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

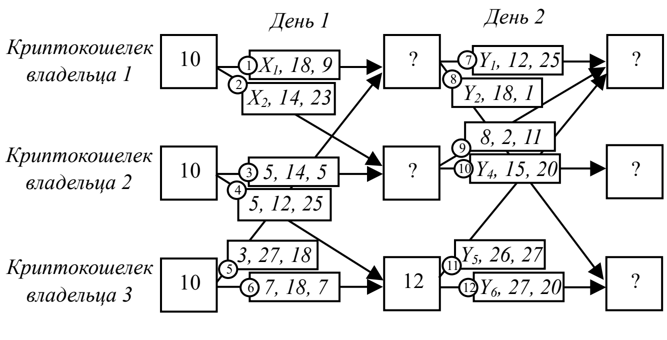
ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

11 КЛАСС

УСЛОВИЯ ЗАДАЧ

1. Катя и Юра играют в следующую игру. Имеется пустая таблица из одной строки, состоящая из $k = 2023^2$ пустых ячеек: $(a_1 \quad ,\dots, \quad a_k)$, которые игроки заполняют числами от 0 до 2022. Первым ходит Юра, который выбирает число t такое, что $1 \le t \le k-1$ и заполняет t ячеек. Второй ходит Катя, которая заполняет оставшиеся ячейки. Победитель определяется по следующему правилу: если в результате получается «счастливая» комбинация чисел – полностью заполненная таблица, в которой числа можно разбить на две непересекающиеся группы, суммы чисел в которых одинаковы, то выигрывает Катя, в противном случае выигрывает Юра. Например, комбинация (7,5,3,4,6) не является «счастливой», так как в ней присутствует нечетное число нечетных чисел. С другой стороны, комбинация (4,5,1,6,8) является «счастливой», так как $4+8=5+1+6$. У кого из игроков имеется выигрышная стратегия? Ответ обосновать.

2. 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$\in \{1,2,\dots,28\}$. 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 $k \in \{1,2,\dots,28\}$, 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?



3. а) перестановка f чисел $\{0,1,\dots,6\}$ задана таблицей:

x	0	1	2	3	4	5	6
$f(x)$	3	2	4	0	5	6	1

Например, $f(2) = 4$. Найдите две различные перестановки g и h такие, что для всех $x \in \{0,1,\dots,6\}$ выполняется

$f(x) = \big(g(x) + h(x)\big)(mod\ 7)$.

b) перестановка f задана на чётном количестве чисел $\{0,1,\ldots,2n-1\}$ таблицей:

x	0	1	2	..	$2n-2$	$2n-1$
f(x)	i_0	i_1	i_2	..	i_{2n-2}	i_{2n-1}

Здесь $(i_0, i_1, \ldots, i_{2n-1})$ – перестановка чисел $\{0,1,\ldots,2n-1\}$.

Докажите, что не существует перестановок g и h таких, что для всех $x \in \{0,1,\ldots,2n-1\}$ выполняется $f(x) = \big(g(x) + h(x)\big)(mod\ (2n))$?

4. В криптосистеме RSA (знания алгоритма шифрования не требуется для решения задачи) элементы надёжности определяются несколькими параметрами. В частности, выбором числа $N = p \cdot q$, где p, q – различные нечётные простые числа, и значением $\varphi(N) = (p-1)\cdot(q-1)$. Известна следующая теорема (малая теорема Ферма): если p – простое число, a – целое число, не делящееся на p, то $a^{p-1} = 1(mod\ p)$. Используя это:

a) докажите, что $x^{\frac{\varphi(N)}{2}+1} = x(mod\ N)$ для всех $x \in \{1,2,\ldots,N-1\}$.

b) найдите p и q, если известно, что $N = 42494861$ и $x^{21240913} = x(mod\ N)$ для всех $x \in \{1,2,\ldots,N-1\}$.

5. Четыре компьютера, расположенные в вершинах квадрата $ABCD$, соединены прямолинейными отрезками проводов с сервером, который находится в точке O пересечения диагоналей. Сторона квадрата равна 2 м. Несложно заметить, что для такого подключения потребуется $4\sqrt{2}$ метров провода. Чтобы уменьшить длину проводов, вам разрешается передвинуть сервер из точки O в любую другую точку O_1, а также компьютер из точки A в любую другую точку A_1 так, чтобы новая суммарная длина проводов $S = O_1A_1 + O_1B + O_1C + O_1D$ была как можно меньше. Разрешается компьютеры и сервер размещать в одной точке (например, точка A_1 может совпасть с точкой B). Компьютеры в вершинах B, C, D двигать нельзя. Чему равно минимальное значение S.

6. Вася хочет заполнить квадратную таблицу (*криптографическую мозаику*) размера 4×4 целыми числами от 1 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 $a_i^{(3)} = (b_i + 13)(mod\ 17), i = 1,2,3,4$ 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. Сумеет ли Вася это сделать? Если да, то чему равны b_1, b_2, b_3, b_4?