XXXIV

Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии

УСЛОВИЯ И РЕШЕНИЯ

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

11 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Функция от 4-х переменных $f(x,y,z,t)$, где $x,y,z,t \in \mathbb{R}$ обладает свойствами:

1) $f(x,0,0,t) = xt$; 2) $f(z,t,x,y) = -f(x,y,z,t)$; 3) $f(x,y,z+\lambda x, t+\lambda y) = f(x,y,x,t)$ для всех $\lambda \in \mathbb{R}$.

Найдите $f(100,101,102,103)$.

2. Найдите все решения системы сравнений $\begin{cases} x^2 = 1 (mod\ 33) \\ x \cdot y^2 = 1 (mod\ 33) \end{cases}$, где $x,y \in \{1,2,\dots,32\}$.

3. В канале связи, имеющим пять входов и пять выходов (Рис. 1), информация передается по пяти линиям. Для обеспечения секретности входы и выходы «перемешивают» (делают, например, так, чтобы сигнал, поданный на вход линии 1, в итоге пришел бы, скажем, на выход линии 4 и т.п.). Для этого некоторые пары линий соединены блоками. Каждый из 8-ми блоков независимо от других находится в одном из двух состояний: *верхняя линия на вход – верхняя на выход, нижняя на вход – нижняя на выход* (Рис. 2а) либо *верхняя на вход – нижняя на выход, нижняя на вход – верхняя на выход* (Рис. 2б). Сколькими способами можно выбрать состояния блоков так, чтобы «перемешивания» не было, то есть, если подать сигнал на вход 1, то он придет на выход 1, сигнал, поданный на вход 2, придет на выход 2 и т.д.?

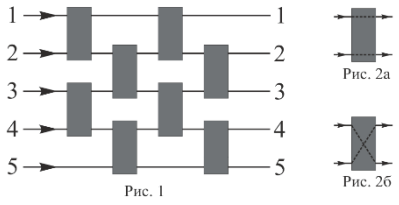


Рис. 1

Рис. 2а

Рис. 2б

4. Знайка использует для зашифрования таблицу:

$$B = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Произвольное сообщение $(x_1, x_2, \dots, x_t)$, состоящее из цифр $\{1,2,3,4\}$ на ключе $(k_1, k_2, \dots, k_t)$, $k_i \in \{1,2,3,4\}$ преобразуется в шифртекст $\left(b_{k_1 x_1}, b_{k_2 x_2}, \dots, b_{k_t x_t}\right)$. Например, сообщение $(4,3,1,1)$ на ключе $(1,2,4,4)$ даст шифртекст $(4,1,2,2)$. Незнайка решает для

пущей надежности добавить шифрование на этом же ключе $(k_1, k_2, \dots, k_t)$, но с использование другой таблицы D также размером 4×4. Какими свойствами должна обладать таблица D, чтобы после двукратного шифрования с использование таблиц B и D имелась возможность по известным открытому и шифрованному текстам однозначно восстанавливать ключ? Приведите пример подходящей таблицы D.

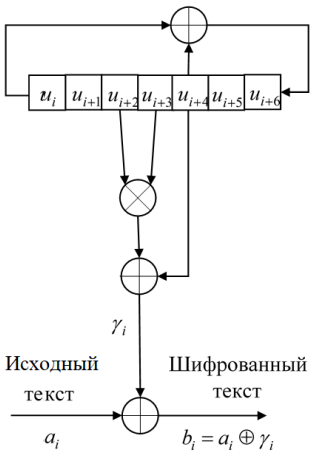
5. Шифрование цифрового текста задается следующим правилом. Каждая цифра x текста заменяется цифрой с помощью функции $f(x) = (b \cdot (x^3 + a) + c)(mod 10)$, $x, a, b, c \in \{0,1, \dots, 9\}$. При каких a, b, c возможно однозначное расшифрование? Найдите многочлен расшифрования при $b = 3$. Ответ обоснуйте.

6. Для зашифрования текста на русском языке его буквы заменяются наборами из 0 и 1 длины 5 по таблице 1. Затем вырабатывается секретная последовательность (*гамма*) $\gamma_0, \gamma_1, \dots$, также состоящая из 0 и 1, и с ее помощью i-я буква исходного текста $\boldsymbol{a_i} = (a_{5i}, a_{5i+1}, a_{5i+2}, a_{5i+3}, a_{5i+4})$, $i = 0,1,2, \dots$ заменяется буквой $\boldsymbol{b_i}$ по правилу:

$$\boldsymbol{b_i} = (a_{5i} \oplus \gamma_{5i}, a_{5i+1} \oplus \gamma_{5i+1}, a_{5i+2} \oplus \gamma_{5i+2}, a_{5i+3} \oplus \gamma_{5i+3}, a_{5i+4} \oplus \gamma_{5i+4}).$$

Здесь $\oplus$ – стандартная операция сложения битов: $0 \oplus 0 = 1 \oplus 1 = 0, 0 \oplus 1 = 1 \oplus 0 = 1$. Далее $\boldsymbol{b_i}$ заменяется на букву из таблицы 1.

Гамму получают с помощью изображенного на рисунке устройства следующим образом: сначала выбирается ключ $k = (u_0, u_1, \dots, u_6), u_i \in \{0,1\}$ и его биты последовательно слева направо записывают в семь ячеек *регистра сдвига*.



На i-м такте работы регистра производятся следующие действия:

1) вычисляется знак гаммы $\gamma_i = u_{i+2}u_{i+3} \oplus u_{i+4}$;

2) вычисляется значение $u_{i+7} = u_i \oplus u_{i+4}$;

3) заполнение регистра сдвигается на одну ячейку влево, при этом в крайнюю правую ячейку записывается значение u_{i+7}.

Например, после нулевого такта работы заполнение регистра будет таким: $(u_1, u_2, \dots, u_6, u_7)$, где $u_7 = u_0 \oplus u_4$ При этом $\gamma_0 = u_2u_3 \oplus u_4$. После первого такта регистр примет вид $(u_2, u_3, \dots, u_6, u_7, u_8)$, где $u_8 = u_1 \oplus u_5$. Очередной знак гаммы будет равен $\gamma_1 = u_3u_4 \oplus u_5$.

В результате зашифрования был получен текст **щнщшйхс**. Также известны первая и вторая буквы исходного текста **ст**. Найдите ключ k и исходный текст.

Таблица 1

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
00000	00001	00010	00011	00100	00101	00110	00111	01000	01001	01010	01011	01100	01101	01110	01111	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001	11010	11011	11100	11101	11110	11111

РЕШЕНИЯ ЗАДАЧ

Задача 1

Докажем, что при $x \neq 0$ и $(xt - yz) \neq 0$ функция имеет вид $f(x, y, z, t) = xt - yz$.

Положим $\lambda = -\frac{z}{x}$. $f(x, y, x, t) = \{\text{по свойству 3)}\} = f(x, y, z + \lambda x, t + \lambda y) = f\left(x, y, 0, t - \frac{zy}{x}\right) = \{\text{по свойству 2)}\} = -f\left(0, t - \frac{zy}{x}, x, y\right) = \{\text{по свойству 3)}\} = -f\left(0, t - \frac{zy}{x}, x + \mu \cdot 0, y - \mu \cdot \left(t - \frac{zy}{x}\right)\right) = \left\{\text{положим } \mu = \frac{xy}{zy - xt} \text{ и по свойству 2)}\right\} = -f\left(0, t - \frac{zy}{x}, x, 0\right) = \{\text{по свойству 2)}\} = f\left(x, 0, 0, t - \frac{zy}{x}\right) = \{\text{по свойству 1)}\} = x\left(t - \frac{zy}{x}\right) = xt - yz.$

Утверждение доказано.

Тогда $f(100,101,102,103) = 100 \cdot 103 - 101 \cdot 102 = -2$.

ОТВЕТ: -2.

Задача 2

Для решения сравнения $x^2 = 1(mod\ 33)$ (*) решим вначале сравнение $x^2 = 1(mod\ 11)$. Отсюда $x_1 = 1(mod\ 11)$, или $x_2 = -1(mod\ 11)$.

Или $x_1 = 1 + 11n,\ x_2 = -1 + 11n, t \in \mathbb{Z}$. Подставляя x_1 и x_2 в (*) найдем все решения сравнения (*): $x = 1, x = -1, x = 10, x = 23$.

Подставим найденные x в сравнение $x \cdot y^2 = 1(mod\ 33)$ (**).

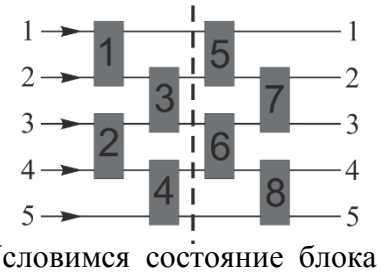
Для $x = 1$ получим $y = 1, y = -1, y = 10, y = 23$.

Для $x = -1, x = 10$ проверим, что ни одно из сравнений $x \cdot y^2 = 1(mod\ 11)$ не имеет решений. А следовательно, и $x \cdot y^2 = 1(mod\ 33)$ не имеет решений.

Для $x = 23$ сравнение $23 \cdot y^2 = 1(mod\ 3)$ не имеет решений.

ОТВЕТ: (1,1), (1,10), (1,23), (1,32).

Задача 3



Воспользуемся методом «встречи посередине». На рисунке эта «середина» отмечена вертикальным пунктиром. Занумеруем блоки. Выпишем все 16 перестановок, которые могут осуществить блоки с номерами 1,2,3,4. Потом составим список из 16 перестановок, которые осуществят блоки 8,7,6,5 – причем именно в таком порядке, поскольку двигаться мы должны в обратном направлении: от выхода к «середине» (пунктиру). Затем лишь останется найти в этих списках одинаковые перестановки. Условимся состояние блока обозначать 0, если он перестановку не осуществляет (см. Рис. 2а в условии задачи), и 1, если осуществляет (Рис. 2б). В приведенных двух списках имеется 8 пар одинаковых перестановок (отмечены одинаковыми цифрами). Таким образом, всего имеется 8 состояний блоков, реализующих тождественную перестановку.

ОТВЕТ: 8.

Задача 4

Двукратное шифрование с использованием таблиц X и D равносильно однократному шифрованию с использованием таблицы $X = B * D = \begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \\ x_{41} & x_{42} & x_{43} & x_{44} \end{pmatrix}$.

Тогда однозначное нахождение ключа по любой паре открытого и шифрованного текстов возможно только при отсутствии повторяющихся элементов в каждом столбце таблицы X.

1 2 3 4		8 7 6 5	
0 0 0 0	1 2 3 4 5 I	0 0 0 0	1 2 3 4 5 I
0 0 0 1	1 2 3 5 4 VIII	0 0 0 1	2 1 3 4 5 III
0 0 1 0	1 3 2 4 5 V	0 0 1 0	1 2 4 3 5 IV
0 0 1 1	1 3 2 5 4 VII	0 0 1 1	2 1 4 3 5 VI
0 1 0 0	1 2 4 3 5 IV	0 1 0 0	1 3 2 4 5 V
0 1 0 1	1 2 4 5 3	0 1 0 1	3 1 2 4 5
0 1 1 0	1 4 2 3 5	0 1 1 0	1 3 4 2 5
0 1 1 1	1 4 2 5 3	0 1 1 1	3 1 4 2 5
1 0 0 0	2 1 3 4 5 III	1 0 0 0	1 2 3 5 4 VIII
1 0 0 1	2 1 3 5 4 II	1 0 0 1	2 1 3 5 4 II
1 0 1 0	2 3 1 4 5	1 0 1 0	1 2 5 3 4
1 0 1 1	2 3 1 5 4	1 0 1 1	2 1 5 3 4
1 1 0 0	2 1 4 3 5 VI	1 1 0 0	1 3 2 5 4 VII
1 1 0 1	2 1 4 5 3	1 1 0 1	3 1 2 5 4
1 1 1 0	2 4 1 3 5	1 1 1 0	1 3 5 2 4
1 1 1 1	2 4 1 5 3	1 1 1 1	3 1 5 2 4

Пример подходящей таблицы: $D = \begin{pmatrix} 1 & 4 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \end{pmatrix}$. Тогда $X = B * D = \begin{pmatrix} 1 & 4 & 2 & 3 \\ 2 & 3 & 1 & 4 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

Задача 5

Очевидно, что a, c любые, $a, c \in \{0,1,\dots,9\}$. Заметим (проверим!), что функция $g(x) = x^3 (mod 10)$ задает взаимно однозначное отображение множества $\{0,1,\dots,9\}$ в множество $\{0,1,\dots,9\}$. А тогда однозначное расшифрование возможно только при условии $\text{НОД}\{b, 10\} = 1$.

ОТВЕТ: a, c любые, $b \in \{1,3,7,9\}$. Многочлен расшифрования $h(x) = 3x^3 - 3a - c (mod 10)$.

Задача 6

Поскольку известны первые две буквы открытого текста, но можем вычислить следующие знаки гаммы:

$$\vec{\gamma}_0 = (\gamma_0, \dots, \gamma_4) = \vec{a}_0 \oplus \vec{b}_0 = c \oplus \text{щ} = (10001) \oplus (11001) = (01000),$$

$$\vec{\gamma}_1 = (\gamma_5, \dots, \gamma_9) = \vec{a}_1 \oplus \vec{b}_1 = \text{т} \oplus \text{н} = (10010) \oplus (01101) = (11111).$$

Основное наблюдение заключается в том, что для определения ключа могут быть опробованы лишь два бита вместо семи: u_2, u_3. При известных битах u_{i+2}, u_{i+3} и известном бите γ_i бит u_{i+4} определяется однозначно: $u_{i+4} = u_{i+2} \cdot u_{i+3} \oplus \gamma_i$. Если опробуемый вариант u_{i+2}, u_{i+3} неверный, то с высокой вероятностью возникнут противоречия с известными и вырабатываемыми знаками гаммы. Определим ключ k и открытый текст. Будем перебирать все возможные варианты u_2, u_3.

Пусть $(u_2, u_3) = (0,0)$. Тогда

i	u_i	u_{i+1}	u_{i+2}	u_{i+3}	u_{i+4}	u_{i+5}	u_{i+6}	γ_i
0	*	*	0	0	$0 \cdot 0 \oplus 0 = 0$	*	*	0
1	*	0	0	0	$0 \cdot 0 \oplus 1 = 1$	*	*	1
2	0	0	0	1	$0 \cdot 1 \oplus 0 = 1$	*	*	0
3	0	0	1	1	$1 \cdot 1 \oplus 0 = 1$	*	$0 \oplus 1 = 1$	0
4	0	1	1	1	$1 \cdot 1 \oplus 0 = 1$	1	$0 \oplus 1 = 1$	0
5	1	1	1	1	1	1	$0 \oplus 1 = 1$	$1 \neq 1 \cdot 1 \oplus 1$

С одной стороны, $\gamma_5 = 1$, с другой стороны $\gamma_5 = u_7 \cdot u_8 \oplus u_9 = 1 \cdot 1 \oplus 1 = 0$. Получили противоречие. Следовательно, $(u_2, u_3) \neq (0,0)$.

Пусть $(u_2, u_3) = (0,1)$. Тогда

i	u_i	u_{i+1}	u_{i+2}	u_{i+3}	u_{i+4}	u_{i+5}	u_{i+6}	γ_i
0	*	*	0	1	$0 \cdot 1 \oplus 0 = 0$	*	*	0
1	*	0	1	0	$1 \cdot 0 \oplus 1 = 1$	*	*	1
2	0	1	0	1	$0 \cdot 1 \oplus 0 = 0$	*	*	0
3	1	0	1	0	$1 \cdot 0 \oplus 0 = 0$	*	$0 \oplus 1 = 1$	0
4	0	1	0	0	$0 \cdot 0 \oplus 0 = 0$	1	$1 \oplus 0 = 1$	0
5	1	0	0	0	1	1	$0 \oplus 0 = 0$	1
6	0	0	0	1	1	0	$1 \oplus 0 = 1$	1
7	0	0	1	1	0	1	$0 \oplus 1 = 1$	1
8	0	1	1	0	1	1	$0 \oplus 1 = 1$	1
9	1	1	0	1	1	1	$0 \oplus 0 = 0$	1
10	1	0	1	1	1	0	$1 \oplus 1 = 0$	0
11	0	1	1	1	0	0	$1 \oplus 1 = 0$	1
12	1	1	1	0	0	0	$0 \oplus 1 = 1$	0
13	1	1	0	0	0	1	$1 \oplus 0 = 1$	0

i	u_i	u_{i+1}	u_{i+2}	u_{i+3}	u_{i+4}	u_{i+5}	u_{i+6}	γ_i
14	1	0	0	0	1	1	$1 \oplus 0 = 1$	1
15	0	0	0	1	1	1	$1 \oplus 0 = 1$	1
16	0	0	1	1	1	1	$0 \oplus 1 = 1$	0
17	0	1	1	1	1	1	$0 \oplus 1 = 1$	0
18	1	1	1	1	1	1	$0 \oplus 1 = 1$	0
19	1	1	1	1	1	1	$1 \oplus 1 = 0$	0
20	1	1	1	1	1	0	$1 \oplus 1 = 0$	0
21	1	1	1	1	0	0	$1 \oplus 1 = 0$	1
22	1	1	1	0	0	0	$1 \oplus 1 = 0$	0
23	1	1	0	0	0	0	$1 \oplus 0 = 1$	0
24	1	0	0	0	0	1	$1 \oplus 0 = 1$	0
25	0	0	0	0	1	1	$1 \oplus 0 = 1$	1
26	0	0	0	1	1	1	$0 \oplus 0 = 0$	1
27	0	0	1	1	1	0	$0 \oplus 1 = 1$	0
28	0	1	1	1	0	1	$0 \oplus 1 = 1$	1
29	1	1	1	0	1	1	$0 \oplus 1 = 1$	1
30	1	1	0	1	1	1	$1 \oplus 0 = 1$	1
31	1	0	1	1	1	1	$1 \oplus 1 = 0$	0
32	0	1	1	1	1	0	$1 \oplus 1 = 0$	0
33	1	1	1	1	0	0	$0 \oplus 1 = 1$	1
34	1	1	1	0	0	1	$1 \oplus 1 = 0$	0

Таким образом, получаем $\vec{\gamma}_2 = (01001), \vec{\gamma}_3 = (10000), \vec{\gamma}_4 = (01000), \vec{\gamma}_5 = (11011),$
$\vec{\gamma}_6 = (10010).$

Следовательно,

$$a_2 = b_2 \oplus \gamma_2 = (11001) \oplus (01001) = (10000) = \text{Р},$$
$$a_3 = b_3 \oplus \gamma_3 = (11000) \oplus (10000) = (01000) = \text{И},$$
$$a_4 = b_4 \oplus \gamma_4 = (01001) \oplus (01000) = (00001) = \text{Б},$$
$$a_5 = b_5 \oplus \gamma_5 = (10101) \oplus (11011) = (01110) = \text{О},$$
$$a_6 = b_6 \oplus \gamma_5 = (10001) \oplus (10010) = (00011) = \text{Г}.$$

Таким образом, **открытый текст – «стрибог»**.

Из таблицы получаем, что

$$(u_2, u_3, u_4, u_5, u_6, u_7, u_8) = (0,1,0,1,0,0,0).$$

Поскольку $u_7 = u_0 \oplus u_3$, то $u_0 = u_3 \oplus u_7 = 1 \oplus 0 = 1$. Аналогично, $u_1 = u_4 \oplus u_8 = 0 \oplus 0 = 0$. **Следовательно,**

$$\boldsymbol{k = (u_0, u_1, u_2, u_3, u_4, u_5, u_6) = (1, 0, 0, 1, 0, 1, 0)}.$$

Варианты $(u_2, u_3) = (1,0)$, $(u_2, u_3) = (1,1)$ могут быть отбракованы аналогично случаю $(u_2, u_3) = (0,0)$. Кратко продемонстрируем это.

Пусть $(u_2, u_3) = (1,0)$. Тогда

i	u_i	u_{i+1}	u_{i+2}	u_{i+3}	u_{i+4}	u_{i+5}	u_{i+6}	γ_i
0	*	*	1	0	0	*	*	0
1	*	1	0	0	1	*	*	1
2	1	0	0	1	0	*	*	0
3	0	0	1	0	0	*	0	0
4	0	1	0	0	0	0	0	0
5	1	0	0	0	0	0	1	$1 \neq u_{i+2} \cdot u_{i+3} \oplus u_{i+4}$

Пусть $(u_2, u_3) = (1,1)$. Тогда

i	u_i	u_{i+1}	u_{i+2}	u_{i+3}	u_{i+4}	u_{i+5}	u_{i+6}	γ_i

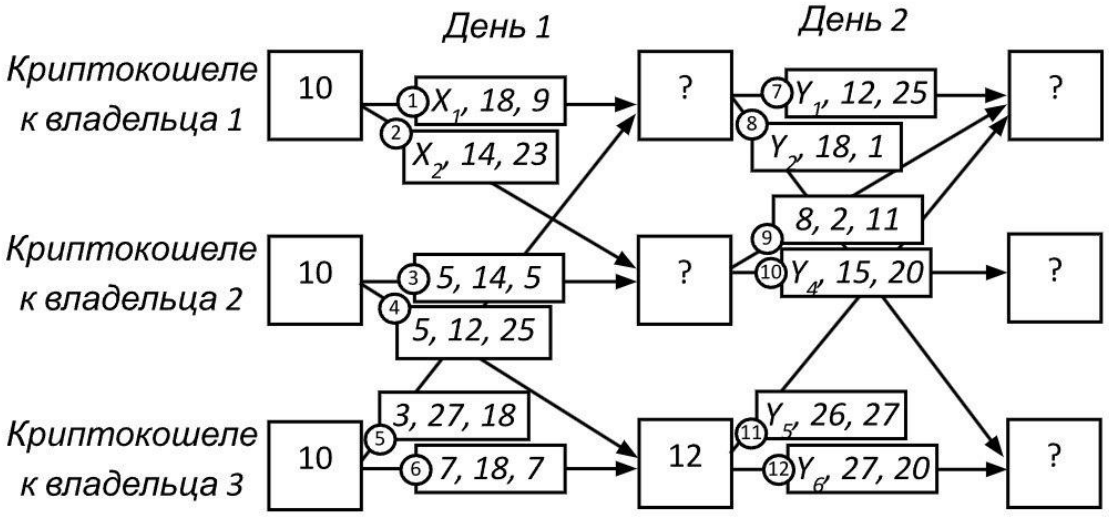
0	*	*	1	1	1	*	*	0
1	*	1	1	1	0	*	*	1
2	1	1	1	0	0	*	*	0
3	1	1	0	0	0	*	1	0
4	1	0	0	0	0	1	1	0
5	0	0	0	0	1	1	1	1
6	0	0	0	1	1	1	0	1
7	0	0	1	1	1	0	1	$1 \neq u_{i+2} \cdot u_{i+3} \oplus u_{i+4}$

ОТВЕТ: СТРИБОГ, $\boldsymbol{k = (u_0, u_1, u_2, u_3, u_4, u_5, u_6) = (1, 0, 0, 1, 0, 1, 0)}$.

ОТБОРОЧНЫЙ ЭТАП

11 КЛАСС

1. Каждый из трех владельцев криптокошельков имеет на своем счету по 10 криптокойнов. Каждый из двух дней ими совершаются по две транзакции: по переводу части криптокойнов со своего криптокошелька на криптокошелек другого владельца и по возврату оставшихся криптокойнов обратно на свой кошелек. У каждого имеется свой секретный ключ $S \in \{1, \dots, 28\}$. При совершении транзакции указываются три числа (X, a, b), где X - число переводимых криптокойнов, (a, b) - электронная подпись перевода. Электронная подпись находится по правилу: выбираем произвольное $k \in \{1, \dots, 28\}$, затем находим $a = r_{29}(2^k)$, $b = r_{28}(Xa + Sk)$, где $r_N(M)$ - остаток от деления числа M на N. На рисунке указаны совершенные транзакции (пронумерованы числами в кружках) за два дня. Сколько будет криптокойнов у каждого владельца криптокошелька по окончании двух дней? В качестве ответа запишите три числа через запятую, начиная с количества криптокойнов первого владельца. Например, 5,7,9.



2. В криптосистеме RSA (знания алгоритма шифрования не требуется для решения задачи) элементы надёжности определяются несколькими параметрами. В частности, выбором числа $N = pq$, где p, q - различные нечётные простые числа, и значением $\varphi(N) = (p-1)(q-1)$. Известно следующее утверждение: для всех $x \in \{1,2, \dots, N-1\}$ $x^{\frac{\phi(N)}{2}+1} = x(mod N)$. Используя это, найдите p и q, если известно, что $N = 78012331$ и $x^{38997333} = x(mod N)$ для всех $x \in \{1,2, \dots, N-1\}$. Запишите значения p и q в порядке возрастания через запятую. Примечание: запись $a = b(mod\ k)$ означает, что целые числа a и b имеют одинаковые остатки от деления на натуральное число k.

3. Квадратная таблица размером 1997x1997 заполнена натуральными числами от 1 до 1997 так, что в каждой строке присутствуют все числа от 1 до 1997. Найдите сумму чисел, стоящих на диагонали, которая соединяет левый верхний и правый нижний углы таблицы, если заполнение таблицы симметрично относительно этой диагонали. В качестве ответа запишите целое число.

4. Шифрпреобразование простой замены в алфавите $A = \{a_1, \dots a_n\}$, состоящем из n различных букв, заключается в замене каждой буквы шифруемого текста буквой того же алфавита, причём разные буквы заменяются разными. Ключом шифра простой замены называется таблица, в которой указано, какой буквой надо заменить каждую букву алфавита А. Если слово КНИГА зашифровать простой заменой с помощью ключа:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
Ч	Я	Ю	Э	Ы	Ь	Щ	Ш	Ц	Х	Ф	У	Б	Д	Т	З	В	Р	П	М	Л	К	А	И	О	Ж	Е	С	Г	Н

то получится слово ХБЦЭЧ. Зашифровав полученное слово с помощью того же ключа ещё раз, получим слово ЛЯКСА. Сколько всего различных слов (включая слово КНИГА) можно получить, если указанный процесс шифрования продолжать неограниченно? В качестве ответа укажите целое число.

5. Пусть $a_1, a_2, a_3, \ldots$ и $b_1, b_2, b_3, \ldots$ - числовые последовательности периодов 18 и 2346 соответственно. Найдите период последовательности $a_1, b_1, a_2, b_2, a_3, b_3 \ldots$ (Периодом последовательности $x_1, x_2, x_3, \ldots$ называется такое наименьшее натуральное число T, что для всех натуральных n верно равенство $x_{n+T} = x_n$). В качестве ответа запишите целое число
6. Вася хочет заполнить квадратную таблицу (криптографическую мозаику) размера 4x4 целыми числами от 0 до 16 по следующему правилу. Сначала он выбирает четыре целых числа $b_1, b_2, b_3, b_4 \in \{0,1, \ldots, 16\}$. Затем первую строку Вася заполняет числами $a_i^{(1)} = (b_i + 1)(mod 17), i = 1,2,3,4$, вторую строку - числами $a_i^{(2)} = (b_i + 4)(mod 17), i = 1,2,3,4$, третью $a_i^{(3)} = (b_i + 13)(mod 13), i = 1,2,3,4$, и, аналогично, четвертую $a_i^{(4)} = (b_i + 16)(mod 17), i = 1,2,3,4$. При этом числа b_1, b_2, b_3, b_4 Вася выбрать должен так, чтобы все числа в таблице оказались различными и не было числа 0. Чему равны b_1, b_2, b_3, b_4? Ответ записать в виде четырёх чисел, упорядоченных по возрастанию и перечисленных через запятую.

ОТВЕТЫ

1) 24,1,5.
2) 8669,8999.
3) 1995003.
4) 390.
5) 14076.
6) 2,8,9,15.