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

6 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

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

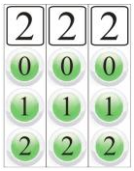
$$\overline{y_k} = (2^k \cdot x_0 + 2^{k-1} \cdot x_1 + \cdots + 2^0 \cdot x_k) + (2^4 \cdot x_{k+1} + 2^3 \cdot x_{k+2} + \cdots + 2^{k+1} \cdot x_4),\ k = 1,2,3.$$

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

А затем полагают y_k равным остатку от деления числа $\overline{y_k}$ на 32. Расшифруйте исходное слово, если $(y_0, y_1, y_2, y_3, y_4) = (0,14,9,5,27)$.

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

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 222. Какое наименьшее количество нажатий кнопок потребуется, чтобы перебрать все возможные варианты пароля?



3. В Крипто-Вегасе на табло игрового автомата отображаются два натуральных числа $x_0 = 7$ и $y_0 = 830$. 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 $y_1 = r_{2017}(y_0 + 451)$. 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 $y_2 = r_{2017}(y_1 + 451)$ и так далее. Игрок получает приз, если при очередном нажатии на табло загорятся числа $x_n = 5$ и $y_n = 1419$.

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

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 $e_A = 3$ и некий секрет, позволяющий для любого натурального y $(y \le 90)$ 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 **В** есть свой ключ $e_B = 25$ и свой секрет.) Тогда **А** 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, **А** 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. 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 $M = 37$.

5. В некоторые клетки доски 4×4 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	6	5	0
6	0	4	5
3	6	5	1
2	3	1	9

6. Известно, что оба числа p и $p^{2018+2} + 42204$ простые. Докажите, что число $p^4 - 6$ тоже простое.