

МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

1. Для шифрования сообщения использовалось устройство из трёх последовательно зацепленных шестерёнок с 5, 30 и 6 зубцами (рис.1). На зубцах первой шестерёнки записаны цифры от 1 до 5, а на третьей – от 1 до 6. На второй шестерёнке также по часовой стрелке записан тридцатибуквенный алфавит: **АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЪЭЮЯ**. Для каждой шестерёнки выделено окошко (на рис.1 оно изображено квадратиком), в котором видна лишь одна буква или цифра. Сообщение шифровалось побуквенно: вторая шестерёнка вращалась по часовой стрелке, пока в окошке не появится первая буква сообщения. Затем выписывалась пара цифр, открывшихся в окошках первой и третьей шестерёнок. Далее продолжали вращать вторую шестерёнку до появления второй буквы сообщения, выписывали пару цифр из окошек и т. д. Так для случая, приведенного на рис.1, буква **Б** заменяется парой **52** (подчеркнем, что рисунок лишь поясняет принцип работы устройства, и на самом деле букве **Б** может соответствовать другая пара цифр). Начальное взаимное расположение шестерёнок неизвестно. Найдите по известным выписанным парам цифр

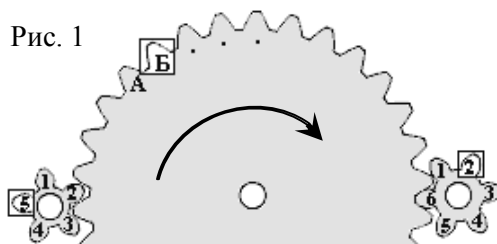


Рис. 1

43 33 55 11 11 31 42 24 32 45 56 13 44 31
55 16 23 55 22 15 56 33 56 15

какое сообщение было зашифровано (пробелы в тексте сохранены).

2. Милла и Стелла разговаривают по телефону и хотят выбрать секретное число так, чтобы оно осталось неизвестным постороннему, возможно подслушивающему разговор. Для этого Милла подбирает натуральное число $a \leq 256$ такое, что числа $r_{257}(a^i)$ – различны при всех $1 \leq i \leq 256$ и $r_{257}(a^{256})=1$, где $r_{257}(t)$ – остаток от деления числа t на 257. Затем Милла загадывает натуральное число $x \leq 256$, а Стелла – натуральное число $y \leq 256$. После этого Милла сообщает числа a и $r_{257}(a^x)$ Стелле, а Стелла ей – число $r_{257}(a^y)$. Теперь они обе вычисляют их секретное число $r_{257}(a^{xy})$. Найдите его, если известно, что $a=6$, $r_{257}(a^x)=4$, $r_{257}(a^y)=251$.

3. Для шифрования SMS-сообщений использовался следующий способ. Первоначально каждый пробел в исходном сообщении заменялся некоторым трёхбуквенным словом. Затем полученная цепочка букв набиралась на клавиатуре с использованием интеллектуального ввода (по типу T9). При этом при вводе каждой буквы осуществлялась лишь однократное нажатие соответствующей клавиши (рис.2), а программа интеллектуального ввода выбирала слово из словаря по следующему принципу: 1-я буква слова выбиралась с 1-й нажатой клавиши, 2-я – со второй и т.д. Полученные таким образом осмысленные слова разделялись запятыми и передавались. Найдите исходное сообщение, соответствующее написанному на экране (рис.2).

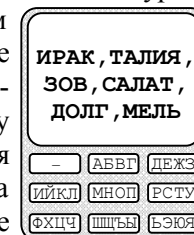


Рис. 2

4. Когда число городов в Криптоландии достигло 5^4 , власти решили провести территориальную реформу, создав 5 провинций по 5^3 городов в каждой. В качестве названий городам планировалось присвоить различные обозначения (a_1, \dots, a_4) – наборы из 4-х целых чисел, в которых a_i принимают значения от 0 до 4. При этом обозначения каждой пары городов из одной провинции должны были отличаться не менее чем в двух позициях. Укажите какой-либо способ построения такой системы названий.

5. Для шифрования передаваемых сообщений Катя и Юра используют следующий способ. Юра заранее выбрал набор коэффициентов (4, 6, 13, 25), натуральное число u и сообщил их Кате. Для шифрования сообщения (x_1, x_2, x_3, x_4) , состоящего из нулей и единиц, Катя вычисляет сумму $S = 4x_1 + 6x_2 + 13x_3 + 25x_4$, а затем находит остаток S' от деления произведения Su на 49 и отправляет S' Юре. Помогите Юре расшифровать сообщение $S'=47$, то есть найти соответствующую ему строку (x_1, x_2, x_3, x_4) , если известно, что остаток от деления числа $13u$ на 49 равен 1.

6. В треугольнике ABC известно: $BC=2$, $AC=2$, угол ACB равен 60° . Точки M и K удовлетворяют условиям: $AM : MC = 1:2$, $BK : CK = 1:2$. Найдите максимально возможное расстояние между точками M и K.