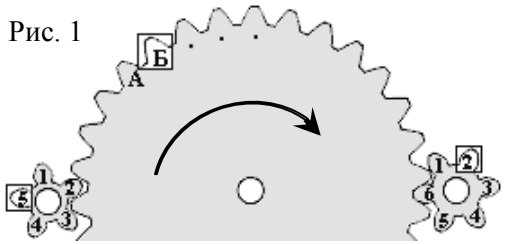
X X I
МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

8-9 КЛАСС

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: **АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ.** 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



11 55 16 53 21 16 31 15 52 14 16 44 46

какое сообщение было зашифровано (пробелы в тексте сохранены).

2. Для шифрования передаваемых сообщений Катя и Юра используют следующий способ. Юра заранее выбрал набор коэффициентов (2, 5, 8, 16), 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 $S = 2x_1 + 5x_2 + 8x_3 + 16x_4$, а затем находит остаток S' от деления произведения Su на 32 и отсылает S' Юре. Помогите Юре расшифровать сообщение S'=11, то есть найти соответствующую ему строку (x_1, x_2, x_3, x_4), если известно, что остаток от деления числа $7u$ на 32 равен 1.

3. Когда число городов в Криптоландии достигло 4^4, власти решили провести территориальную реформу, создав 4 провинции по 4^3 городов в каждой. В качестве названий городам планировалось присвоить различные обозначения $(a_1,...,a_4)$ – наборы из 4-х целых чисел, в которых a_i принимают значения от 0 до 3. 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.

4. 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 осуществлялось 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

5. Крокодил Гена посылает Чебурашке по радиоканалу сообщение, заменяя его буквы наборами из нулей и единиц согласно табл.1 (другие буквы не встретились).

Табл. 1

А	(0,0,0,0,0,0,0)	**Е**	(0,1,1,0,1,0,0)	**Р**	(1,1,0,1,0,0,0)	**Х**	(1,0,1,1,1,0,0)
В	(1,1,1,0,0,0,1)	**И**	(1,0,0,0,1,0,1)	**С**	(0,0,1,1,0,0,1)	**Ч**	(0,1,0,1,1,0,1)
Г	(1,0,1,0,0,1,0)	**М**	(1,1,0,0,1,1,0)	**Т**	(0,1,1,1,0,1,0)	**Ы**	(0,0,0,1,1,1,0)
Д	(0,1,0,0,0,1,1)	**О**	(0,0,1,0,1,1,1)	**У**	(1,0,0,1,0,1,1)	**Я**	(1,1,1,1,1,1,1)

Из-за помех некоторые биты исказились, но не более двух в одном наборе. Определите, какое сообщение отправил крокодил Гена, если Чебурашка получил:
(1,0,0,1,0,1,1) (0,1,0,0,0,1,1) (0,0,1,0,0,0,0) (1,1,0,1,0,0,0) (1,0,1,0,1,1,0) (0,0,0,0,0,0,0)
(0,0,1,1,0,0,0) (0,1,1,1,0,1,0) (0,0,1,0,1,0,0) (1,1,0,1,0,0,0) (0,0,0,0,0,0,1) (1,0,1,1,0,0,0)
(0,1,1,1,0,1,0) (0,0,1,0,1,1,0) (1,0,0,0,1,0,1) (0,1,1,0,0,1,0) (0,1,1,1,0,1,0) (1,0,0,1,1,1,0)
(0,0,1,1,0,0,1) (1,1,1,0,1,1,1) (0,1,0,1,1,0,1) (1,0,0,0,0,0,1) (0,1,0,0,0,1,1) (1,1,0,1,0,1,1)
(1,0,0,1,0,1,1) (1,0,1,0,0,0,0) (1,0,0,0,1,0,1) (1,0,1,1,1,0,0) (1,0,0,0,0,1,0) (0,1,0,0,0,1,1)
(1,0,0,0,0,1,0) (1,1,0,1,0,0,0) (0,0,0,0,1,1,1) (1,0,0,0,0,0,1).

6. 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 $a \le 256$ такое, что числа $r_{257}(a^i)$ – различны при всех $1 \le i \le 256$ и $r_{257}(a^{256}) = 1$, где $r_{257}(t)$ – остаток от деления числа t на 257. Затем Милла загадывает натуральное число $x \le 256$, а Стелла – натуральное число $y \le 256$. 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 $r_{257}(a^x)$=9, $r_{257}(a^y)$=256.