XIX

МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

10 КЛАСС

Р Е Ш Е Н И Я

ВАРИАНТ 1

Решение 1.

Сначала заметим, что если $N = pq$, где p и q – простые числа, количество натуральных чисел, меньших N и взаимно простых с N равно $(p-1)(q-1)$ (обозначим это число как $\varphi(N)$). Это можно понять, если составить таблицу, содержащую p строк и q столбцов в ячейках которой значком "–" отмечать те числа вида $t_1 \cdot t_2$, $t_1 \in \{1,...,p\}$, $t_2 \in \{1,...,q\}$, которые содержат с $\varphi(N)$ общие сомножители, а "+" – которые не содержат.

	1	2	…	$q-1$	q
1	+	+	…	+	–
2	+	+	…	+	–
⋮	⋮	⋮	⋮	⋮	⋮
$p-1$	+	+	…	+	–
p	–	–		–	–

Поэтому, получаем систему: $\begin{cases} pq = N \\ (p-1)(q-1) = \varphi(N) \end{cases}$; $\begin{cases} pq = N \\ p+q = N+1-\varphi(N) \end{cases}$.

По теореме Виета получаем, что p и q – решения квадратного уравнения:

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

В представленной задаче $N = 200970851$, $\varphi(N) = 200940792$ и квадратное уравнение примет вид:

$$x^2 - (200970851+1-200940792)x + 200970851 = 0;$$

$$x^2 - 30060x + 200970851 = 0.$$

Тогда:

$$\sqrt{D} = \sqrt{30060^2 - 4 \cdot 200970851} = \sqrt{903603600 - 803883404} = \sqrt{99720196}.$$

Для того, 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 равна 4 или 6. Тогда претендентами будут следующие числа: 9996, 9994, 9986, 9984 … Начинаем последовательно возводить их в квадрат, в результате находим: $9986^2 = 99720196$. Итак:

$$x_1 = \frac{30060 - 9986}{2} = 10037 = p;$$

$$x_2 = \frac{30060 + 9986}{2} = 20023 = q.$$

ОТВЕТ: 10037 и 20023

Решение 2.

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 4.

Полученное английское слово переводится в числовой вид и формируются столбцы длины 3: букве переданного русского пароля может соответствовать данное числовое значение, либо значение плюс 7, либо минус 7 (табл. 1).

ОТВЕТ: ШАРИК

Решение 5.

Пусть в двоичной системе координат $A = (x_n,...,x_0)$. 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 $a_1 \oplus a_2$:

```
1 0 0 1
0 1 1 0
-------
1 1 1 1
```

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

```
0 1 1 0
* 1 1 1
-------
* 0 0 1
```

ОТВЕТ: 9 и 1.

X I X

МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

10 КЛАСС

ВАРИАНТ 1

Р Е Ш Е Н И Я

Решение 6.

Фактически надо найти x,y такие, что $ax+by=n$. Уравнение $ax+by=n$, в котором 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)*. В самом деле, покажем, что уравнение $ax+by=c$ 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*, откуда $x\geq b$, тогда $ax+by>ab$. Пусть *c>ab* тогда в силу НОД(*a,b*)=1 найдутся такие натуральные *u,v*, что $au-bv=c>ab$, т.е. $\frac{u}{b}-\frac{v}{a}>1$.

Следовательно, найдется такое натуральное *t*, что $\frac{u}{b}>t>\frac{v}{a}$.При этом t зададим натуральные числа $x=u-bt, y=at-v$. Тогда

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

Перебором чисел от 1 до 17 находим не возможные значение. Любое значение 18 и более возможно.

ОТВЕТ:{1,2,3,5,6,9,10,13,17}

Решение 3.

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. Предположим, что это сочетание ВЗТ. Из этого следует, что при шифровании З->В и П->З. Рассмотрим все возможные варианты поворота трёх граней и выделим из них те, при которых такие переходы возможны:

1	2	3	4	5	6	З->В	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	-	

Для перехода З->В существует шесть вариантов. Отбросим из них те, в которых не возможен переход П->З. Остаётся один вариант: **101100**. Значит, чтобы получить куб, на котором проводилось шифрование, необходимо один раз повернуть первую грань, третью и четвёртую. Расшифровывая сообщение, получим открытый текст: ПРИВЕТЗПТМОИСВЕТЛЫЕДУМЫТЧК. Здесь отметим, что для других вариантов расположения ЗПТ получается нечитаемый текст.

ОТВЕТ: "Привет, мои светлые думы."

XIX

МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

10 КЛАСС

РЕШЕНИЯ

ВАРИАНТ 2

Решение 1.

Сначала заметим, что если $N = pq$, где p и q – простые числа, количество натуральных чисел, меньших N и взаимно простых с N равно $(p-1)(q-1)$ (обозначим это число как $\varphi(N)$). Это можно понять, если составить таблицу, содержащую p строк и q столбцов в ячейках которой значком "–" отмечать те числа, вида $t_1 \cdot t_2$, $t_1 \in \{1,...,p\}, t_2 \in \{1,...,q\}$, которые содержат с $\varphi(N)$ общие сомножители, а "+" – которые не содержат.

	1	2	…	$q-1$	q
1	+	+	…	+	–
2	+	+	…	+	–
⋮	⋮	⋮	⋮	⋮	⋮
$p-1$	+	+	…	+	–
p	–	–		–	–

Поэтому, получаем систему: $\begin{cases} pq = N \\ (p-1)(q-1) = \varphi(N) \end{cases}; \begin{cases} pq = N \\ p+q = N+1-\varphi(N) \end{cases}.$

По теореме Виета получаем, что p и q – решения квадратного уравнения:

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

В представленной задаче $N = 201071131$, $\varphi(N) = 201041064$ и квадратное уравнение примет вид:

$$x^2 - 30068x + 201071131 = 0.$$

Тогда:

$$\sqrt{D} = \sqrt{99800100}.$$

Для того, 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 0. Тогда претендентами будут следующие числа: 9990, 9980, 9970… Начинаем последовательно возводить их в квадрат, в результате находим: $9990^2 = 99800100$. Итак:

$$x_1 = \frac{30068 - 9990}{2} = 10039 = p;$$

$$x_2 = \frac{30068 + 9990}{2} = 20029 = q.$$

ОТВЕТ: 10039 и 20029.

Решение 2.

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 четвертая.

Решение 4.

Полученное английское слово переводится в числовой вид и формируются столбцы длины 3: букве переданного русского пароля может соответствовать данное числовое значение, либо значение плюс 7, либо минус 7 (табл. 1).

ОТВЕТ: ЩЕПКА

Решение 5.

Пусть в двоичной системе координат $A = (x_n,...,x_0)$. 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 $a_1 \oplus a_2$

```
1 0 1 0
0 1 0 0
-------
1 1 1 0
```

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

```
0 1 0 0
* 1 1 1
-------
* 0 1 1
```

ОТВЕТ: 11 и 3.

X I X

МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

10 КЛАСС

Р Е Ш Е Н И Я

ВАРИАНТ 2

Решение 6.

Фактически надо найти x,y такие, что $ax+by=n$. Уравнение $ax+by=n$, в котором 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)*. В самом деле, покажем, что уравнение $ax+by=c$ 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*, откуда $x\geq b$, тогда $ax+by>ab$. Пусть *c>ab* тогда в силу НОД(*a,b*)=1 найдутся такие натуральные *u,v*, что $au-bv=c>ab$, т.е. $\frac{u}{b}-\frac{v}{a}>1$.

Следовательно, найдется такое натуральное *t*, что $\frac{u}{b}>t>\frac{v}{a}$.При этом t зададим натуральные числа $x=u-bt, y=at-v$. Тогда

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

Перебором чисел от 1 до 11 находим не возможные значение. Любое значение 12 и более возможно.

ОТВЕТ:{1,2,4,5,8,11}.

Решение 3.

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. Предположим, что это сочетание ЖЗТ. Из этого следует, что при шифровании З->Ж и П->З. Рассмотрим все возможные варианты поворота трёх граней и выделим из них те, при которых такие переходы возможны:

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	-	

Для перехода З->Ж существует шесть вариантов. Отбросим из них те, в которых не возможен переход П->З. Остаётся один вариант: **100011**. Значит, чтобы получить куб, на котором проводилось шифрование, необходимо один раз повернуть первую грань, четвёртую и пятую. Расшифровывая сообщение, получим открытый текст: ДОЖДУСЬТЕБЯЗПТМОЕТВОРЕНЬЕТЧК. Здесь отметим, что для других вариантов расположения ЗПТ получается нечитаемый текст.

ОТВЕТ: "Дождусь тебя, моё творенье."