11 КЛАСС

1. В тексте, состоящем из 22 букв и записанном без пробелов, буквы переставлены по следующему правилу: 22-я буква поставлена на 1-е место, 1-я буква – на 2-е место, 21-я – на 3-е место, 2-я – на 4-е и так далее (в конце 12-я буква поставлена на 21-е место, 11-я – на 22-е). Затем такую же процедуру повторили ещё 49 раз. В результате получилось **КЬАТСТЯЕЕССОЧОТРИКОЕТЙ.** 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.

Код замка

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

Ключ Кати

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

Ключ Юры

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

3. 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. Выберите все (с точностью до перестановки) такие наборы 3-битовых комбинаций (среди которых обязательно должна быть 000), чтобы, проанализировав выходные значения, суметь однозначно определить тип неисправности или же убедиться, что устройство работает правильно. **Варианты ответов:** 000-100-110, 000-111-110, 000-100-111, 000-101-001.

вход	П	Н1	Н2	Н3
000	0	1	0	1
001	0	0	0	1
010	0	1	0	0
011	1	1	1	0
100	1	1	0	1
101	1	0	0	0
110	1	0	1	1
111	1	1	1	1

4. 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 6B,5F,4B,F0,29 (но неизвестно какому числу какой именно байт соответствует). Найдите d, если $n = 57439, y = 38507$. *Указание*: фигурирующие в задаче числа представимы в виде двух байт, например $57439 = 14 \cdot 16^3 + 0 \cdot 16^2 + 5 \cdot 16^1 + 15 \cdot 16^0$ =E0 5F (см. таблицу); 5F – младший байт числа 57439.

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

5. (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: $x_1^{(2)} = x_2^{(1)} \oplus k_2$, ... На 8-м такте вычисляется выходной байт $\boldsymbol{x}^{\boldsymbol{out}} = \boldsymbol{x}^{(8)}$. Найдите ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, на котором байт $\boldsymbol{x}^{\boldsymbol{in}} = (1,0,1,0,1,0,1,0)$ преобразуется в байт $\boldsymbol{x}^{\boldsymbol{out}} = (0,0,0,0,0,1,1,1)$, а байт $\boldsymbol{x}^{\boldsymbol{in}} = (1,1,1,1,1,1,1,1)$ – в байт $\boldsymbol{x}^{\boldsymbol{out}} = (1,0,0,1,1,1,0,1)$.

6. Известно, что целые числа a и b больше 10 и связаны соотношением $3a - 2b = 1$. Известно также, что $r_a(279) = 4$ и $r_b(279) = 7$, где $r_n(x)$ - остаток от деления числа x на n. Найдите $r_{ab}(279)$.