

МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ  
ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

1. Для шифрования сообщения использовалось устройство из трёх последовательно зацепленных шестерёнок с 7, 30 и 9 зубцами (рис.1). На зубцах первой шестерёнки записаны цифры от 1 до 7, а на третьей – от 1 до 9. На второй шестерёнке также по часовой стрелке записан тридцатидвухбуквенный алфавит: **АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ**. 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

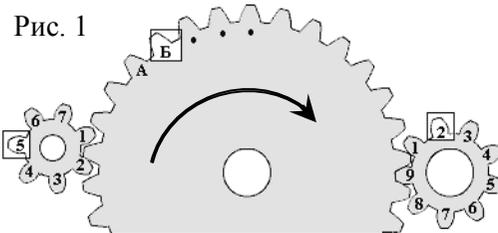


Рис. 1

11 64 12 46 66 75 56 65 29 42 71 12 23 67 76 28 52  
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  $r_{257}(a^{256})=1$ , например 3,5,6,7,10,12, 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  $r_{257}(a^{xy+1})$ . Найдите его, если известно, что  $a=5$ ,  $r_{257}(a^x)=16$ ,  $r_{257}(a^y)=248$ .

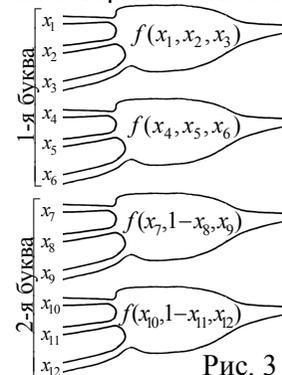
3. Каждое из чисел  $x_1, x_2, x_3, x_4, x_5, x_6$  принимает значение либо 0, либо 1. Известно, что числа  $x_1x_2 + x_2x_3 + x_1x_4$ ,  $x_1x_2x_4 + x_3x_6 + x_4$ ,  $x_2x_6 + x_4 + x_5$ ,  $x_1x_2x_4 + x_4x_6 + x_2x_3$ ,  $x_1x_4 + x_2x_6 + x_3$  чётны, а число  $x_1x_4 + x_4x_6 + x_4$  – нечётно. Найдите все варианты для  $x_1, x_2, x_3, x_4, x_5, x_6$ .

4. Для шифрования SMS-сообщений использовался следующий способ. Выбиралось секретное осмысленное трёхбуквенное слово. Каждый пробел в сообщении заменялся очередной буквой секретного слова: первый – на первую, второй – на вторую, третий – на третью, четвёртый – снова на первую и т.д. 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 (см. 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. Перед записью в память сервера пароли пользователей системы преобразуются. Сначала обрабатывается 1-я и 2-я буква пароля, затем 2-я и 3-я и т.д. Пара букв представляется набором, состоящим из двенадцати битов  $x_1, \dots, x_{12}$ , первые шесть из которых соответствуют первой букве, а вторые шесть – второй согласно табл.1.



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	Ъ	Ы	Ь	Э	Ю	Я	
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	0	0
0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Табл. 1

Биты получившегося набора подаются на четыре одинаковых логических элемента (рис.3). На вход каждого из них поступает три бита, а на выходе формируется значение  $f(x, y, z)$  равно 1, если среди битов  $x, y, z$  больше единиц, чем нулей, иначе формируется значение 0. В память сервера для каждой пары букв записывают четыре бита:  $(f(x_1, x_2, x_3), f(x_4, x_5, x_6), f(x_7, 1-x_8, x_9), f(x_{10}, 1-x_{11}, x_{12}))$ . Определите осмысленный пароль, если в памяти компьютера он хранится в следующем сжатом виде: (0,1,1,0), (0,0,1,0), (1,0,1,0), (0,0,1,0), (0,0,1,0), (0,0,1,1), (0,0,0,0), (0,1,1,0), (0,0,0,1).

6. В треугольнике ABC известно: BC=2, AC=3, угол ACB равен  $60^\circ$ . Точки M и K удовлетворяют условиям: AM : MC = 1:2, BK : CK = 2:3. Найдите максимально возможное расстояние между точками M и K.