11 класс XXVII МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ
**(сайт олимпиады www.cryptolymp.ru) 26.11.2017**

**4 вариант**

**1.** В тексте, состоящем из 18 букв и записанном без пробелов, буквы переставлены по следующему правилу: 18-я буква поставлена на 1-е место, 1-я буква – на 2-е место, 17-я – на 3-е место, 2-я – на 4-е и так далее (в конце 10-я буква поставлена на 17-е место, 9-я – на 18-е). Затем такую же процедуру повторили ещё 73 раза. В результате получилось **РЙОТЕЕЯЕВТТОЯСНРИО.** Найдите исходный текст.

**2.** Чтобы попасть в Криптоландию, необходимо пройти через ворота с электронным замком, предъявив правильный ключ. В микросхеме замка хранится таблица размерами 3x8 (3 строки и 8 столбцов), заполненная целыми числами от 1 до 8 так, что в каждой строке этой таблицы встречаются все числа от 1 до 8, а в каждом столбце нет повторяющихся чисел. Такие таблицы принято называть *латинскими прямоугольниками*. Путешественник должен предъявить в качестве ключа латинский прямоугольник размерами 4x8. Замок откроется в том и только том случае, если два эти прямоугольника (в памяти замка и предъявленный путешественником) можно единственным способом дополнить до латинских прямоугольников размеров 4x8 и 5x8, дописав к каждому из них *одну и ту же* строку. Если это условие не выполняется, то есть такое дополнение невозможно или неоднозначно, то ворота остаются закрытыми. Катя и Юра решили посетить Криптоландию. Определите, чей ключ правильный и почему.

**Код замка**

$$\begin{pmatrix} 3 & 8 & 2 & 4 & 5 & 6 & 1 & 7 \\ 5 & 7 & 8 & 3 & 2 & 4 & 6 & 1 \\ 8 & 4 & 5 & 1 & 6 & 7 & 2 & 3 \end{pmatrix}$$

**КлючКати**

$$\begin{pmatrix} 5 & 2 & 7 & 1 & 8 & 3 & 4 & 6 \\ 4 & 6 & 5 & 2 & 1 & 8 & 3 & 7 \\ 6 & 7 & 1 & 8 & 3 & 4 & 5 & 2 \\ 1 & 3 & 2 & 5 & 7 & 6 & 8 & 4 \end{pmatrix}$$

**Ключ Юры**

$$\begin{pmatrix} 4 & 1 & 6 & 8 & 5 & 7 & 3 & 2 \\ 8 & 6 & 3 & 2 & 1 & 4 & 5 & 7 \\ 7 & 5 & 8 & 1 & 3 & 2 & 6 & 4 \\ 1 & 3 & 7 & 6 & 4 & 8 & 2 & 5 \end{pmatrix}$$

**3.** Даны $k$ различных наборов натуральных чисел, причем каждый набор содержит $n$ натуральных чисел: $\boldsymbol{w_1} = (w_{11}, w_{12}, \dots, w_{1n}), \dots, \boldsymbol{w_k} = (w_{k1}, w_{k2}, \dots, w_{kn})$. (Наборы $\boldsymbol{w_i}$ и $\boldsymbol{w_j}$ называются различными, если существует натуральное число $m \in \overline{1,n}$ такое, что $w_{im} \neq w_{jm}$. Например, наборы (1,1,3,1) и (1,1,1,3) различны.) Докажите, что для каждой пары натуральных чисел $n$ и $k$ существует отображение $\sigma: \mathbb{N} \to \overline{1,k}$ (правило, ставящее в соответствие каждому натуральному числу натуральное число от 1 до $k$) такое, что наборы $\boldsymbol{w_1^\sigma} = \big(\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})\big), \dots, \boldsymbol{w_k^\sigma} = \big(\sigma(w_{k1}), \sigma(w_{k2}), \dots, \sigma(w_{kn})\big)$ также будут различны.

**4.** Имеется устройство, преобразующее 3-х битовые комбинации в двоичные символы. Известно, что сейчас устройство или работает правильно (режим ПР), или имеет неисправность одного из 3-х типов (Н1, Н2 и Н3). В таблице указано, какие символы в зависимости от входа устройство выдает при правильной работе, а также при возможных неисправностях. Какое *наименьшее* количество 3-битовых комбинаций (среди которых обязательно должна быть 010) следует подать на вход, чтобы, проанализировав выходные значения, суметь однозначно определить тип неисправности или же убедиться, что устройство работает правильно? Выпишите все (с точностью до перестановки) такие наборы 3-битовых входов.

| вход | ПР | Н1 | Н2 | Н3 |
|---|---|---|---|---|
| 000 | 0 | 0 | 0 | 1 |
| 001 | 1 | 1 | 0 | 1 |
| 010 | 0 | 1 | 0 | 1 |
| 011 | 0 | 1 | 0 | 0 |
| 100 | 1 | 1 | 1 | 0 |
| 101 | 1 | 0 | 0 | 0 |
| 110 | 1 | 0 | 1 | 1 |
| 111 | 1 | 1 | 1 | 1 |

**5.** При использовании криптосистемы RSA для расшифрования числового сообщения $y$, где $n = p \cdot q$, $p$ и $q$ – простые числа, находят секретное число $d$ из уравнения $r_{(p-1)(q-1)}(3d) = 1$ ($r_b(a)$ – остаток от деления числа $a$ на $b$). Известно, что младшие байты чисел $y, p, n, (p-1)\cdot(q-1)$ и $d$ равны `85,00,C1,F5,AB` (но неизвестно какому числу какой именно байт соответствует). Найдите $d$, если $n = 64501, y = 59781$. *Указание*: фигурирующие в задаче числа представимы в виде двух байтов, например $64501 = 15 \cdot 16^3 + 11 \cdot 16^2 + 15 \cdot 16^1 + 5 \cdot 16^0 =$ `FB F5` (см. таблицу); `F5` – младший байт числа 64501.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |

**6.** **(Встреча посередине.)** Шифратор принимает на вход и выдает на выход 8-битное число (1 байт). Поданный на вход байт $\boldsymbol{x^{in}} = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$ преобразуется в выходной байт $\boldsymbol{x^{out}}$ за 8 тактов. На 1-м такте входной байт $\boldsymbol{x^{in}}$ преобразуется в байт $\boldsymbol{x^{(1)}} = (x_1^{(1)}, x_2^{(1)}, x_3^{(1)}, x_4^{(1)}, x_5^{(1)}, x_6^{(1)}, x_7^{(1)}, x_8^{(1)})$ по формулам $x_1^{(1)} = x_2 \oplus k_1$, $x_2^{(1)} = x_3$, $x_3^{(1)} = x_4 \oplus k_1$, $x_4^{(1)} = x_5$, $x_5^{(1)} = x_6 \oplus k_1$, $x_6^{(1)} = x_7$, $x_7^{(1)} = x_8 \oplus k_1$, $x_8^{(1)} = x_2 x_7 \oplus x_1$. Здесь $k_1$ – секретный ключ 1-го такта ($k_1 \in \{0,1\}$); $\oplus$ – стандартная операция сложения битов ($0 \oplus 0 = 1 \oplus 1 = 0, 0 \oplus 1 = 1 \oplus 0 = 1$). Полученный на 1-м такте байт $\boldsymbol{x^{(1)}}$ на 2-м такте преобразуется в байт $\boldsymbol{x^{(2)}} = (x_1^{(2)}, \dots, x_8^{(2)})$ по аналогичным формулам: $x_1^{(2)} = x_2^{(1)} \oplus k_2, \dots$ На 8-м такте вычисляется выходной байт $\boldsymbol{x^{out}} = \boldsymbol{x^{(8)}}$. Найдите ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, на котором байт $\boldsymbol{x^{in}} = (1,0,1,0,1,0,1,0)$ преобразуется в байт $\boldsymbol{x^{out}} = (1,0,0,0,1,0,1,1)$, а байт $\boldsymbol{x^{in}} = (1,1,1,1,1,1,1,1)$ – в байт $\boldsymbol{x^{out}} = (0,0,1,1,0,0,0,0)$.