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

УСЛОВИЯ И РЕШЕНИЯ

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

9 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) $f(x,y,z+\lambda x,t+\lambda y) = f(x,y,z,t)$ для всех $\lambda \in \mathbb{R}$. Найдите $f(1,2,3,4)$.

2. Найдите все решения системы сравнений $\begin{cases} x^2 = 1 (mod\ 15) \\ x \cdot y^2 = 1 (mod\ 15) \end{cases}$, где $x,y \in \{1,2,\dots,14\}$.

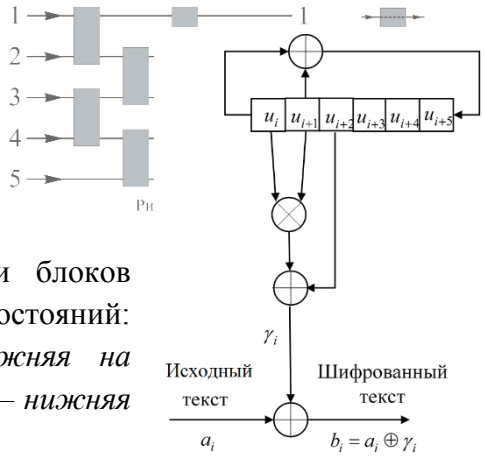
3. Шифрование цифрового текста задается следующим правилом. Каждая цифра x текста заменяется цифрой с помощью функции $f(x) = (b \cdot (x^3 + a) + c)(mod 10)$, $x,a,b,c \in \{0,1,\dots,9\}$. При каких a,b,c возможно однозначное расшифрование? Ответ обоснуйте.

4. 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? Ответ обоснуйте.

Для зашифрования открытого текста $\boldsymbol{x} = (x_1,x_2,x_3,x_4)$, состоящего из цифр 1,2,3,4, Знайка использует таблицу $B = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, а также секретный ключ $\boldsymbol{k} = (k_1,k_2,k_3,k_4)$, тоже состоящий из цифр 1,2,3,4. В результате он получает шифрованный текст $\boldsymbol{b} = \left(b_{k_1x_1}, b_{k_2x_2}, b_{k_3x_3}, b_{k_4x_4}\right)$. Например, текст $(4,3,1,1)$ на ключе $(1,2,4,4)$ дал бы шифртекст $(4,1,2,2)$. Незнайка для пущей надежности тем же способом зашифровал текст $\boldsymbol{b}$ на этом же ключе $\boldsymbol{k}$, но с использованием другой (отличной от B) таблицы D размером 4×4 (также составленной из цифр 1,2,3,4). В результате такого двойного шифрования получился текст $\boldsymbol{d}$. Пусть нам известны открытый текст $\boldsymbol{x}$, ему соответствующий дважды зашифрованный текст $\boldsymbol{d}$, а также таблицы B,D. Можно ли по ним найти ключ $\boldsymbol{k}$? Не всегда. Если, например, $D = \begin{pmatrix} 3 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \end{pmatrix}$, то после двойного зашифрования (сначала по B, потом по D)

открытый текст $\boldsymbol{x} = (4,4,4,4)$ и на ключе $(1,1,1,1)$, и на ключе $(2,2,2,2)$ даст один и тот же шифртекст $\boldsymbol{d} = (2,2,2,2)$, а значит ключ однозначно не определится. Какими свойствами должна обладать таблица D, чтобы, имея в своем распоряжении произвольную пару $\boldsymbol{x}, \boldsymbol{d}$ и таблицы B, D, ключ однозначно удалось бы восстановить? Приведите пример подходящей таблицы D.

5. 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).



Покажите, что: а) два таких канала (как на Рис.1), в которых состояния блоков отличаются, могут тем не менее давать одинаковые «перемешивания», б) не всякое «перемешивание» такой канал реализовать сможет.

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*) $\gamma_0, \gamma_1, \ldots$, также состоящая из 0 и 1, и с ее помощью i-я буква исходного текста $\boldsymbol{a_i} = (a_{5i}, a_{5i+1}, a_{5i+2,} a_{5i+3}, a_{5i+4})$, $i = 0,1,2, \ldots$ 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 $k = (u_0, u_1, \ldots, u_5), u_i \in \{0,1\}$ и его биты последовательно слева направо записывают в шесть ячеек *регистра сдвига*.

На i-м такте работы регистра производятся следующие действия:

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

2) вычисляется значение $u_{i+6} = u_i \oplus u_{i+1}$;

3) заполнение регистра сдвигается на одну ячейку влево, при этом в крайнюю правую ячейку записывается значение u_{i+6}.

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

В результате зашифрования был получен текст **кцюэив**. Также известны первая и вторая буквы исходного текста **фи**. 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 $f(1,2,3,4) = 1\cdot 4 - 2\cdot 3 = -2$.
ОТВЕТ: -2.

Задача 2

Для решения сравнения $x^2 = 1(mod\ 15)$ (*)

решим вначале сравнение $x^2 = 1(mod\ 5)$. Отсюда $x_1 = 1(mod\ 5)$, или $x_2 = -1(mod\ 5)$.

Тогда $x_1 = 1+5n$, $x_2 = -1+5n$, $t \in \mathbb{Z}$. Подставляя x_1 и x_2 в (*) найдем все решения сравнения (*):

$x = 1, x = -1, x = 11, x = 4$.

Подставим найденные x в сравнение $x\cdot y^2 = 1(mod\ 15)$.

Для $x = 1$ получим $y = 1, y = -1, y = 11, y = 4$.

Для $x = -1$ проверим, что сравнение $-y^2 = 1(mod\ 3)$ не имеет решений. А следовательно, и $-y^2 = 1(mod\ 15)$ не имеет решений.

Для $x = 11$ проверим, что сравнение $11y^2 = 1(mod\ 3)$ не имеет решений. А следовательно, и $11y^2 = 1(mod\ 15)$ не имеет решений.

Для $x = 4$ получим $y = 2, y = 7, y = 8, y = 13$.
ОТВЕТ: $(1,1), (1,14), (1,4), (1,11), (4,2), (4,7), (4,8), (4,13)$.

Задача 3

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, $b \in \{1,3,7,9\}$.

Задача 4

Двукратное шифрование с использование таблиц B и D можно рассматривать как однократное шифрование с использованием таблицы $A = B * D = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$. А тогда однозначное нахождение ключа по любой паре открытого и шифрованнного текстов равносильно тому, что в каждом столбце матрицы A отсутствуют повторяющиеся элементы.

Задача 5

а) Рассмотрим следующие состояния блоков. *Состояние 1*: блок 1 находится в состоянии, изображенном на Рис. 2б условия. Остальные блоки находятся в состоянии, изображенном на Рис. 2а. *Состояние 2*: блок 2 находится в состоянии, изображенном на Рис. 2б условия. Остальные блоки находятся в состоянии, изображенном на Рис. 2а. Состояния 1 и 2 дают, очевидно, одинаковые перемешивания.

б) Невозможно сделать так, чтобы сигнал, поданный на вход 5, пришел бы на выход 1.

Задача 6

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

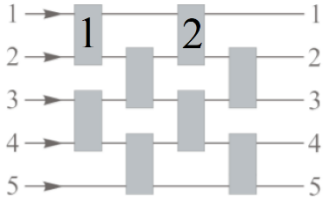
$$\vec{\gamma}_0 = (\gamma_0, \dots, \gamma_4) = \vec{a}_0 \oplus \vec{b}_0 = \text{ф} \oplus \text{к} = (10100) \oplus (01010) = (11110),$$

$$\vec{\gamma}_1 = (\gamma_5, \dots, \gamma_9) = \vec{a}_1 \oplus \vec{b}_1 = \text{и} \oplus \text{ц} = (01000) \oplus (10110) = (11110).$$

Основное наблюдение заключается в том, что для определения ключа могут быть опробованы лишь два бита вместо шести: u_0, u_1. При известных битах u_i, u_{i+1} и известном бите γ_i бит u_{i+2} определяется однозначно: $u_{i+2} = u_i \cdot u_{i+1} \oplus \gamma_i$. Если опробуемый вариант u_i, u_{i+1} 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 $(u_0, u_1) = (0,0)$. Тогда

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



С одной стороны, $\gamma_6 = 1$, с другой стороны $\gamma_6 = u_6 \cdot u_7 \oplus u_8 = 0 \cdot 1 \oplus 0 = 0$. Получили противоречие. Следовательно, $(u_0, u_1) \neq (0,0)$.

Пусть $(u_0, u_1) = (0,1)$. Тогда

i	u_i	u_{i+1}	u_{i+2}	u_{i+3}	u_{i+4}	u_{i+5}	γ_i
0	0	1	1	*	*	*	1
1	1	1	0	*	*	1	1
2	1	0	1	*	1	0	1
3	0	1	1	1	0	1	1
4	1	1	1	0	1	1	0
5	1	1	0	1	1	0	1
6	1	0	1	1	0	0	1
7	0	1	1	0	0	1	1
8	1	1	0	0	1	1	1
9	1	0	0	1	1	0	0
10	0	0	1	1	0	1	1
11	0	1	1	0	1	0	1

i	u_i	u_{i+1}	u_{i+2}	u_{i+3}	u_{i+4}	u_{i+5}	γ_i
12	1	1	0	1	0	1	1
13	1	0	1	0	1	0	1
14	0	1	0	1	0	1	0
15	1	0	1	0	1	1	1
16	0	1	0	1	1	1	0
17	1	0	1	1	1	1	1
18	0	1	1	1	1	1	1
19	1	1	1	1	1	1	0
20	1	1	1	1	1	0	0
21	1	1	1	1	0	0	0
22	1	1	1	0	0	0	0
23	1	1	0	0	0	0	1
24	1	0	0	0	0	0	0
25	0	0	0	0	0	1	0
26	0	0	0	0	1	0	0
27	0	0	0	1	0	0	0
28	0	0	1	0	0	0	1
29	0	1	0	0	0	0	0

Таким образом, получаем $\vec{\gamma}_2 = (11110), \vec{\gamma}_3 = (10110), \vec{\gamma}_4 = (00010), \vec{\gamma}_5 = (00010),$
$\vec{\gamma}_6 = (10010).$

Следовательно,

$$a_2 = b_2 \oplus \gamma_2 = (11110) \oplus (11110) = (00000) = \text{А},$$
$$a_3 = b_3 \oplus \gamma_3 = (11101) \oplus (10110) = (01011) = \text{Л},$$
$$a_4 = b_4 \oplus \gamma_4 = (01000) \oplus (00010) = (01010) = \text{К},$$
$$a_5 = b_5 \oplus \gamma_5 = (00010) \oplus (00010) = (00000) = \text{А}.$$

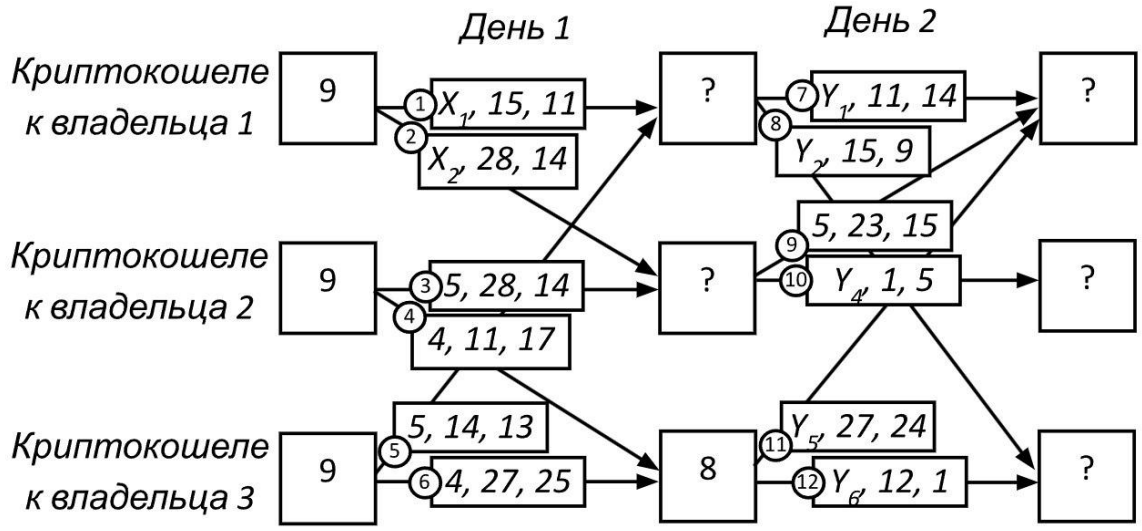
Таким образом, открытый текст – «фиалка», $k = (u_0, u_1, u_2, u_3, u_4, u_5) = (0,1,1,0,1,1)$.
Варианты $(u_0, u_1) = (1,0)$, $(u_0, u_1) = (1,1)$ могут быть отбракованы аналогично случаю $(u_0, u_1) = (0,0)$.

ОТВЕТ: 011011, фиалка.

ОТБОРОЧНЫЙ ЭТАП

9 КЛАСС

1. Каждый из трех владельцев криптокошельков имеет на своем счету по 9 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 $N = 57543757$ и $x^{28764289} = x(mod N)$ 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. Разложите на простые множители число $3^{20} + 3^4 + 1$, если известно, что оно делится на 167. В качестве ответа запишите наибольший простой множитель.

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 ВЕСНА 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 ЮЬВБЧ. Зашифровав полученное слово с помощью того же ключа ещё раз, получим слово ГЖЮЯА. Сколько всего различных слов (включая слово ВЕСНА) 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 16 и 2006 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 8. 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) 17,5,5.
2) 7309,7873.
3) 449.
4) 210.
5) 32096.
6) 0,6,10,16.