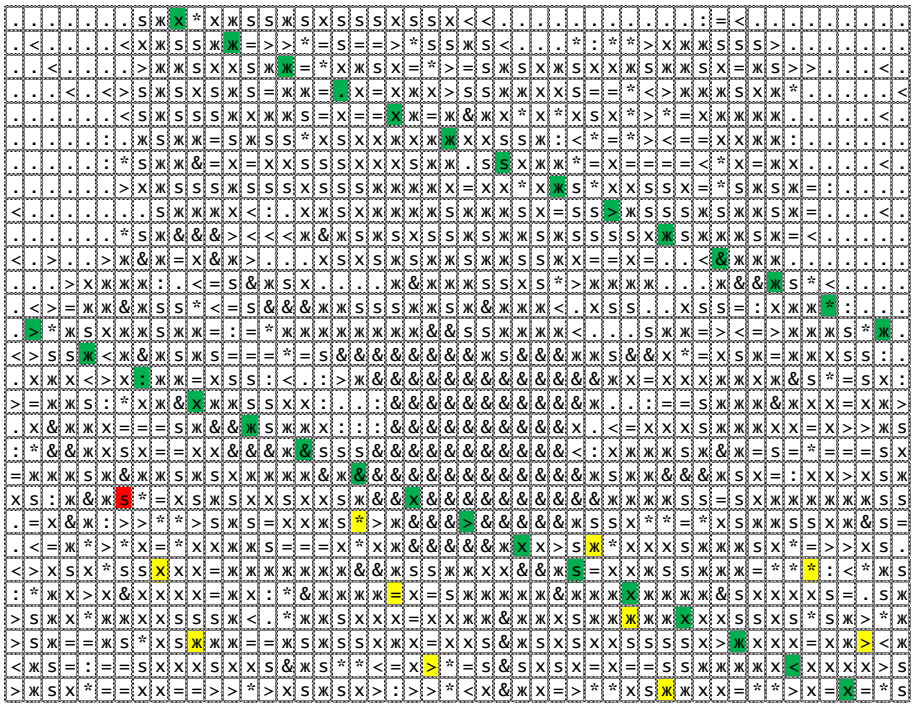


Рис. 5

В рис. 5 цветами выделены «цвета» (согласно рис. 4) для значений *p*, равных 37 и 47.

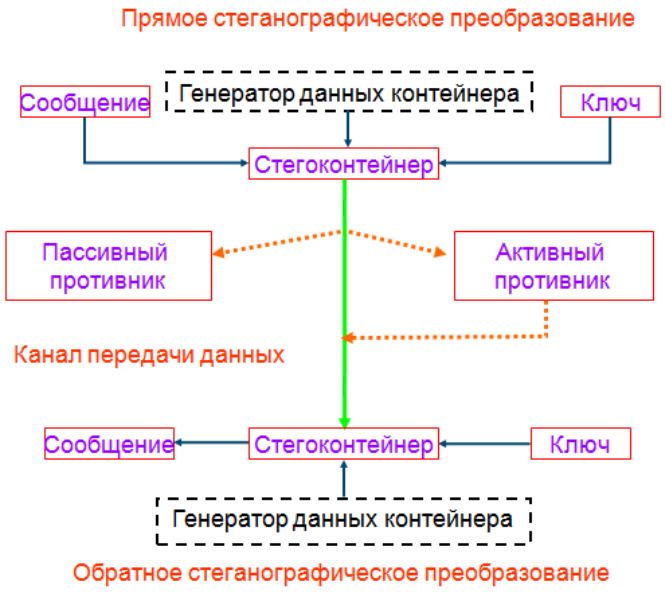
Ответ: ПАРОЛЬ МЕДВЕЖАТА.

Комментарий

Отметим, что схожая по формулировке задача предлагалась и для 11 класса, в которой последовательность расстояний между соседними знаками послания являлась арифметической прогрессией.

В приведенной задаче идет речь о таком методе защиты информации как ***стеганография***. Для решения определенных практических задач информационной безопасности важно не только сделать информацию

недоступной для понимания нарушителем (как известно, это одна из задач, решаемая с помощью криптографии), но и скрыть сам факт ее передачи. Стеганография – это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. Этот термин ввел в 1499 году Иоганн Тритемий в своем трактате «Стеганография», смысл которого был скрыт под видом магической книги. При использовании методов стеганографии передаваемое сообщение может выглядеть как обычное изображение (именно так и есть в данной задаче), видео-, аудио-файл, текстовый документ, сетевой пакет или даже исполняемый файл. Такие файлы, в которых помещается скрываемая информация, называются ***стегоконтейнерами***, при этом, как правило, способ вложения информации в стегоконтейнер зависит от ***ключа*** – секретной информации, определяющей конкретный вид алгоритма сокрытия. Современные методы стеганографии довольно разнообразны и отличаются не только способами вложения информации, но и, также как в криптографии, методами защиты от ***пассивных атак*** (анализ перехваченной информации) и от ***активных атак*** (вмешательство в канал связи, изменение информации).



Стеганографию обычно используют совместно с методами криптографии, например, предварительно зашифровав информацию перед помещением в стегоконтейнер.

Задача 9 (10, 11 классы)

Пусть a_{ij} – число, стоящее в строке с номером i и столбце с номером j квадратной таблицы A (табл. 6). По таблице A построена таблица B, в строке с номером i и столбце с номером j которой стоит выражение $x^{2^{a_{ij}}}$. Набор из

десяти клеток таблицы будем называть «правильным», если в нем присутствуют ровно по одной клетке из каждого столбца и каждой строки. Вычисляются произведения элементов, входящих в правильные наборы. Результатом являются выражения вида x^n. Найдите наибольшую возможную степень правильного набора (число n) и число правильных наборов степени 1023.

Решение

Наибольшая возможная степень правильного набора получается при перемножении элементов, стоящих в таблице $\boldsymbol{B}$ на местах, соответствующих местам в таблице $\boldsymbol{A}$, которые в табл. 6 выделены жирным шрифтом. Поэтому наибольшая степень равна $4 \cdot 2^8 + 3 \cdot 2^9 + 3 \cdot 2^4 = 2608$.

Табл. 6

5	6	7	**8**	0	0	0	0	0	0
6	5	**8**	7	0	0	0	0	0	0
7	**8**	5	6	0	0	0	0	0	0
8	7	6	5	0	0	0	0	0	0
0	0	0	0	**9**	0	1	0	0	0
0	0	0	0	0	1	**9**	0	0	0
0	0	0	0	1	**9**	0	0	0	0
0	0	0	0	0	0	0	2	3	**4**
0	0	0	0	0	0	0	3	**4**	2
0	0	0	0	0	0	0	**4**	2	3

Чтобы решить вторую часть задачи, заметим, что верно следующее:

$$1023 = 2^0 + 2^1 + \cdots + 2^9.$$

Отсюда следует, что искомый коэффициент равен числу таких наборов по 10 элементов, стоящих в различных строках и столбцах в табл. 6, в которых каждое число от 0 до 9 встречается по одному разу. Любой такой набор распадается на 3 набора: набор с числами 2, 3, 4 в нижнем правом квадрате, набор с числами 0, 1, 9 в центральном квадрате и набор с числами 5, 6, 7, 8 в верхнем левом квадрате. Непосредственной проверкой убеждаемся в том, что в каждом из указанных квадратов соответственно имеется 3, 3 и 8 таких наборов, следовательно, общее число наборов равно $3 \cdot 3 \cdot 8 = 72$.

Ответ: 2608; 72.

Комментарий

Каждый из трех рассмотренных в данной задаче квадратов является ***латинским квадратом***. Латинским квадратом n-го порядка называется таблица L размера $n \times n$, заполненная символами некоторого -элементного

множества M таким образом, что в каждой строке и в каждом столбце каждый символ из M встречается ровно один раз. Так, например, верхний левый квадрат в таблице является латинским квадратом размера 4×4 для множества $M = \{5,6,7,8\}$. «Правильный» набор в латинском квадрате такой, что в нем присутствуют все элементы множества M ровно по одному разу, называется его ***трансверсалью***. Ясно, что в данной терминологии, вторая часть приведенной задачи сводится к нахождению числа трансверсалей в каждом из трех выделенных латинских квадратов. Впервые латинские квадраты (4-го порядка) были опубликованы в книге «Шамс аль Маариф» («Книга о Солнце Гнозиса»), написанной Ахмадом аль-Буни в Египте приблизительно в 1200 г. Свое название латинские квадраты получили благодаря математику Леонарду Эйлеру, который в качестве множества M использовал буквы латинского алфавита.

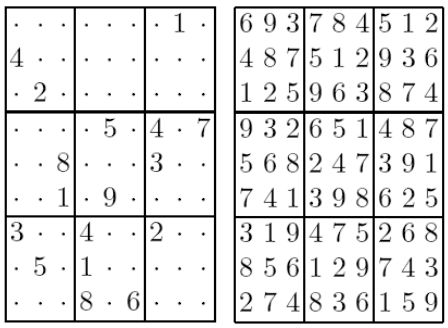


Рис. 6

Латинские квадраты находят широкое применение в алгебре, комбинаторике, статистике, криптографии, теории кодирования и многих других областях науки. Кроме того существует ряд игр, использующих латинские квадраты. Одной из таких игр является «судоку». В ней требуется дополнить таблицу до латинского квадрата размера 9×9 так, чтобы все девять его подквадратов содержали по одному разу все натуральные числа от 1 до 9 (см. рис. 6).