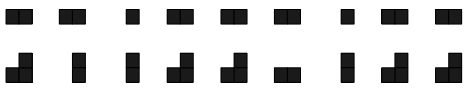
Избранные задачи Межрегиональной олимпиады школьников по математике и криптографии

УСЛОВИЯ И РЕШЕНИЯ ЗАДАЧ

Задача 1

Цепочка ПТИУААМДЛ получена перестановкой букв в некотором слове. Имеется последовательность цифр, задающая порядок, в котором надо выписать буквы цепочки для получения исходного слова. Каждая цифра записывалась в прямоугольный шаблон размера 5 на 3 пикселей по образцу

При передаче часть пикселей на местах, одинаковых для каждой цифры, стерлись. Получилось вот что:



Восстановите исходное слово и перехваченную перестановку.

Решение задачи 1

Исходя из характера стертых пикселей, нетрудно восстановить возможную перестановку, которой соответствуют варианты слов.

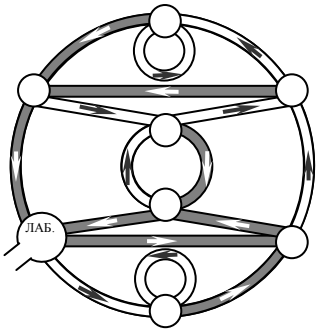
3			3	3			3	3		И			И	**И**			И	И
5		1	5	5		4	5	5		**А**		**П**	А	А		П	А	А
6	7		6	6	2		6	6		А	**М**		А	А	**Т**		А	**А**
8		4	8	8		1	8	8		Д		У	Д	Д		**У**	**Д**	Д
9			9	9			9	9		Л			**Л**	Л			Л	Л

Ответ: слово – АМПЛИТУДА, перестановка – (571932486) или (671932485).

Задача 2

На космической станции, состоящей из отсеков (круглых комнат) и соединяющих их коридоров, произошел сбой электроснабжения, в результате чего связь с роботом, работающим на станции, прервалась. После восстановления работы станции выяснилось, что движение по коридорам, половина из которых оказались неосвещенными, возможно только по

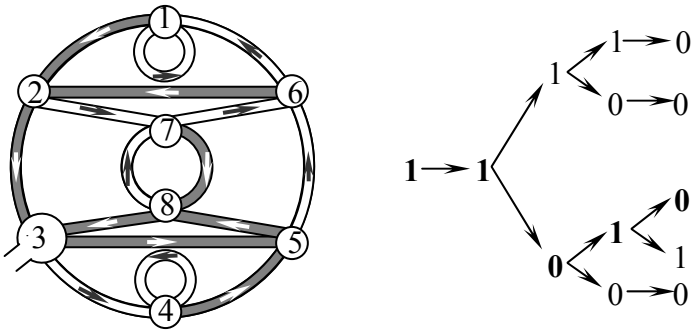
направлениям, указанным на схеме и занимает 1 минуту для каждого коридора. При этом неизвестно, в каком отсеке находится робот. Робот управляется командами из нулей и единиц, при этом 0 соответствует движению по освещенному коридору, а 1 – по неосвещенному. Передайте команду роботу, которая приведет его из любой комнаты в лабораторию (где находится выход). С момента начала движения робота его энергоснабжения хватит не более, чем



на 5 минут.

Решение задачи 2

Для решения поставленной задачи, найдем пути длины 5, ведущих ИЗ заданной вершины (лаборатории, вершины №3), то есть куда и по каким коридорам за 5 шагов можно попасть из этой вершины, двигаясь ПРОТИВ стрелок. Сначала из нее можно попасть в вершины №8 и №2 и двигаться можно только по неосвещенным коридорам. Из вершин №8 и №2 ведут пути только по неосвещенным коридорам в вершины №7, №5 и №1, 6 и т.д. Это приводит к построению дерева поиска, приведенного на рисунке. Остаётся перебрать 6 вариантов, считывая последовательности справа налево. Истинный вариант: 01011 (выделен жирным).



Задача 3

Число n представляется в виде произведение двух чисел $n = p \cdot q$. Найти эти числа и привести решение, если известно, что

А. $n = 40003200063$, а $|p - q| = 2$.

Б. $n = 40000398401$, а p, q – простые и $|p - q| \le 100$.

Решение задачи 3

для А): $p = x - 1,\ q = x + 1,\ 40003200063 = x^2 - 1, x^2 = 40003200064$.

Нетрудно заметить, что $40003200064 = (200000 + z)^2$ и $z \in \{1, 2, \ldots, 9\}$ (небольшое). Число 40003200064 заканчивается на 64, следовательно $z = 8$. (**ответ:** $p = 200007,\ q = 200009$)

для Б): $n = x^2 - t^2, x^2 = n + t^2$, t – маленькое, $x > \sqrt{n}$. Из представленных чисел легко определяется целая часть корня $\sqrt{n}$. Это число – 200000. Оно увеличивается на единицу и возводится в квадрат (первый кандидат на x) и из полученного вычитается число n (кандидат для t^2). Проверяется, извлекается ли квадратный корень – он извлекается сразу же для первого кандидата и равен 40.

(**ответ:** $p = 199961,\ q = 200041$)

Задача 4

Для зашифрования сообщения на русском языке его записывают в одну строку без пробелов и знаков препинания. Заглавные буквы заменяются на строчные. В получившейся цепочке буквы нумеруются слева направо $1, 2, ..., L$. Зашифрование происходит путем перестановки букв исходной цепочки по следующему правилу. Фиксируем два натуральных числа a и b. Буква с номером n в исходной цепочке должна в зашифрованной цепочке иметь номер, равный остатку от деления числа $a \cdot n + b$ на L (с одним исключением: если $a \cdot n + b$ нацело делится на L, то остаток полагается равным L). Например, если длина цепочки $L = 25$ и $a = 9, b = 11$, то третья буква исходной цепочки будет тринадцатой в зашифрованной цепочке (т.к. $9 \cdot 3 + 11 = 38$, а число 38 дает остаток 13 при делении на 25). Известно, что в результате применения этого метода зашифрования к цепочке из 43 букв

светитнезнакомаязвездасновамыоторваныотдома

была получена цепочка

таытоеонсоовзмевтрадазедвмаянтоаысзаимнонвк

При этих же значениях a, b проведено зашифрование еще некоторой цепочки из 38 букв. Получилось вот что:

видхьврлмаояооаоддсемдроиввоеозтообнзо

Найдите значения a и b и восстановите исходное сообщение.

Решение задачи 4

Для начала найдём в открытом тексте две уникальные буквы (по возможности близкие). Это например К и Я, стоящие соответственно на 12 и 16 позициях в открытом тексте. В шифрованном тексте они стоят соответственно на 43 и на 28. Составляем систему уравнений

$$\begin{cases} 12a + b = 43k \\ 16a + b = 28 + 43l \end{cases}$$

Вычитая, получаем уравнение $4a = 28 + 43m$, при $m = 0$ находим $a = 7$, из первого уравнения находим $b = 2$.

Расшифровав второй текст, получим:

морозвоеводадозоромобходитвладеньясвои

Задача 5 (10 класс)

Для зашифрования фразы был взят кубик Рубика с нанесенными на гранях русскими буквами. Развертка кубика показана на рис. 1. Три его грани повернули по часовой стрелке на 90°. При этом грань с меньшим номером поворачивалась раньше, чем грань с большим номером. Затем каждая буква фразы отыскивалась на грани кубика и заменялась на букву этой же грани, которая следует за ней по часовой стрелке (так, например, для рис. 1 буква **А** перейдет в букву **Б**, буква **П** в **С**). Буквы, находящиеся в центре грани, не заменялись. Известно, что перед шифрованием запятая во фразе заменялась на **ЗПТ**, точка – на **ТЧК**, а пробелы пропускались. Получилось:

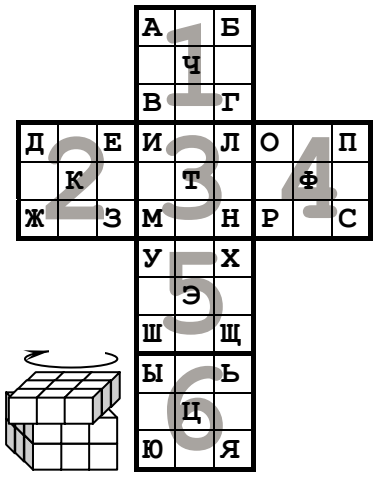


Рис. 1

ЕПОЕЬРИТСГХЖЗТЯПСТАПДСБИСТЧК.

Прочтите исходное сообщение.

Решение задачи 5

Поскольку при данном способе шифрования буквы Т, Ч, К, Ф, Э, Ц не изменяются, то можно предположить, что одна из букв Т в шифрованном тексте принадлежит трёхбуквенному сочетанию ЗПТ:

ЕПОЕЬРИТСГХЖЗТЯПСТАПДСБИСТЧК
ЗПТ ЗПТ ЗПТ

Предположим, что это сочетание ЖЗТ. Из этого следует, что при шифровании З переходит в Ж, а П переходит в З. Рассмотрим все возможные варианты поворота трёх граней и выделим из них те, при которых такие переходы возможны (см. табл. 1).

Таблица 1

1	2	3	4	5	6	З→Ж	П→З
0	0	0	1	1	1	+	-
0	0	1	1	1	0	-	
0	1	1	1	0	0	+	-
1	1	1	0	0	0	+	-
0	0	1	0	1	1	-	
0	0	1	1	0	1	-	
0	1	0	1	1	0	-	
0	1	1	0	1	0	-	
1	0	1	1	0	0	-	
1	1	0	1	0	0	+	-
0	1	0	0	1	1	-	
0	1	1	0	0	1	+	-
1	0	0	1	1	0	+	-
1	1	0	0	1	0	-	
1	**0**	**0**	**0**	**1**	**1**	+	+
1	1	0	0	0	1	+	-
0	1	0	1	0	1	+	-
1	0	1	0	1	0	-	
1	0	0	1	0	1	-	
1	0	1	0	0	1	-	

Рассмотрим первый случай: 000111, который говорит о том, что поворачивалась грань 4, 5 и затем 6. Отследим движение выделенных букв исходя из такого вращения (рис. 2, первая строка). Тогда буква З и П при

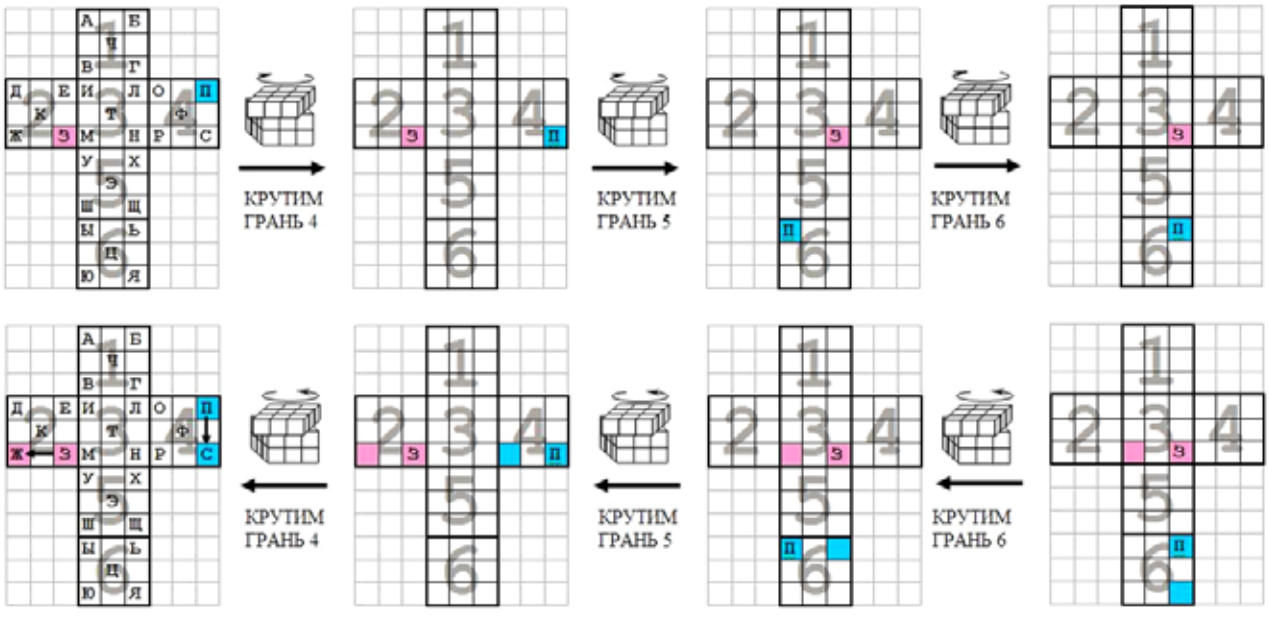


Рис. 2

шифровании будут переходить в буквы, стоящие в соответствующих окрашенных ячейках (рис. 2, вторая строка, справа). Совершая обратное преобразование, находим эти буквы. Таким образом, при таком движении З переходит в Ж, а П в З не переходит, о чем делаем отметку в табл. 1. Продолжаем эту процедуру для других возможных комбинаций движения и заполняем табл. 1. Для перехода З→Ж существует девять вариантов. Отбросим из них те, для которых не возможен переход П→З. Остаётся один вариант: **100011**. Значит, чтобы получить кубик, на котором проводилось шифрование, необходимо один раз повернуть первую грань, пятую и шестую. Расшифровывая сообщение, получим открытый текст: **ДОЖДУСЬТЕБЯЗПТМОЕТВОРЕНЬЕТЧК**. Здесь отметим, что для других вариантов расположения **ЗПТ** получается либо нечитаемый текст, либо нарушаются условия перехода выделенных букв.

Ответ: "Дождусь тебя, моё творенье."

Задача 6 (8-10 класс)

Для доступа к общему почтовому ящику в Интернете Катя и Юра пользуются паролем **СВЕЧА**. Катя решает сменить этот пароль на новый (осмысленное слово русского языка из пяти букв). Новый пароль передается по сети Юре в зашифрованном виде. Зашифрование осуществляется так: первые буквы нового и старого пароля заменяются числами согласно табл. 2, затем эти числа складываются, а полученная сумма заменяется остатком от деления на 33. Таким же образом затем поступают со вторыми буквами паролей, затем с третьими и т.д. После процедуры расшифрования Юра получил нечитаемый пароль из английских букв: **SARCL**. Оказалось, что программа расшифрования Юры была настроена на работу с английским алфавитом. При этом перед расшифрованием программа приводила числовые значения поступившего зашифрованного пароля и старого пароля к остаткам от деления на 26, а расшифрование заключалось в нахождении их разностей (к отрицательной разнице прибавлялось число 26), которые приводились к буквенному виду согласно табл. 1. Помогите Юре понять, какой новый пароль установила Катя.

Таблица 1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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	0

Решение задачи 6

Рассмотрим сумму полученного нового пароля **SARCL** и известного старого пароля **СВЕЧА**, от числовых значений которого взяты остатки от деления на 26, и от значений полученной суммы также возьмём остатки от деления на 26:

$$\begin{array}{ccccc} S & A & R & C & L \\ + & & & & \\ C & B & E & Ч & A \end{array} = \begin{array}{ccccc} 19 & 1 & 18 & 3 & 12 \\ + & & & & \\ 19 & 3 & 6 & 25 & 1 \end{array} = 12 \quad 4 \quad 24 \quad 2 \quad 13.$$

Таким образом, получено зашифрованное сообщение, переданное Катей и искаженное на приемном конце программой Юры. На самом деле зашифрование осуществлялось в русском алфавите, поэтому для некоторых числовых значений зашифрованного сообщения могли быть варианты:

$$12 \quad \begin{array}{c} 4 \\ 4+26 \end{array} \quad 24 \quad \begin{array}{c} 2 \\ 2+26 \end{array} \quad 13 \;=\; 12 \quad \begin{array}{c} 4 \\ 30 \end{array} \quad 24 \quad \begin{array}{c} 2 \\ 28 \end{array} \quad 13.$$

Вычитаем теперь числовые значения старого пароля в русском алфавите $19 \quad 3 \quad 6 \quad 25 \quad 1$, и возьмём от полученных разностей остатки от деления на 33:

$$26 \quad \begin{array}{c} 1 \\ 27 \end{array} \quad 18 \quad \begin{array}{c} 10 \\ 3 \end{array} \quad 12 \;=\; Ш \quad \begin{array}{c} А \\ Щ \end{array} \quad Р \quad \begin{array}{c} И \\ В \end{array} \quad К.$$

Единственный читаемый вариант – ШАРИК.

Ответ: ШАРИК

Задача 7 (8-10 класс)

Четыре фразы на русском языке записываются без знаков препинания и пробелов. Для зашифрования каждой фразы используются неизвестные последовательности цифр $x_1, x_2, \ldots$. Буквы во фразе последовательно заменяются на пары цифр согласно табл. 2 (к одноразрядным числам слева дописывается **0**: например, **А** будет заменяться на **01**). Зашифрование состоит в преобразовании получившейся цепочки цифр по следующему правилу. К первой цифре цепочки прибавляем цифру x_1 и записываем последнюю цифру суммы, потом ко второй цифре цепочки прибавляем x_2 и также записываем последнюю цифру суммы и т.д. Результат зашифрования выглядит следующим образом:

1) 0436389637110156289614062778022668915272874106897713780236

2) 9039139733062534159224233576011442716092 71

3) 1791509407749724556782203674236517597 1

4) 3703532519925327917085909750657981901587194945023834835000452922

Известно, что две фразы зашифрованы с помощью одной и той же последовательности. Укажите, какие именно (ответ обосновать).

Решение задачи 7

Заметим, что на нечетных местах исходного текста могут появляться только цифры 0,1,2 и 3. Поэтому, если из одного шифртекста вычесть другой, зашифрованный с помощью той же последовательности, на нечетных местах разности могут получиться не любые цифры, а только 0,1,2,3,7,8,9, что будет являться критерием для выбора искомых цепочек.

Ответ: первая и вторая.
