XIX Межрегиональная олимпиада школьников по математике и криптографии

Задачи для 10 класса

Решение задачи 1

Сначала заметим, что если $N = pq$, где p и q – простые числа, то количество натуральных чисел, меньших N и взаимно простых с N равно $(p-1)(q-1)$ (обозначим это число $\varphi(N)$). Действительно, всего имеется $pq-1$ натуральных чисел, меньших N. Из них не взаимно-просты с N те числа, которые делятся либо на p, а именно $p, 2p, \text{К}, (q-1)p$ (всего $(q-1)$ чисел), либо на q, это числа $q, 2q, \text{К}, (p-1)q$ (всего $(p-1)$ чисел). Значит

$$\varphi(N) = pq-1-(p-1)-(q-1) = pq-p-q+1 = (p-1)(q-1).$$

Получаем систему уравнений: $\begin{cases} pq = N \\ (p-1)(q-1) = \varphi(N) \end{cases}$; или $\begin{cases} pq = N \\ p+q = N+1-\varphi(N) \end{cases}$.

По теореме Виета получаем, что p и q – корни уравнения

$$x^2 - (N+1-\varphi(N))x + N = 0.$$

$N = 202718099$, $\varphi(N) = 202687920$, и уравнение имеет вид $x^2 - 30180x + 202718099 = 0$. Корень из дискриминанта равен $\sqrt{D} = \sqrt{99960004}$. Чтобы извлечь квадратный корень из этого числа, можно заметить, что результат должен быть немного меньше, чем 10000, причем последняя цифра в этом числе должна быть 2 или 8. Претендентами будут следующие числа: 9998, 9992, 9988, 9982… Последовательно возводя их в квадрат, находим: $9998^2 = 99960004$. Итак:

$$x_1 = \frac{30180-9998}{2} = 10091 = p; \quad x_2 = \frac{30180+9998}{2} = 20089 = q.$$

Ответ: 10091 и 20089.

Решение задачи 2

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

ЕПОЕЬРИТСГХЖЗТЯПСТАПДСБИСТЧК
ЗПТ ЗПТ ЗПТ

Предположим, что это сочетание ЖЗТ. Отсюда 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 свидетельствует о том, что поворачивались грани 4, 5 и затем 6. Проследим движение выделенных букв, исходя из такого вращения (рис. 2, первая строка). Заметим, что буквы З и П при шифровании будут переходить в бук-

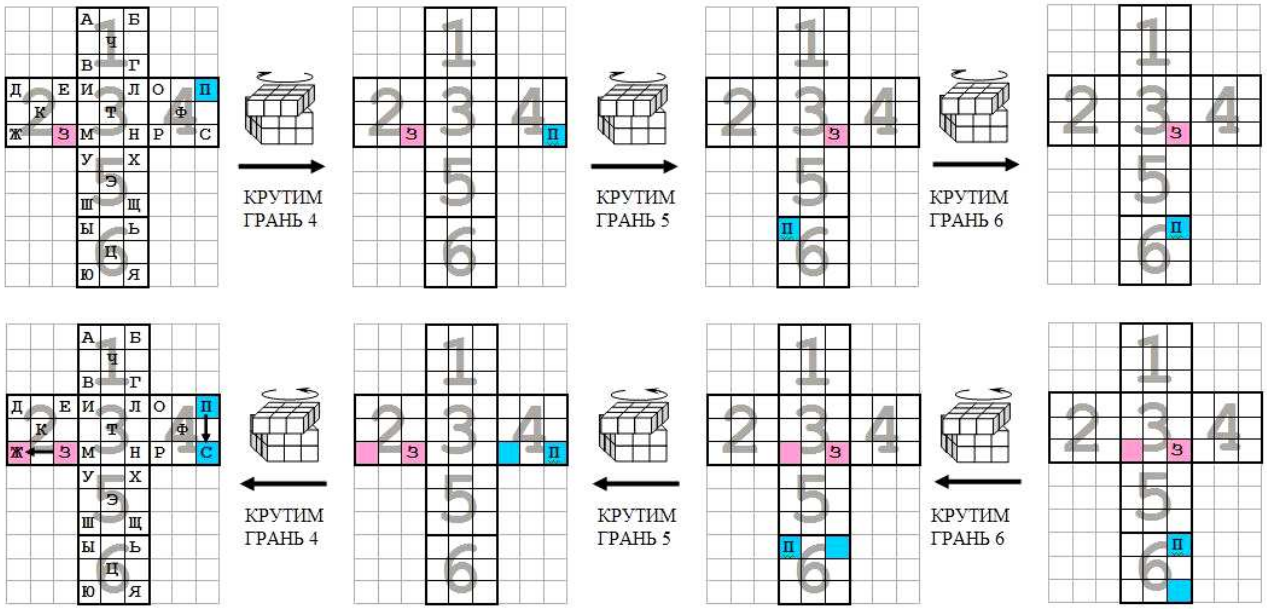

Рис. 2

вы, стоящие в соответствующих окрашенных клетках (рис. 2, вторая строка, справа). Совершая обратное преобразование, находим эти буквы. Таким образом, при указанном движении З переходит в Ж, а П в З не переходит, о чем сделаем отметку в табл. 1. Продолжая эту процедуру для других возможных комбинаций движения, заполняем табл. 1. Для перехода $З \to Ж$ существует девять вариантов. Отбросим из них те, для которых невозможен переход $П \to З$. Остаётся один вариант: **100011**. Следовательно, чтобы получить кубик, на котором проводилось шифрование, необходимо по одному разу повернуть первую грань, пятую и шестую. Расшифровывая сообщение, получим открытый текст:

ДОЖДУСЬТЕБЯЗПТМОЕТВОРЕНЬЕТЧК

Отметим, что для других вариантов расположения триграммы **ЗПТ** получается либо нечитаемый текст, либо нарушаются условия перехода выделенных букв.

Ответ: Дождусь тебя, моё творенье.

Решение задачи 3

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

$$\begin{matrix} S & A & R & C & L \\ + & & & & \\ С & В & Е & Ч & А \end{matrix} = \begin{matrix} 19 & 1 & 18 & 3 & 12 \\ + & & & & \\ 19 & 3 & 6 & 25 & 1 \end{matrix} = 12 \quad 4 \quad 24 \quad 2 \quad 13.$$

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 возможны варианты:

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

Вычтем теперь из полученных числовых вариантов зашифрованного пароля числовые значения старого пароля в русском алфавите $19 \quad 3 \quad 6 \quad 25 \quad 1$:

$$-7 \quad \begin{matrix} 1 \\ 27 \end{matrix} \quad 18 \quad \begin{matrix} -23 \\ 3 \end{matrix} \quad 12$$

и возьмём от полученных разностей остатки от деления на 33, получим:

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

Единственный читаемый вариант – ШАРИК.

Ответ: ШАРИК

Решение задачи 4

Заметим, что 12=3+3+3+3, 13=7+3+3, 14=7+7. Таким образом, имеется три подряд идущих чисел, которые представимы в требуемом виде. Очевидно, что все последующие числа получаются прибавлением или к 12, или к 13, или к 14 нужного числа монет достоинством 3 единицы. Остается перебором чисел от 1 до 11 найти цены, которые нельзя устанавливать.

Приведем здесь еще одно решение этой задачи, несколько более «математизированное», но вместе с тем познавательное и поучительное.

Фактически надо найти числа *x,y* такие, что $ax+by=n$ (в данном случае, $a=3,\ b=7$). Уравнение $ax+by=n$, где НОД(*a,b*)=1, неразрешимо в неотрицательных целых числах *x, y* при $n=F(a,b)=ab-a-b$ и разрешимо при всех натуральных $n>F(a,b)=ab-a-b$. Число *F*(*a,b*) называется числом Фробениуса для пары *(a,b)*. Чтобы заметить это покажем, что каждое из равносильных уравнений

$$ax+by=ab-a-b;\ a(x+1)+b(y+1)=ab;\ ax'+by'=c$$

не имеет натуральных решений $x',\ y'$ при $c=ab$ и имеет такие решения при всех $c>ab$. Пусть при натуральных *a, b,* $x',\ y'$ выполнено $ax'+by'=ab$. Тогда $ax'=b(a-y')$, т.е. x' делится на *b* (так как НОД(*a,b*)=1 и у чисел *a,b* нет общих делителей, кроме 1). Следовательно $x'\ge b$. Тогда $ax'+by'>ab$. Пусть *c*>*ab,* тогда, в силу условия НОД(*a,b*)=1, найдутся такие натуральные *u,v* (алгоритм Евклида), что $au-bv=c>ab$, т.е. $\frac{u}{b}-\frac{v}{a}>1$. Следовательно, найдется такое натуральное *t,* что $\frac{u}{b}>t>\frac{v}{a}$. Для этого *t* зададим натуральные числа $x',\ y'$ следующим образом: $x'=u-bt,\ y'=at-v$. Тогда

$$ax'+by'=a(u-bt)+b(at-v)=au-bv=c.$$

Ответ: $\{1,2,4,5,8,11\}$.

Решение задачи 5

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.

Решение задачи 6

Пусть в двоичной системе счисления $A=(x_n,...,x_0)$. Тогда $A_1=(x_3,x_2,x_1,x_0)$, $A_2=(x_4,x_3,x_2,x_1)$, $A_3=(x_5,x_4,x_3,x_2)$. Следовательно,

$$a_1\oplus a_2=(A_1\oplus B)\oplus(A_2\oplus B)=A_1\oplus A_2=(x_3\oplus x_4,x_2\oplus x_3,x_1\oplus x_2,x_0\oplus x_1),$$

$$a_3\oplus a_2=(A_3\oplus B)\oplus(A_2\oplus B)=A_3\oplus A_2=(x_5\oplus x_4,x_4\oplus x_3,x_3\oplus x_2,x_2\oplus x_1).$$

Итак, если вычислить $a_1 \oplus a_2$, то три младших бита $a_3 \oplus a_2$ будут найдены, а старший бит будет произвольным.

Вычислим значение $a_1 \oplus a_2$:

$$\begin{array}{cccc} 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 0 \end{array}.$$

Тогда возможные значения $(a_2 \oplus a_3)$ имеют вид $(*,1,1,1)$, и $a_3 = a_2 \oplus (a_3 \oplus a_2)$:

$$\begin{array}{cccc} 1 & 0 & 1 & 0 \\ \hline * & 1 & 1 & 1 \\ \hline * & 1 & 0 & 1 \end{array}.$$

Итак, $a_3 = 13$, либо $a_3 = 5$. Можно убедиться в том, что оба варианты верны, если рассмотреть последовательности с параметрами $A = 20$, либо $A = 52$ и $B = 0$.

Ответ: 13 и 5.

Критерии определения победителей и призеров XIX межрегиональной олимпиады школьников по математике и криптографии

Жюри XIX Межрегиональной олимпиады школьников по математике и криптографии установило следующие критерии определения победителей и призеров среди учащихся 10 классов:

1 место – решены пять задач (возможно с одним существенным недостатком);

2 место – решены четыре задачи (возможно с одним существенным недостатком);

3 место – решены три задачи (возможно с одним существенным недостатком).