11 класс XXVIII МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ
**(сайт олимпиады www.cryptolymp.ru) 25.11.2018**

**1 вариант**

**1.** Для зашифрования слова из пяти букв каждая его буква заменяется на число согласно таблице. Полученный набор чисел $(x_0, x_1, x_2, x_3, x_4)$ затем преобразуется в набор $(y_0, y_1, y_2, y_3, y_4)$ по следующему правилу. Сначала вычисляют вспомогательные числа $\overline{y_0}, \overline{y_1}, \overline{y_2}, \overline{y_3}, \overline{y_4}$ по формулам

$$\overline{y_0} = 2^0 \cdot x_0 + 2^4 \cdot x_1 + 2^3 \cdot x_2 + 2^2 \cdot x_3 + 2^1 \cdot x_4,$$

$$\overline{y_k} = (2^k \cdot x_0 + 2^{k-1} \cdot x_1 + \cdots + 2^0 \cdot x_k) + (2^4 \cdot x_{k+1} + 2^3 \cdot x_{k+2} + \cdots + 2^{k+1} \cdot x_4),\ k = 1,2,3.$$

$$\overline{y_4} = 2^4 \cdot x_0 + 2^3 \cdot x_1 + 2^2 \cdot x_2 + 2^1 \cdot x_3 + 2^0 \cdot x_4.$$

А затем полагают $y_k$ равным остатку от деления числа $\overline{y_k}$ на 32. Расшифруйте исходное слово, если $(y_0, y_1, y_2, y_3, y_4) = (11,27,2,16,0)$.

| 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 |

**Решение**: Заметим, что для $k = 0,1,2,3$ справедливо равенство $2\overline{y_k} - \overline{y_{k+1}} = 31x_{k+1}$. Кроме того $2\overline{y_4} - \overline{y_0} = 31x_0$. Числа 31 и (-1) при делении на 32 дают один и тот же остаток 31, то есть $31 = r_{32}(31) = r_{32}(-1)$. (Здесь традиционно $r_{32}(x)$ – остаток от деления числа $x$ на 32.) Значит $r_{32}(31x_{k+1}) = r_{32}(-x_{k+1})$ и $r_{32}(31x_0) = r_{32}(-x_0)$. В результате получаем формулы, непосредственно выражающие искомые числа $x_0, x_1, x_2, x_3, x_4$ через данные в условии $y_0, y_1, y_2, y_3, y_4$:

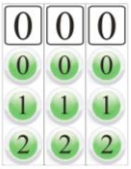
$$r_{32}(2\overline{y_k} - \overline{y_{k+1}}) = r_{32}(31x_{k+1}) = r_{32}(-x_{k+1}) \Rightarrow x_{k+1} = r_{32}(\overline{y_{k+1}} - 2\overline{y_k}) = r_{32}(y_{k+1} - 2y_k), k = 0,1,2,3.$$

$$\text{Аналогично, } x_0 = r_{32}(\overline{y_0} - 2\overline{y_4}) = r_{32}(y_0 - 2y_4).$$

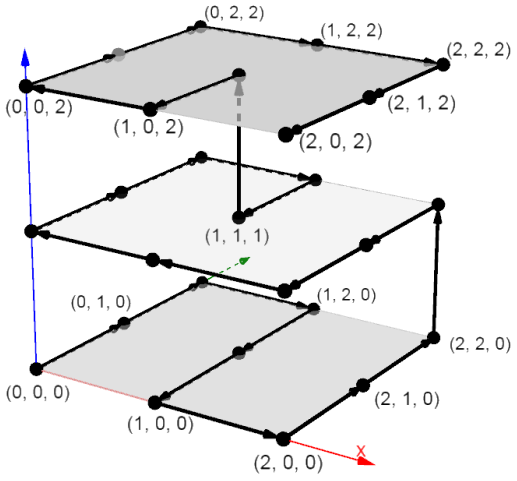
Отсюда находим $(x_0, x_1, x_2, x_3, x_4) = (11,5,12,12,0)$. Зашифрованное слово – ЛЕММА.

**Ответ**: ЛЕММА.

**2.** При входе в личный кабинет на терминале требуется ввести трехзначный пароль $x_1, x_2, x_3$, где $x_i \in \{0,1,2\}$. Для этого на терминале имеются 3 окошка, а под каждым окошком расположены три кнопки. При нажатии на кнопку в окошке над ней появляется соответствующая цифра. Сейчас в окошках выставлена комбинация 000. Какое наименьшее количество нажатий кнопок потребуется, чтобы перебрать все возможные варианты пароля?




**Решение**: Всего имеется $27 = 3^3$ трехзначных паролей (наборов) из 0, 1 и 2. Один такой пароль 000 уже набран, значит нам остается перебрать оставшиеся 26 вариантов, для чего потребуется по крайней мере 26 нажатий кнопок. Покажем, что 26 нажатий действительно хватит. Для этого все трехзначные наборы упорядочим так, чтобы соседние наборы отличались только в одном символе (классический код Грея). Тогда переход от одного набора к соседнему будет осуществляться нажатием одной кнопки, и всего потребуется как раз 26 нажатий.




Упорядочить так наборы можно многими способами. Одна из возможных идей состоит в следующем: каждый пароль будем интерпретировать как координаты точки в трехмерном пространстве (рис.). Координаты точек, лежащих на прямой, параллельной одной из координатных осей, как раз отличаются только в одном символе. Значит, если, двигаясь параллельно осям, мы обойдем все точки, то тем самым получим требуемое упорядочение. Один из возможных обходов представлен на рисунке.

**Ответ**: 26 нажатий. Один из способов перебора представлен на рисунке: (**0,0,0**), (**0,1,0**), …, (**2,0,2**).

**3.** В Крипто-Вегасе на табло игрового автомата отображаются два натуральных числа $x_0 = 5$ и $y_0 = 201$. При нажатии кнопки первое из этих чисел заменяется на $x_1 = r_{11}(a \cdot x_0 + b)$, где $a$ и $b$ – некоторые неизвестные натуральные числа, а второе число заменяется на $y_1 = r_{2017}(y_0 + 523)$. Здесь $r_k(m)$ – остаток от деления натурального числа $m$ на $k$. Нажав кнопку еще раз, получим (по таким же формулам) числа $x_2 = r_{11}(a \cdot x_1 + b)$ и $y_2 = r_{2017}(y_1 + 523)$ и так далее. Игрок получает приз, если при очередном нажатии на табло загорятся числа $x_n = 4$ и $y_n = 1993$.

Определите а) какие из следующих четырех последовательностей **(1):** (2, 5, 4, 7, 1), **(2):** (6, 9, 7, 1, 3), **(3):** (7, 10, 9, 2, 8), **(4):** (1, 0, 8, 8, 7) при надлежащем выборе $a$ и $b$ и вышеуказанных фиксированных $x_0, y_0$ могли бы совпасть с последовательностью $(x_1, \dots, x_5)$, полученной на этом игровом автомате? б) может ли игрок получить приз, если $(x_1, \dots, x_5)$ – одна из (реализуемых) последовательностей из пункта а)?

**Решение**: Последовательность $(x_n)$ задается рекуррентной формулой

$$x_n = r_{11}(a \cdot x_{n-1} + b), n \in \mathbb{N}. \qquad (1)$$

Следовательно, значение каждого члена последовательности $x_n$ (начиная со второго) однозначно вычисляется по значению ее предыдущего члена $x_{n-1}$. Покажем, что последовательность **(1)** получена быть не могла. В ней $x_0 = 5$ и $x_1 = 2$. Значит сразу после 5 всегда должна идти 2, но далее мы видим, что вслед за 5 идет 4. По этой же причине отбраковываем и последовательность **(4)**: после 8 встречается и 7, и 8.

Рассмотрим последовательность **(2)**. Для членов $x_1$ и $x_2$ этой последовательности, согласно (1), можем записать: $x_1 = 6 = r_{11}(a \cdot 5 + b), x_2 = 9 = r_{11}(a \cdot 6 + b)$. Вычтя из второго равенства первое, найдем $a = 3$. Тогда $b = 2$. Проверяем далее: $x_3 = 7 = r_{11}(3 \cdot 9 + 2)$ – верно, $x_4 = 1 = r_{11}(3 \cdot 7 + 2)$ – верно, $x_5 = 3 = r_{11}(3 \cdot 1 + 2)$ – неверно. Значит последовательность **(2)** также отбрасываем.

Рассмотрим последовательность **(3)**. Как и для последовательности **(2)** находим $a = 7, b = 5$, а затем убеждаемся, что последовательность **(3)** проверку проходит.

Итак, только последовательность **(3)** из пункта а) могла быть получена на игровом автомате. Выясним теперь получит ли в этом случае игрок приз. Выпишем больше членов соответствующей последовательности $(x_n)$: $\mathbf{5}, 7, 10, 9, 2, 8, 6, 3, 4, 0, \mathbf{5}, 7, \dots$ Видно, что это периодическая последовательность с периодом 10, и в ней встречается 4.

Докажем, что последовательность $(y_n)$ также является периодической, и ее период равен 2017. Заметим что эта последовательность, как и последовательность $(x_n)$, обладает тем свойством, что каждый ее последующий член однозначно находится по предыдущему. Поэтому для доказательства периодичности достаточно убедиться, что среди членов последовательности встречаются все целые числа от 0 до 2016. То есть, надо доказать, что для любого целого числа $m$ от 0 до 2016 существует такое $n \in \mathbb{N}$, что $y_n = m$. Последовательность $(y_n)$ (являющаяся ничем иным, как арифметической прогрессией на множестве остатков от деления на 2017) может быть задана формулой $n$-ого члена: $y_n = r_{2017}(201 + 523n),\ n \in \mathbb{N}$. Далее $y_n = m \Leftrightarrow m = r_{2017}(201 + 523n) \Leftrightarrow$ существует такое целое $t$, что $201 + 523n = m + 2017t \Leftrightarrow 523n - 2017t = m - 201$. Числа 523 и 2017 взаимно простые, поэтому данное линейное диофантово уравнение разрешимо в целых числах относительно $n$ и $t$ при любом значении $m$. Следовательно, любое значение $m$ от 0 до 2016, и в частности 1993, встретится в последовательности $(y_n)$. Остается заметить, что периоды последовательностей $(x_n)$ и $(y_n)$ взаимно простые, поэтому рано или поздно при каком-то $n \in \mathbb{N}$ окажутся справедливыми равенства $x_n = 4$ и $y_n = 1993$.

**Ответ:** а) **(3)**, б) да.

**4.** Для подтверждения переводимой в банк суммы братья **А** и **В** используют «кольцевую подпись», которая не позволяет определить, кто именно из них совершил перевод. **А** имеет свой открытый ключ $e_A = 5$ и некий секрет, позволяющий для любого натурального $y$ $(y \leq 90)$ находить $x_A$ такое,

что $y = r_{91}(x_A^{e_A})$. Здесь $r_k(m)$ – остаток от деления натурального числа $m$ на $k$. (У **B** есть свой ключ $e_B = 25$ и свой секрет.) Тогда **A** для подписи суммы $M$ случайно выбирает натуральные числа $x_B$ и $v$, не превосходящие 100, вычисляет $y_B = r_{91}(x_B^{e_B})$ и находит $y_A$ из уравнения:

$$r_{101}\big(M\big(y_A + M(y_B + v)\big) - v^3\big) = 0. \quad (*)$$

Используя свой секрет, **A** находит $x_A$ такой, что $y_A = r_{91}(x_A^{e_A})$. Тогда тройка чисел $(x_A, x_B, v)$ будет подтверждением факта перевода суммы $M$. В банке корректность подтверждения проверяют подстановкой $y_A = r_{91}(x_A^{e_A}), y_B = r_{91}(x_B^{e_B})$ и $v$ в уравнение $(*)$. Например, $(1, 90, 46)$ корректное подтверждение суммы 46. Постройте хотя бы одно корректное подтверждение суммы $M = 69$.

**Решение**: Надо найти такие числа $x_A, x_B$ и $v$, что если по ним вычислить $y_A = r_{91}(x_A^{e_A}), y_B = r_{91}(x_B^{e_B})$, а затем подставить эти $y_A, y_B, v$ и $M = 69$ в $(*)$, то получится верное равенство. Перепишем уравнение $(*)$ в виде:

$$r_{101}\big(M(y_A + My_B) + v \cdot (M^2 - v^2)\big) = 0.$$

Последнее равенство заведомо справедливо, если

$$\begin{cases} r_{101}(y_A + My_B) = 0 & (1) \\ r_{101}(M^2 - v^2) = 0. & (2) \end{cases}$$

Второму уравнению системы можно удовлетворить, положив $v = M$. Уравнение (1) эквивалентно уравнению

$$r_{101}\left(r_{91}\left(x_A^{e_A}\right)\right) = r_{101}\left(-M \cdot r_{91}\left(x_B^{e_B}\right)\right).$$

Возьмем, например, $x_B = 1$. Тогда $r_{101}\left(r_{91}\left(x_A^{e_A}\right)\right) = r_{101}(-M) \Leftrightarrow r_{91}\left(x_A^{e_A}\right) = 101 - M \Leftrightarrow r_{91}(x_A^5) = 32$. Значит, годится $x_A = 2$.

**Ответ**: Например, $(2, 1, 69)$.

**5.** В некоторые клетки доски $4 \times 4$ Аня положила по нескольку зерен и передала доску Боре (см. рис.). *Трансверсалью* доски называется набор из 4 клеток, любые две из которых расположены в разных строках и разных столбцах. Боря за один ход может снять одинаковое количество зерен с каждой клетки какой-либо одной трансверсали. За какое минимальное число ходов Боря может снять все зерна с доски?

| | | | |
|---|---|---|---|
| 4 | 5 | 6 | 0 |
| 5 | 0 | 4 | 6 |
| 5 | 5 | 3 | 2 |
| 1 | 5 | 2 | 7 |

**Решение**: Заметим, что в последней строке пустых клеток нет. За один ход Боря может освободить от зерен от силы одну клетку этой строки. Следовательно, ему придется сделать *минимум* 4 хода. Более того, в этой строке есть клетка с 7 зернами, а в остальных клетках доски зерен меньше. Значит с этой клетки зерна придется снимать минимум дважды. Поэтому за 4 хода Боря не справится. Покажем как снять зерна за 5 ходов (серым отмечены трансверсали, с которых сняли зерна):

| | | | |
|---|---|---|---|
| 4 | 5 | 1 | 0 |
| 5 | 0 | 4 | 1 |
| 0 | 5 | 3 | 2 |
| 1 | 0 | 2 | 7 |

| | | | |
|---|---|---|---|
| 4 | 3 | 1 | 0 |
| 3 | 0 | 4 | 1 |
| 0 | 5 | 3 | 0 |
| 1 | 0 | 0 | 7 |

| | | | |
|---|---|---|---|
| 0 | 3 | 1 | 0 |
| 3 | 0 | 0 | 1 |
| 0 | 1 | 3 | 0 |
| 1 | 0 | 0 | 3 |

| | | | |
|---|---|---|---|
| 0 | 3 | 0 | 0 |
| 3 | 0 | 0 | 0 |
| 0 | 0 | 3 | 0 |
| 0 | 0 | 0 | 3 |

| | | | |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 |

**Ответ**: За **5** ходов.

**6.** Известно, что оба числа $p$ и $p^{2018} + 800$ простые. Докажите, что число $p^4 + 8$ тоже простое.

**Решение**: Будем перебирать возможные значения простого числа $p$. Если $p = 2$, то число $p^{2018} + 800$ четное, что противоречит условию. Пусть $p = 3$. Тогда число $3^{2018} + 800$ может и оказаться простым. Убедимся, что для любого другого простого $p$ число $p^{2018} + 800$ делится на 3. Действительно, если $p \neq 3$, то остаток от деления числа $p$ на 3 равен либо 1, либо 2. Но остаток от деления числа $p^{2018}$ на 3 в любом случае будет равен 1 (поскольку $p^{2018} = (p^2)^{1009}$, а число $p^2$ всегда дает остаток 1 при делении на 3). Тогда $p^{2018} + 800$ делится на 3 (так как 800 дает остаток 2

при делении на 3) и не может быть простым. Таким образом, $p = 3$ – единственно возможный вариант. И тогда $p^4 + 8 = 3^4 + 8 = 89$ – простое число. Утверждение доказано.