11 класс XXIX МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
им. И.Я. ВЕРЧЕНКО ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ
**(сайт олимпиады www.cryptolymp.ru) 24.11.2019**

## 1 вариант

**1.** Известно, что $p, p_1, p_2, p_3$ – различные простые числа, и $p^3 - 2p^2 - 16p = p_1 \cdot p_2 \cdot p_3 - 32$. Найдите все такие числа $p, p_1, p_2, p_3$. Ответ обоснуйте.

**2.** Для зашифрования осмысленного слова его буквы переводят в числа $x_1, x_2, \ldots, x_n$ по таблице. Затем выбирают натуральные числа $x_0$ и $k$. Далее число $x_0$ приписывают в начало последовательности $x_1, x_2, \ldots, x_n$, а число $x_{n+1} = x_0 + 19^{n+4}$ (где $n$ – длина слова) – в ее конец. Получившаяся в результате последовательность $x_0, x_1, \ldots, x_n, x_{n+1}$ затем преобразуется в последовательность $y_0, y_1, \ldots, y_n, y_{n+1}$ по формуле $y_i = r_{32}(x_i + 6x_i \cdot k^3 + k)$, $i = 0,1, \ldots, n+1$, где $r_{32}(a)$ – остаток от деления числа $a$ на 32. Затем числа $y_0, y_1, \ldots, y_{n+1}$ заменяют буквами согласно таблице. В результате получили вот что: **КЙЫЦНБНЦЛ**. Какое слово было зашифровано?

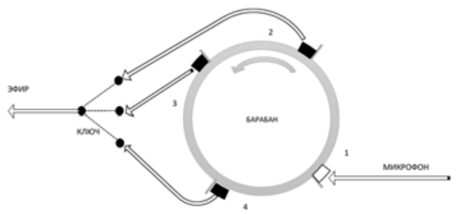
| А | Б | В | Г | Д | Е Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |

**3.** Каждому из четырех абонентов $A_1, A_2, A_3, A_4$ надо выдать по два уравнения вида $aw + bx + cy + dz = t$, где $a, b, c, d, t, w, x, y, z \in \{0,1\}$. Значения секретных битов $w, x, y, z$ одинаковы для всех абонентов и им заранее неизвестны. Приведите хотя бы один пример уравнений, которые надо выдать этим четырем абонентам, чтобы каждая пара $\{A_1, A_3\}, \{A_1, A_4\}, \{A_2, A_3\}$ могла достоверно вычислить $w, x, y, z$, но чтобы при этом: 1) ни одна другая пара абонентов не могла бы достоверно вычислить более одного секретного бита; 2) ни один абонент в одиночку не был в состоянии достоверно вычислить даже один секретный бит. Например, если абонент $A_1$ получит уравнения $\{w + x + y + z = 1;\ w + x + 0 \cdot y + 0 \cdot z = 1\}$, а $A_2$ – $\{w + 0 \cdot x + y + 0 \cdot z = 0;\ w + x + 0 \cdot y + z = 0\}$. Тогда, объединившись, из имеющихся в их распоряжении четырех уравнений они однозначно найдут, что $w = 1, x = 0, y = 1, z = 1$. При этом будем говорить, что пара абонентов $\{A_1, A_2\}$ может *достоверно вычислить* секретные биты $w, x, y, z$. Здесь традиционно полагается, что 1+1=0.

**4.** Саша решил отправить Маше записку. Для этого каждую букву сообщения он заменил комбинацией из 0 и 1 согласно таблице (А – 00000, Б – 00001, …, Я – 11111). Взяв день "Д" и номер месяца "М" своего рождения Саша вычислил $u_1 = \text{Д}^2 + \text{М}^2, u_2 = \text{Д} \cdot \text{М}, u_3 = \text{Д} - \text{М}$. Далее Саша вычислил четвертое $u_4 = r_{32}(u_1 + u_2 u_3)$, пятое $u_5 = r_{32}(u_2 + u_3 u_4)$, …, n-ое число
$u_n = r_{32}(u_{n-3} + u_{n-2} u_{n-1})$, где $r_{32}(a)$ – остаток от деления числа $a$ на 32. К $i$-му биту символу исходного сообщения (0 или 1) он прибавил число $u_i$ и взял остаток от деления на 2. Полученную последовательность из 0 и 1 он вновь преобразовал в буквы по таблице и получил следующее сообщение: **ЖДУЛЩБШЛТВШЩЦЧ**. Помогите Маше прочитать его.

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 0 | 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 |
| 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 |
| 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 | 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 | 1 |

**5.** Звук записывается на магнитный слой барабана (рис. 1), который вращается с постоянной скоростью, совершая один оборот за 4 секунды. Рядом с барабаном по окружности через равные расстояния размещены записывающая (1) и три читающие головки (2), (3), (4). В каждый момент времени в телефонную линию передается сигнал с одной из читающих головок. Устройство спроектировано так, что каждый участок сигнала будет передан в линию один раз, а сама передача стартует, как только начало записи окажется у 3-й читающей головки.




Сколько различных вариантов звука, переданного в линию, может получиться, если сообщение длилось 20 секунд?

**6.** Рассмотрим девять чисел $k_1, \ldots, k_9$, где $k_i \in \{0,1,2\}$. При этом хотя бы одно число $k_i$ отлично от нуля. С помощью этих чисел вырабатывают последовательность $u_1, u_2, \ldots, u_{2019}$ по формулам:
$u_1 = k_1, u_2 = k_2, \ldots, u_9 = k_9, \qquad u_{i+9} = r_3(u_i + u_{i+1}), \qquad i = 1,2, \ldots, 2010,$
где $r_3(a)$ – остаток от деления числа $a$ на 3. Найдите такое наименьшее натуральное число $l$, что какие бы исходные числа $k_1, \ldots, k_9$ мы ни взяли, в последовательности $u_1, u_2, \ldots, u_l$ каждое из чисел 0, 1 и 2 гарантированно встретится хотя бы один раз.