8-9 класс XXVII МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

(сайт олимпиады www.cryptolymp.ru) 26.11.2017

1 вариант

1. На бумажную ленту в строку записан 30-буквенный русский алфавит (Е=Ё, И=Й, Ь=Ъ). Из ленты вырезается фрагмент, содержащий 15 букв (например, от М до Ы). Остальные части ленты располагаются под ним "вверх ногами" так, чтобы на краях получившейся таблицы друг над другом оказались соседние буквы алфавита. Для зашифрования сообщения каждую его букву заменяют на вторую букву, стоящую в том же столбце таблицы. Например, зашифровав слово ДЕПО с помощью таблицы на рисунке, получим ТСЗИ. Расшифруйте сообщение **ЬВЫГВЭВВЕ ГЬЯХЧЯЯ ЯЕЗЫЩЕЯР**, полученное указанным способом (возможно, с использованием другой таблицы).

М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы
Л	К	И	З	Ж	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь

Решение: Всего ленту можно разрезать 16 способами, так что задача может быть решена перебором. С другой стороны, заметим, что удвоенная Я на конце второго слова может соответствовать только сочетаниям ИИ, ИЙ, ЯЯ или ЕЕ в открытом сообщении (по условию, при зашифровании разные буквы заменяются разными, а одинаковые – одинаковыми). Буква Я, очевидно, не могла быть заменена снова на Я, поэтому остается рассмотреть два случая: 1) буква Е заменялась буквой Я и 2) буква И заменялась буквой Я. Осмысленное сообщение получается во втором случае. (Более того, первый случай неосуществим: при зашифровании буквы с нечетными номерами заменяются на буквы с четными номерами и наоборот, поэтому Е (6-я буква) не могла быть заменена на Я (30-я буква).)

Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У
Г	В	Б	А	Я	Ю	Э	Ь	Ы	Щ	Ш	Ч	Ц	Х	Ф

Ответ: МЕНДЕЛЕЕВ ДМИТРИЙ ИВАНОВИЧ

2. Отпирающие комбинации кодового замка представляют собой набор из четырех цифр x_1, x_2, x_3, x_4, каждая из которых равна либо 0, либо 1. Про эти комбинации известно следующее: 1) ровно половина всех наборов открывают замок, 2) если в наборе $x_1 = 1$, то замок откроется в 75% случаев, 3) если $x_1 \cdot x_3 = 1$, то замок откроется в 50% случаев, 4) если $x_4 = 1$, то замок откроется в 25% случаев и 5) если $x_2 + x_3 = 1$, то в 62,5% случаев. Найдите все отпирающие комбинации.

Решение: Выпишем и пронумеруем все комбинации, и для каждой укажем, каким из свойств 2–5 она удовлетворяет.

Номер	Комбинация	Свойство	Номер	Комбинация	Свойство
0	0000		8	1000	2
1	0001	4	9	1001	2,4
2	0010	5	10	1010	2,3,5
3	0011	4,5	11	1011	2,3,4,5
4	0100	5	12	1100	2,5
5	0101	4,5	13	1101	2,4,5
6	0110		14	1110	2,3
7	0111	4	15	1111	2,3,4

Введем 16 неизвестных $y_0, \dots, y_{15}$, полагая $y_i = 1$, если комбинация с номером i отпирает замок, и $y_i = 0$, если i-тая комбинация замок не отпирает. Согласно условию, составим 5 уравнений:

$$\begin{cases} \mathbf{1)}\ y_0 + \dots + y_{15} = 8 \text{ (свойство 1: ровно половина комбинаций открывают замок)} \\ \mathbf{2)}\ y_8 + \dots + y_{15} = 6 \text{ (свойству 2 (см. таблицу) удовлетворяют 75\% комбинаций } 8-15) \\ \mathbf{3)}\ y_{10} + y_{11} + y_{14} + y_{15} = 2 \text{ (свойство 3: половина комбинаций 10,11,14,15 открывает замок)} \\ \mathbf{4)}\ y_1 + y_3 + y_5 + y_7 + y_9 + y_{11} + y_{13} + y_{15} = 2 \text{ (свойство 4)} \\ \mathbf{5)}\ y_2 + y_3 + y_4 + y_5 + y_{10} + y_{11} + y_{12} + y_{13} = 5 \text{ (свойство 5: 62,5\% от 8 равно 5)} \end{cases}$$

Вычтя из второго уравнения третье, получим $y_8+y_9+y_{12}+y_{13}=4$. Следовательно, $y_8=y_9=y_{12}=y_{13}=1$, то есть комбинации 8,9,12,13 отпирают замок. Подставив $y_{13}=y_9=1$ в уравнение (4), получим $y_1+y_3+y_5+y_7+y_{11}+y_{15}=0$. Значит, $y_1=y_3=y_5=y_7=y_{11}=y_{15}=0$. С учетом найденного, уравнения (1), (3) и (5) принимают вид:

$$\begin{cases} y_0+y_2+y_4+y_6=2 \\ y_{10}+y_{14}=2 \\ y_2+y_4+y_{10}=3. \end{cases}$$

Отсюда находим недостающие 4 отпирающие комбинации: 2, 4, 10, 14.

Ответ: Замок отпирают комбинации 2,4,8,9,10,12,13,14.

3. В тексте, состоящем из 24 букв и записанном без пробелов, буквы переставлены по следующему правилу: 24-я буква поставлена на 1-е место, 1-я буква – на 2-е место, 23-я – на 3-е место, 2-я – на 4-е и так далее (в конце 13-я буква поставлена на 23-е место, 12-я – на 24-е). Затем такую же процедуру повторили ещё 85 раз. В результате получилось **ТЯИМАИВУКЦНЛИКАЬЛНЯТПУФИ**. Найдите исходный текст.

Решение: По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	4	6	8	10	12	14	16	18	20	22	24	23	21	19	17	15	13	11	9	7	5	3	1

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте:

1→2→4→8→16→17→15→19→11→22→5→10→20→9→18→13→23→3→6→12→24→**1**→ …

То есть, после того как буквы переставили 21 раз, первая буква снова оказалась на первом месте. Попутно получили еще последовательность промежуточных положений первой буквы, а именно: 2,4,...,24. Очевидно, что буквы, стоявшие на этих местах, также займут исходное положение на 21-м шаге. Оставшиеся три буквы, стоящие на местах 7, 14, 21, перемещаются по циклу длины 3: **7**→14→21→**7**→…

Следовательно, после 21 преобразования текст будет совпадать с исходным.

Всего текст был преобразован 86 раз, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).

Ответ: МУЛЬТИПЛИКАТИВНАЯ ФУНКЦИЯ.

4. Для формирования защищенного соединения Алиса, Боб и Стелла используют хранящийся в секрете многочлен с целыми коэффициентами a, b, c вида

$$f(x,y)=ax^2+bx+cxy+by+ay^2,$$

и целые числа (ключи) k_A, k_B, k_C, которые имеют различные остатки при делении на 83. Чтобы отправить Бобу и Стелле сообщение, Алиса формирует новые ключи k_{AB} и k_{AC} по формулам:

$$k_{AB}=r_{83}(f(k_A,k_B)), \qquad k_{AC}=r_{83}(f(k_A,k_C)),$$

где $r_{83}(z)$ – остаток от деления числа zна 83. Аналогично Боб для отправки сообщений Стелле вычисляет $k_{BC}=r_{83}(f(k_B,k_C))$. Известно, что $k_A=28$, $k_{AB}=k_{AC}=73$, и при всех целых x выполняется равенство $r_{83}(f(x,k_A))=r_{83}(x^2+61x+11)$. Найдите ключ k_{BC}.

Решение: Из вида многочлена $f(x,y)$ нетрудно понять, что $f(x,y)=f(y,x)$, поэтому

$$r_{83}(f(x,k_A))=r_{83}(f(k_A,x)).$$

Следовательно,

$$k_{AC}=r_{83}(f(k_A,k_C))=r_{83}({k_C}^2+61k_C+11)=73,$$

А в силу равенства $k_{AB}=k_{AC}$, ключи k_B, k_C являются решениями уравнения:

$$r_{173}(x^2+61x+11)=73.$$

Запишем, по определению остатка:

$$x^2+61x+11=73+83t \ (t\in\mathbb{Z}) \Leftrightarrow x^2+61x-62=83t \Leftrightarrow$$

$$\Leftrightarrow (x-1)(x+62)=83t.$$

Из простоты числа 83 вытекает, что либо $x-1 \vdots 83$ либо $x+62 \vdots 83$. Таким образом:

$$x=1+83t_1, x=-62+83t_2.$$

Но согласно условию числа k_B, k_C имеют различные остатки от деления на 83, поэтому, без ограничения общности, можно считать, что $k_B = 1 + 83t_1, k_C = -62 + 83t_2 = 21 + 83t_2'$.
Для нахождения k_{BC} найдем коэффициенты многочлена $f(x, y)$. Имеем для любого целого x равенство:

$$r_{83}(x^2 + 61x + 11) = r_{83}(ax^2 + (b + 28c)x + 37a + 28b).$$

Отсюда $r_{83}(a) = 1, r_{83}(b + 28c) = 61, r_{83}(37a + 28b) = 11$.Значит,

$$37 + 28b = 11 + 83t \Leftrightarrow 22b = -26 + 83t \Leftrightarrow 84b = -78 + 83 \cdot 3t$$
$$\Leftrightarrow b = -78 + 83t' \Leftrightarrow b = 5 + 83t''$$

В итоге, $b = 5 + 83t''$, т.е. $r_{83}(b) = 5$. Аналогично, находим$c = 2 + 83k$,т.е. $r_{83}(c) = 2$. Теперь, осталось подставить полученные значения в равенство

$$k_{BC} = r_{83}\big(f(k_B, k_C)\big) = 13.$$

Ответ: k_{BC} =13.

5. *Латинским квадратом порядка n* называется квадратная таблица из *n* строк и *n* столбцов, заполненная натуральными числами от 1 до *n* таким образом, что каждый столбец и каждая строка не содержат одинаковые числа. Пусть L – латинский квадрат порядка *n*. Число, стоящее в этом квадрате в строке с номером i и столбце с номером j, обозначим $L(i, j)$.
Два латинских квадрата L_1 и L_2 назовем *ортогональными*, если при их "наложении" не образуется одинаковых пар элементов в разных ячейках таблицы. А именно, если $(i, j) \neq (s, t)$, то $\big(L_1(i, j), L_2(i, j)\big) \neq \big(L_1(s, t), L_2(s, t)\big)$.
а) Постройте пару ортогональных латинских квадратов порядка 4.
б) Докажите, что множество, состоящее из попарно не ортогональных латинских квадратов порядка *n*, не может содержать более чем $n - 1$ квадрат.

Решение: а) Например,

$$L_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \text{и} \quad L_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

Замечание. *Ортогональные квадраты существуют для всех* n, *отличных от 2 и 6. Для* $n = p^t$, *где* p *– простое* ($t > 1$, *если* $p = 2$), *способ построение попарно ортогональных квадратов в 1938 г. опубликовал Р. Боуз (R.S. Bose) (потом выяснилось, что этот способ был открыт Муром в 1896 г.). Оказывается, ортогональными будут квадраты L1 и L2, где* $L_i(x, y) = a_i \cdot x + y, i = 1,2$. *Сложение и умножение выполняются в поле* $GF(p^t)$, $a_i \neq 0$, $a_1 \neq a_2$.

б) Рассмотрим для примера следующий латинский квадрат $\begin{matrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{matrix}$. *Переобозначим* в нем элементы: 1 заменим на 2, 2 – на 3, 3 – на 1. В результате, естественно, вновь получим латинский квадрат: $\begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix}$. Несложно видеть, что если в двух ортогональных квадратах переобозначить элементы (не обязательно одинаковым образом!), то полученные квадраты тоже будут ортогональными.
Пусть теперь есть множество из k попарно ортогональных квадратов. Переобозначим в каждом квадрате элементы так, чтобы, как в разобранном примере, у каждого квадрата первая строка была:$1,2, \dots, n$. Теперь посмотрим, какое число стоит у всех этих квадратов на первом месте во второй строке. Во-первых, так как квадраты латинские, это число отлично от 1. Во-вторых, у разных квадратов эти числа должны быть различными, так как они ортогональны. Всего имеется только $n - 1$ различных чисел, не равных 1. Значит, $k \leq n - 1$. Утверждение доказано.

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 $\boldsymbol{x^{(1)}} = \left(x_1^{(1)}, x_2^{(1)}, x_3^{(1)}, x_4^{(1)}, x_5^{(1)}, x_6^{(1)}, x_7^{(1)}, x_8^{(1)}\right)$ по формулам $x_1^{(1)} = x_2 \oplus k_1, x_2^{(1)} = x_3$, $x_3^{(1)} = x_4 \oplus k_1, x_4^{(1)} = x_5, x_5^{(1)} = x_6 \oplus k_1, x_6^{(1)} = x_7, x_7^{(1)} = x_8 \oplus k_1, x_8^{(1)} = x_2x_7 \oplus x_1$. 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 $\boldsymbol{x}^{in} = (0,0,0,0,0,0,0,0)$ преобразуется в байт $\boldsymbol{x}^{out} = (1,1,1,0,0,1,0,1)$.

Решение: Обозначим $\boldsymbol{x}^{in} = \boldsymbol{x}^{(0)}$. На i-том такте выполняется преобразование $\boldsymbol{x}^{(i)} = \boldsymbol{f}_i(\boldsymbol{x}^{(i-1)})$, которое в покомпонентной записи выглядит, согласно условию, следующим образом:

$$x_1^{(i)} = x_2^{(i-1)} \oplus k_i, x_2^{(i)} = x_3^{(i-1)}, x_3^{(i)} = x_4^{(i-1)} \oplus k_i, x_4^{(i)} = x_5^{(i-1)}, x_5^{(i)} = x_6^{(i-1)} \oplus k_i, x_6^{(i)} = x_7^{(i-1)}, \; x_7^{(i)} = x_8^{(i-1)} \oplus k_i, x_8^{(i)} = x_2^{(i-1)} x_7^{(i-1)} \oplus x_1^{(i-1)}.$$

Требуется найти такой ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, что

$$\boldsymbol{x}^{(8)} = \boldsymbol{f}_8\left(\boldsymbol{f}_7\left(\dots \boldsymbol{f}_1(\boldsymbol{x}^{(0)})\right)\right). \qquad (1)$$

Несложно проверить, что отображение $\boldsymbol{x}^{(i-1)} = \boldsymbol{g}_i(\boldsymbol{x}^{(i)})$, покомпонентная запись которого имеет вид

$$x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = x_6^{(i)}, \; x_8^{(i-1)} = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}\left(x_1^{(i)} \oplus k_i\right),$$

является обратным к $\boldsymbol{x}^{(i)} = \boldsymbol{f}_{i-1}(\boldsymbol{x}^{(i-1)})$. (Эти формулы обращения следуют из элементарных соображений типа $a = b \oplus c \Leftrightarrow b = a \oplus c$, поэтому выражение для $x_1^{(i-1)}$ естественно получить в последнюю очередь, когда остальные $x_j^{(i-1)}$ уже найдены.) Уравнение (1) эквивалентно уравнению $\boldsymbol{f}_4\left(\boldsymbol{f}_3\left(\boldsymbol{f}_2\left(\boldsymbol{f}_1(\boldsymbol{x}^{(0)})\right)\right)\right) = \boldsymbol{g}_5\left(\boldsymbol{g}_6\left(\boldsymbol{g}_7\left(\boldsymbol{g}_8(\boldsymbol{x}^{(8)})\right)\right)\right)$. Последнее решается полным перебором "половинок" ключа: мы вычисляем правую часть при всевозможных значениях (k_5, k_6, k_7, k_8) (16 вариантов), а затем левую часть для всех (k_1, k_2, k_3, k_4) (также 16 вариантов). Те "половинки", при которых левая и правая части окажутся равными, дадут искомый ключ. Результаты вычислений представлены в таблице.

k_1, k_2, k_3, k_4	$\boldsymbol{f}_4\left(\boldsymbol{f}_3\left(\boldsymbol{f}_2\left(\boldsymbol{f}_1(\boldsymbol{x}^{(0)})\right)\right)\right)$	k_5, k_6, k_7, k_8	$\boldsymbol{g}_5\left(\boldsymbol{g}_6\left(\boldsymbol{g}_7\left(\boldsymbol{g}_8(\boldsymbol{x}^{(8)})\right)\right)\right)$
0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0	1 1 0 0 1 1 1 0
0 0 0 1	1 0 1 0 1 0 1 0	0 0 0 1	1 1 0 1 0 1 0 0
0 0 1 0	0 1 0 1 0 1 0 1	0 0 1 0	0 0 0 1 1 0 1 1
0 0 1 1	1 1 1 1 1 1 1 1	0 0 1 1	1 1 1 0 0 0 0 1
0 1 0 0	1 0 1 0 1 0 1 0	0 1 0 0	1 1 1 0 0 1 0 0
0 1 0 1	0 0 0 0 0 0 0 0	0 1 0 1	1 1 1 1 1 1 1 0
0 1 1 0	1 1 1 1 1 1 1 0	0 1 1 0	1 1 1 1 0 0 0 1
0 1 1 1	0 1 0 1 0 1 0 0	0 1 1 1	0 0 0 0 1 0 1 1
1 0 0 0	0 1 0 1 0 1 0 1	1 0 0 0	0 0 0 1 1 0 1 1
1 0 0 1	1 1 1 1 1 1 1 1	1 0 0 1	1 0 0 0 0 0 0 1
1 0 1 0	0 0 0 0 0 0 0 0	1 0 1 0	1 1 0 0 1 1 1 0
1 0 1 1	1 0 1 0 1 0 1 0	1 0 1 1	1 0 1 1 0 1 0 0
1 1 0 0	1 1 1 1 1 1 0 0	1 1 0 0	1 0 1 1 0 0 0 1
1 1 0 1	0 1 0 1 0 1 1 0	1 1 0 1	0 0 1 0 1 0 1 1
1 1 1 0	1 0 1 0 1 0 0 0	1 1 1 0	1 0 1 0 0 1 0 0
1 1 1 1	0 0 0 0 0 0 1 0	1 1 1 1	1 1 0 1 1 1 1 0

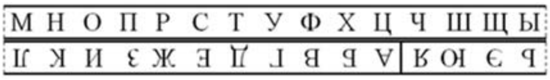
Ответ: 0, 1, 1, 0, 0, 1, 0, 1.

8-9 класс XXVII МЕЖРЕГИОНАЛЬНАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО МАТЕМАТИКЕ И КРИПТОГРАФИИ

(сайт олимпиады www.cryptolymp.ru) 26.11.2017

2 вариант

1. На бумажную ленту в строку записан 30-буквенный русский алфавит (Е=Ё, И=Й, Ь=Ъ). Из ленты вырезается фрагмент, содержащий 15 букв (например, от М до Ы). Остальные части ленты располагаются под ним "вверх ногами" так, чтобы на краях получившейся таблицы друг над другом оказались соседние буквы алфавита. Для зашифрования сообщения каждую его букву заменяют на вторую букву, стоящую в том же столбце таблицы. Например, зашифровав слово ДЕПО с помощью таблицы на рисунке, получим ТСЗИ. Расшифруйте сообщение **ОЛНЛМЛЗЛЦ НРГШРО ЦШЗРОЭУЦРБ**, полученное указанным способом (возможно, с использованием другой таблицы).



Решение: Всего ленту можно разрезать 16 способами, так что задача может быть решена перебором. С другой стороны, заметим, что буква Л встречается в первом слове три раза, значит, можно предположить, что Л соответствует одной и той же гласной букве в открытом сообщении (по условию, при зашифровании разные буквы заменяются разными, а одинаковые – одинаковыми). Гласная буква, встречающаяся три раза в одном слове, – это, скорее всего, А, Е, И или О. Осмысленное сообщение получается, когда Л заменяется на О. (Есть еще и простое дополнительное соображение: при зашифровании буквы с нечетными номерами заменяются на буквы с четными номерами и наоборот, поэтому, например, А (1-я буква) не могла быть заменена на Л (11-я буква).)

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь
М	Л	К	И	З	Ж	Е	Д	Г	В	Б	А	Я	Ю	Э

Ответ: ЛОМОНОСОВ МИХАИЛ ВАСИЛЬЕВИЧ

2. Отпирающие комбинации кодового замка представляют собой набор из четырех цифр x_1, x_2, x_3, x_4, каждая из которых равна либо 0, либо 1. Про эти комбинации известно следующее: 1) ровно половина всех наборов открывают замок, 2) если в наборе $x_2 = 1$, то замок откроется в 75% случаев, 3) если $x_2 \cdot x_4 = 1$, то замок откроется в 50% случаев, 4) если $x_1 = 1$, то замок откроется в 25% случаев и 5) если $x_3 + x_4 = 1$, то в 62,5% случаев. Найдите все отпирающие комбинации.

Решение: Выпишем и пронумеруем все комбинации, и для каждой укажем, каким из свойств 2–5 она удовлетворяет.

Номер	Комбинация	Свойство
0	0000	
1	0001	5
2	0010	5
3	0011	
4	0100	2
5	0101	2,3,5
6	0110	2,5
7	0111	2,3

Номер	Комбинация	Свойство
8	1000	4
9	1001	4,5
10	1010	4,5
11	1011	4
12	1100	2,4
13	1101	2,3,4,5
14	1110	2,4,5
15	1111	2,3,4

Введем 16 неизвестных $y_0, \dots, y_{15}$, полагая $y_i = 1$, если комбинация с номером i отпирает замок, и $y_i = 0$, если i-тая комбинация замок не отпирает. Согласно условию, составим 5 уравнений:

$$\begin{cases} \mathbf{1})\ y_0+\dots+y_{15}=8 \text{ (свойство 1: ровно половина комбинаций открывают замок)} \\ \mathbf{2})\ y_4+y_5+y_6+y_7+y_{12}+y_{13}+y_{14}+y_{15}=6 \text{ (свойство 2)} \\ \mathbf{3})\ y_5+y_7+y_{13}+y_{15}=2 \text{ (свойство 3: половина комбинаций 5,7,13,15 отпирает замок)} \\ \mathbf{4})\ y_8+\dots+y_{15}=2 \text{ (свойству 4 удовлетворяют 25\% комбинаций } 8-15) \\ \mathbf{5})\ y_1+y_2+y_5+y_6+y_9+y_{10}+y_{13}+y_{14}=5 \text{ (свойство 5: 62,5\% от 8 равно 5)} \end{cases}$$

Вычтя из второго уравнения третье, получим $y_4+y_6+y_{12}+y_{14}=4$. Следовательно, $y_4=y_6=y_{12}=y_{14}=1$, то есть комбинации 4, 6, 12, 14 отпирают замок. Подставив $y_{12}=y_{14}=1$ в уравнение (4), получим $y_8+y_9+y_{10}+y_{11}+y_{13}+y_{15}=0$. Значит, $y_8=y_9=y_{10}=y_{11}=y_{13}=y_{15}=0$. С учетом найденного, уравнения (1), (3) и (5) принимают вид:

$$\begin{cases} y_0+y_1+y_2+y_3+y_5+y_7=4 \\ y_5+y_7=2 \\ y_1+y_2+y_5=3. \end{cases}$$

Отсюда находим недостающие 4 отпирающие комбинации: 1, 2, 5, 7.

Ответ: Замок отпирают комбинации 1, 2, 4, 5, 6, 7, 12, 14.

3. 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.

Решение: По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2	4	6	8	10	12	14	16	18	20	22	21	19	17	15	13	11	9	7	5	3	1

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте:

1→2→4→8→16→13→19→7→14→17→11→22→**1**→…

То есть, после того как буквы переставили 12 раз, первая буква снова оказалась на первом месте. Попутно получили еще последовательность промежуточных положений первой буквы, а именно: 2,4,...,22. Очевидно, что буквы, стоявшие на этих местах, также займут исходное положение на 21-м шаге. Оставшиеся буквы, перемещаются по циклам длины 4, 3 и 2: **3**→6→12→21→**3**→…, **5**→10→20→**5**→…, **9**→18→**9**→…

Следовательно, после 12 преобразований текст будет совпадать с исходным.

Всего текст был преобразован 50 раз, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).

Ответ: ТЕОРЕТИЧЕСКАЯ СТОЙКОСТЬ.

4. Для формирования защищенного соединения Алиса, Боб и Стелла используют хранящийся в секрете многочлен с целыми коэффициентами a, b, c вида

$$f(x,y)=ax^2+bx+cxy+by+ay^2,$$

и целые числа (ключи) k_A, k_B, k_C, которые имеют различные остатки при делении на 83. Чтобы отправить Бобу и Стелле сообщение, Алиса формирует новые ключи k_{AB} и k_{AC} по формулам:

$$k_{AB}=r_{83}(f(k_A,k_B)), \qquad k_{AC}=r_{83}(f(k_A,k_C)),$$

где $r_{83}(z)$ – остаток от деления числа z на 83. Аналогично Боб для отправки сообщений Стелле вычисляет $k_{BC}=r_{83}(f(k_B,k_C))$. Известно, что $k_A=42$, $k_{AB}=k_{AC}=24$, и при всех целых x выполняется равенство $r_{83}(f(x,k_A))=r_{83}(x^2+28x+76)$. Найдите ключ k_{BC}.

Решение: Из вида многочлена $f(x,y)$ нетрудно понять, что $f(x,y)=f(y,x)$, поэтому

$$r_{83}(f(x,k_A))=r_{83}(f(k_A,x)).$$

Следовательно,

$$k_{AC}=r_{83}(f(k_A,k_C))=r_{83}({k_C}^2+28k_C+76)=24,$$

А в силу равенства $k_{AB}=k_{AC}$, ключи k_B, k_C являются решениями уравнения:

$$r_{83}(x^2+28x+76)=24.$$

Запишем, по определению остатка:

$$x^2 + 28x + 76 = 24 + 83t\ (t \in \mathbb{Z}) \Leftrightarrow\ x^2 + 28x + 52 = 83t \Leftrightarrow$$
$$\Leftrightarrow (x + 2)(x + 26) = 83t.$$

Из простоты числа 83 вытекает, что либо $x + 2 \vdots 83$ либо $x + 26 \vdots 83$. Таким образом:

$$x = -2 + 83t_1, x = -26 + 83t_2.$$

Но согласно условию числа k_B, k_C имеют различные остатки от деления на 83, поэтому без ограничения общности можно считать, что $k_B = -2 + 83t_1, k_C = -26 + 83t_2$.

Для нахождения k_{BC} найдем коэффициенты многочлена $f(x,y)$. Имеем для любого целого x равенство:

$$r_{83}(x^2 + 28x + 76) = r_{83}(ax^2 + (b + 42c)x + 21a + 42b).$$

Отсюда $r_{83}(a) = 1, r_{83}(b + 42c) = 28, r_{83}(21a + 42b) = 76.$Значит,

$$21 + 42b = 76 + 83t \Leftrightarrow 42b = 55 + 83t \Leftrightarrow 84b = 110 + 83 \cdot 2t$$
$$\Leftrightarrow b = 110 + 83t' \Leftrightarrow b = 27 + 83t''$$

В итоге, $b = 27 + 83t''$, т.е. $r_{83}(b) = 27$. Аналогично, находим$c = 2 + 83k$,т.е. $r_{83}(c) = 2$. Теперь, осталось подставить полученные значения в равенство

$$k_{BC} = r_{83}\big(f(k_B, k_C)\big) = 28.$$

Ответ: k_{BC} =28.

5. *Латинским квадратом порядка n* называется квадратная таблица из *n* строк и *n* столбцов, заполненная натуральными числами от 1 до *n* таким образом, что каждый столбец и каждая строка не содержат одинаковые числа. Пусть L – латинский квадрат порядка *n*. Число, стоящее в этом квадрате в строке с номером i и столбце с номером j, обозначим $L(i,j)$.

Два латинских квадрата L_1 и L_2 назовем *ортогональными*, если при их "наложении" не образуется одинаковых пар элементов в разных ячейках таблицы. А именно, если $(i,j) \neq (s,t)$, то $\big(L_1(i,j), L_2(i,j)\big) \neq\ \big(L_1(s,t), L_2(s,t)\big)$.

а) Постройте пару ортогональных латинских квадратов порядка 4.

б) Докажите, что множество, состоящее из попарно не ортогональных латинских квадратов порядка *n*, не может содержать более чем $n - 1$ квадрат.

Решение: а) Например,

$$L_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \text{и} \quad L_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

Замечание. *Ортогональные квадраты существуют для всех* n, *отличных от 2 и 6. Для* $n = p^t$, *где* p *– простое* ($t > 1$, *если* $p = 2$), *способ построение попарно ортогональных квадратов в 1938 г. опубликовал Р. Боуз (R.S. Bose) (потом выяснилось, что этот способ был открыт Муром в 1896 г.). Оказывается, ортогональными будут квадраты L*$_1$ *и L*$_2$*, где* $L_i(x,y) = a_i \cdot\ x + y, i = 1{,}2$. *Сложение и умножение выполняются в поле* $GF(p^t)$, $a_i \neq\ 0,\ a_1 \neq a_2$.

б) Рассмотрим для примера следующий латинский квадрат $\begin{matrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{matrix}$. *Переобозначим* в нем элементы: 1 заменим на 2, 2 – на 3, 3 – на 1. В результате, естественно, вновь получим латинский квадрат: $\begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix}$. Несложно видеть, что если в двух ортогональных квадратах переобозначить элементы (не обязательно одинаковым образом!), то полученные квадраты тоже будут ортогональными.

Пусть теперь есть множество из k попарно ортогональных квадратов. Переобозначим в каждом квадрате элементы так, чтобы, как в разобранном примере, у каждого квадрата первая строка была:$1,2, \dots, n$. Теперь посмотрим, какое число стоит у всех этих квадратов на первом месте во второй строке. Во-первых, так как квадраты латинские, это число отлично от 1. Во-вторых, у разных квадратов эти числа должны быть различными, так как они ортогональны. Всего имеется только $n - 1$ различных чисел, не равных 1. Значит, $k \leq n - 1$. Утверждение доказано.

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

$\boldsymbol{x}^{(\mathbf{1})} = \left(x_1^{(1)}, x_2^{(1)}, x_3^{(1)}, x_4^{(1)}, x_5^{(1)}, x_6^{(1)}, x_7^{(1)}, x_8^{(1)}\right)$ по формулам $x_1^{(1)} = x_2 \oplus k_1, x_2^{(1)} = x_3$, $x_3^{(1)} = x_4 \oplus k_1, x_4^{(1)} = x_5, x_5^{(1)} = x_6 \oplus k_1, x_6^{(1)} = x_7, x_7^{(1)} = x_8 \oplus k_1, x_8^{(1)} = x_2x_7 \oplus x_1$. 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 $\boldsymbol{x}^{(\mathbf{1})}$ на 2-м такте преобразуется в байт $\boldsymbol{x}^{(\mathbf{2})} = (x_1^{(2)}, \dots, x_8^{(2)})$ по аналогичным формулам: $x_1^{(2)} = x_2^{(1)} \oplus k_2, \dots$ На 8-м такте вычисляется выходной байт $\boldsymbol{x}^{\boldsymbol{out}} = \boldsymbol{x}^{(\mathbf{8})}$**.** Найдите ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, на котором байт $\boldsymbol{x}^{\boldsymbol{in}} = (0,0,0,0,0,0,0,0)$ преобразуется в байт $\boldsymbol{x}^{\boldsymbol{out}} = (0,0,1,1,0,1,0,1)$.

Решение: Обозначим $\boldsymbol{x}^{\boldsymbol{in}} = \boldsymbol{x}^{(\mathbf{0})}$. На i-том такте выполняется преобразование $\boldsymbol{x}^{(\boldsymbol{i})} = \boldsymbol{f_i}(\boldsymbol{x}^{(\boldsymbol{i-1})})$, которое в покомпонентной записи выглядит, согласно условию, следующим образом:

$$x_1^{(i)} = x_2^{(i-1)} \oplus k_i, x_2^{(i)} = x_3^{(i-1)}, x_3^{(i)} = x_4^{(i-1)} \oplus k_i, x_4^{(i)} = x_5^{(i-1)}, x_5^{(i)} = x_6^{(i-1)} \oplus k_i, x_6^{(i)} = \\ = x_7^{(i-1)},\ x_7^{(i)} = x_8^{(i-1)} \oplus k_i, x_8^{(i)} = x_2^{(i-1)}x_7^{(i-1)} \oplus x_1^{(i-1)}.$$

Требуется найти такой ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, что

$$\boldsymbol{x}^{(\mathbf{8})} = \boldsymbol{f_8}\left(\boldsymbol{f_7}\left(\dots \boldsymbol{f_1}(\boldsymbol{x}^{(\mathbf{0})})\right)\right). \tag{1}$$

Несложно проверить, что отображение $\boldsymbol{x}^{(\boldsymbol{i-1})} = \boldsymbol{g_i}(\boldsymbol{x}^{(\boldsymbol{i})})$, покомпонентная запись которого имеет вид

$$x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = \\ = x_6^{(i)},\ x_8^{(i-1)} = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}\left(x_1^{(i)} \oplus k_i\right),$$

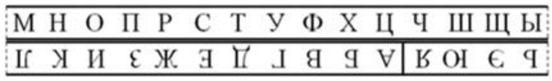
является обратным к $\boldsymbol{x}^{(\boldsymbol{i})} = \boldsymbol{f_{i-1}}\big(\boldsymbol{x}^{(\boldsymbol{i-1})}\big)$. (Эти формулы обращения следуют из элементарных соображений типа $a = b \oplus c \Leftrightarrow b = a \oplus c$, поэтому выражение для $x_1^{(i-1)}$ естественно получить в последнюю очередь, когда остальные $x_j^{(i-1)}$ уже найдены.) Уравнение (1) эквивалентно уравнению $\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}(\boldsymbol{x}^{(\mathbf{0})})\right)\right)\right) = \boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}(\boldsymbol{x}^{(\mathbf{8})})\right)\right)\right)$. Последнее решается полным перебором "половинок" ключа: мы вычисляем правую часть при всевозможных значениях (k_5, k_6, k_7, k_8) (16 вариантов), а затем левую часть для всех (k_1, k_2, k_3, k_4) (также 16 вариантов). Те "половинки", при которых левая и правая части окажутся равными, дадут искомый ключ. Результаты вычислений представлены в таблице.

k_1, k_2, k_3, k_4	$\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}(\boldsymbol{x}^{(\mathbf{0})})\right)\right)\right)$	k_5, k_6, k_7, k_8	$\boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}(\boldsymbol{x}^{(\mathbf{8})})\right)\right)\right)$
0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0	1 1 0 1 0 0 1 1
0 0 0 1	1 0 1 0 1 0 1 0	0 0 0 1	1 0 1 0 1 0 0 1
0 0 1 0	0 1 0 1 0 1 0 1	0 0 1 0	0 0 0 0 0 1 1 0
0 0 1 1	1 1 1 1 1 1 1 1	0 0 1 1	1 0 0 1 1 1 0 0
0 1 0 0	1 0 1 0 1 0 1 0	0 1 0 0	1 0 1 1 1 0 0 1
0 1 0 1	0 0 0 0 0 0 0 0	0 1 0 1	1 1 0 0 0 0 1 1
0 1 1 0	1 1 1 1 1 1 1 0	0 1 1 0	1 0 1 0 1 1 0 0
0 1 1 1	0 1 0 1 0 1 0 0	0 1 1 1	0 0 1 1 0 1 1 0
1 0 0 0	0 1 0 1 0 1 0 1	1 0 0 0	0 0 0 0 0 1 1 0
1 0 0 1	1 1 1 1 1 1 1 1	$\boxed{1\ 0\ 0\ 1}$	$\boxed{1\ 1\ 1\ 1\ 1\ 1\ 0\ 0}$
1 0 1 0	0 0 0 0 0 0 0 0	1 0 1 0	1 1 0 1 0 0 1 1
1 0 1 1	1 0 1 0 1 0 1 0	1 0 1 1	1 1 0 0 1 0 0 1
$\boxed{1\ 1\ 0\ 0}$	$\boxed{1\ 1\ 1\ 1\ 1\ 1\ 0\ 0}$	1 1 0 0	1 1 1 0 1 1 0 0
1 1 0 1	0 1 0 1 0 1 1 0	1 1 0 1	0 0 0 1 0 1 1 0
1 1 1 0	1 0 1 0 1 0 0 0	1 1 1 0	1 1 1 1 1 0 0 1
1 1 1 1	0 0 0 0 0 0 1 0	1 1 1 1	1 1 1 0 0 0 1 1

Ответ: 1, 1, 0, 0, 1, 0, 0, 1.

1 вариант

1. На бумажную ленту в строку записан 30-буквенный русский алфавит (Е=Ё, И=Й, Ь=Ъ). Из ленты вырезается фрагмент, содержащий 15 букв (например, от М до Ы). Остальные части ленты располагаются под ним "вверх ногами" так, чтобы на краях получившейся таблицы друг над другом оказались соседние буквы алфавита. Для зашифрования сообщения каждую его букву заменяют на вторую букву, стоящую в том же столбце таблицы. Например, зашифровав слово ДЕПО с помощью таблицы на рисунке, получим ТСЗИ. Расшифруйте сообщение **ФЖЛСУЖК ЭМЧЯШЩГГ БРКЮКГФ**, полученное указанным способом (возможно, с использованием другой таблицы).



Решение: Всего ленту можно разрезать 16 способами, так что задача может быть решена перебором. С другой стороны, заметим, что удвоенная Г на конце второго слова может соответствовать только сочетаниям ИИ, ИЙ, ЯЯ или ЕЕ в открытом сообщении (по условию, при зашифровании разные буквы заменяются разными, а одинаковые – одинаковыми). Есть еще и простое дополнительное соображение: при зашифровании буквы с нечетными номерами заменяются на буквы с четными номерами и наоборот, поэтому буква Г (4-я буква) не могла быть заменена на Я (30-я буква) и на Е (6-я буква). Поэтому остается убедиться, что в случае, когда буква И заменяется на Г, действительно получается осмысленное сообщение.

Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Щ	Ш	Ч	Ц

Ответ: ЧЕБЫШЁВ ПАФНУТИЙ ЛЬВОВИЧ

2. Отпирающие комбинации кодового замка представляют собой набор из четырех цифр x_1, x_2, x_3, x_4, каждая из которых равна либо 0, либо 1. Про эти комбинации известно следующее: 1) ровно половина всех наборов открывают замок, 2) если в наборе $x_3 = 1$, то замок откроется в 75% случаев, 3) если $x_1 \cdot x_3 = 1$, то замок откроется в 50% случаев, 4) если $x_2 = 1$, то замок откроется в 25% случаев и 5) если $x_1 + x_4 = 1$, то в 62,5% случаев. Найдите все отпирающие комбинации.

Решение: Выпишем и пронумеруем все комбинации, и для каждой укажем, каким из свойств 2–5 она удовлетворяет.

Номер	Комбинация	Свойство	Номер	Комбинация	Свойство
0	0000		8	1000	5
1	0001	5	9	1001	
2	0010	2	10	1010	2,3,5
3	0011	2,5	11	1011	2,3
4	0100	4	12	1100	4,5
5	0101	4,5	13	1101	4
6	0110	2,4	14	1110	2,3,4,5
7	0111	2,4,5	15	1111	2,3,4

Введем 16 неизвестных $y_0, \dots, y_{15}$, полагая $y_i = 1$, если комбинация с номером i отпирает замок, и $y_i = 0$, если i-тая комбинация замок не отпирает. Согласно условию, составим 5 уравнений:

$$\begin{cases} \mathbf{1)}\ y_0 + \dots + y_{15} = 8 \text{ (свойство 1: ровно половина комбинаций открывают замок)} \\ \mathbf{2)}\ y_2 + y_3 + y_6 + y_7 + y_{10} + y_{11} + y_{14} + y_{15} = 6 \text{ (свойство 2)} \\ \mathbf{3)}\ y_{10} + y_{11} + y_{14} + y_{15} = 2 \text{ (свойство 3: половина комбинаций 10,11,14,15 отпирает замок)} \\ \mathbf{4)}\ y_4 + y_5 + y_6 + y_7 + y_{12} + y_{13} + y_{14} + y_{15} = 2 \text{ (свойство 4)} \\ \mathbf{5)}\ y_1 + y_3 + y_5 + y_7 + y_8 + y_{10} + y_{12} + y_{14} = 5 \text{ (свойство 5: 62,5\% от 8 равно 5)} \end{cases}$$

Вычтя из второго уравнения третье, получим $y_2 + y_3 + y_6 + y_7 = 4$. Следовательно, $y_2 = y_3 = y_6 = y_7 = 1$, то есть комбинации 2, 3, 6, 7 отпирают замок. Подставив $y_6 = y_7 = 1$ в уравнение (4), получим $y_4 + y_5 + y_{12} + y_{13} + y_{14} + y_{15} = 0$. Значит, $y_4 = y_5 = y_{12} = y_{13} = y_{14} = y_{15} = 0$. С учетом найденного, уравнения (1), (3) и (5) принимают вид:

$$\begin{cases} y_0 + y_1 + y_8 + y_9 + y_{10} + y_{11} = 4 \\ y_{10} + y_{11} = 2 \\ y_1 + y_8 + y_{10} = 3. \end{cases}$$

Отсюда находим недостающие 4 отпирающие комбинации: 1, 8, 10, 11.

Ответ: Замок отпирают комбинации 1, 2, 3, 6, 7, 8, 10, 11.

3. В тексте, состоящем из 24 букв и записанном без пробелов, буквы переставлены по следующему правилу: 24-я буква поставлена на 1-е место, 1-я буква – на 2-е место, 23-я – на 3-е место, 2-я – на 4-е и так далее (в конце 13-я буква поставлена на 23-е место, 12-я – на 24-е). Затем такую же процедуру повторили ещё 85 раз. В результате получилось **ААЯАНМШСЧЕИИИТФМРСРМТИСЕ.** Найдите исходный текст.

Решение: По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	4	6	8	10	12	14	16	18	20	22	24	23	21	19	17	15	13	11	9	7	5	3	1

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте:

1→2→4→8→16→17→15→19→11→22→5→10→20→9→18→13→23→3→6→12→24→**1**→ …

То есть, после того как буквы переставили 21 раз, первая буква снова оказалась на первом месте. Попутно получили еще последовательность промежуточных положений первой буквы, а именно: 2,4,...,24. Очевидно, что буквы, стоявшие на этих местах, также займут исходное положение на 21-м шаге. Оставшиеся три буквы, стоящие на местах 7, 14, 21, перемещаются по циклу длины 3: **7**→14→21→**7**→…

Следовательно, после 21 преобразования текст будет совпадать с исходным.

Всего текст был преобразован 86 раз, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).

Ответ: АСИММЕТРИЧНАЯ ШИФРСИСТЕМА.

4. Для формирования защищенного соединения Алиса, Боб и Стелла используют хранящийся в секрете многочлен с целыми коэффициентами a, b, c вида

$$f(x, y) = ax^2 + bx + cxy + by + ay^2,$$

и целые числа (ключи) k_A, k_B, k_C, которые имеют различные остатки при делении на 173. Чтобы отправить Бобу и Стелле сообщение, Алиса формирует новые ключи k_{AB} и k_{AC} по формулам:

$$k_{AB} = r_{173}\big(f(k_A, k_B)\big), \qquad k_{AC} = r_{173}\big(f(k_A, k_C)\big),$$

где $r_{173}(z)$ – остаток от деления числа zна 173. Аналогично Боб для отправки сообщений Стелле вычисляет $k_{BC} = r_{173}\big(f(k_B, k_C)\big)$. Известно, что $k_A = 17$, $k_{AB} = k_{AC} = 52$, и при всех целых x выполняется равенство $r_{173}\big(f(x, k_A)\big) = r_{173}(x^2 + 36x + 59)$. Найдите ключ k_{BC}.

Решение: Из вида многочлена$f(x, y)$ нетрудно понять, что $f(x, y) = f(y, x)$, поэтому

$$r_{173}\big(f(x, k_A)\big) = r_{173}\big(f(k_A, x)\big).$$

Следовательно,

$$k_{AC} = r_{173}\big(f(k_A, k_C)\big) = r_{173}\big({k_C}^2 + 36k_C + 59\big) = 52,$$

А в силу равенства $k_{AB} = k_{AC}$, ключи k_B, k_C являются решениями уравнения:

$$r_{173}(x^2 + 36x + 59) = 52.$$

Запишем, по определению остатка:

$$x^2 + 36x + 59 = 52 + 173t \ (t \in \mathbb{Z}) \Leftrightarrow \ x^2 + 36x + 7 = 173t \Leftrightarrow$$
$$\Leftrightarrow x^2 + 36x + 324 + 7 - 324 = 173t \Leftrightarrow (x + 18)^2 - 317 = 173t \Leftrightarrow$$
$$\Leftrightarrow (x + 18)^2 - 144 = 173t' \Leftrightarrow (x + 30)(x + 6) = 173t'.$$

Из простоты числа 173 вытекает, что либо $x + 30 \,\vdots\, 173$ либо $x + 6 \,\vdots\, 173$. Таким образом:

$$x = -30 + 173t_1, x = -6 + 173t_2.$$

Но согласно условию числа k_B, k_C имеют различные остатки от деления на 173, поэтому, без ограничения общности, можно считать, что $k_B = -30 + 173t_1, k_C = -6 + 173t_2$.

Для нахождения k_{BC} найдем коэффициенты многочлена $f(x,y)$. Имеем для любого целого x равенство:

$$r_{173}(x^2 + 36x + 59) = r_{173}(ax^2 + (b + 17c)x + 116a + 17b).$$

Отсюда $r_{173}(a) = 1, r_{173}(b + 17c) = 36, r_{173}(116a + 17b) = 59$.Значит,

$$116 + 17b = 59 + 173t \Leftrightarrow b = -4 + 10t + \frac{11 + 3t}{17}$$

$$\Leftrightarrow 11 + 3t = 17k \Leftrightarrow t = 6k - 4 + \frac{-k + 1}{3} \Leftrightarrow k = 1 + 3n.$$

В итоге, $b = 17 + 173n$, т.е. $r_{173}(b) = 17$. Аналогично, находим$c = 52 + 173k$,т.е. $r_{173}(c) = 52$.

Теперь, осталось подставить полученные значения в равенство

$$k_{BC} = r_{173}\big(f(k_B, k_C)\big) = 169.$$

Ответ: k_{BC} =169.

5. *Латинским квадратом порядка n* называется квадратная таблица из *n* строк и *n* столбцов, заполненная натуральными числами от 1 до *n* таким образом, что каждый столбец и каждая строка не содержат одинаковые числа. Пусть L – латинский квадрат порядка *n*. Число, стоящее в этом квадрате в строке с номером i и столбце с номером j, обозначим $L(i,j)$.

Два латинских квадрата L_1 и L_2 назовем *ортогональными*, если при их "наложении" не образуется одинаковых пар элементов в разных ячейках таблицы. А именно, если $(i,j) \neq (s,t)$, то $\big(L_1(i,j), L_2(i,j)\big) \neq \big(L_1(s,t), L_2(s,t)\big)$.

а) Постройте пару ортогональных латинских квадратов порядка 4.

б) Докажите, что множество, состоящее из попарно не ортогональных латинских квадратов порядка *n*, не может содержать более чем $n - 1$ квадрат.

Решение: а) Например,

$$L_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix} \quad \text{и} \quad L_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \end{bmatrix}.$$

Замечание. *Ортогональные квадраты существуют для всех* n*, отличных от 2 и 6. Для* $n = p^t$*, где* p *– простое (*$t > 1$*, если* $p = 2$*), способ построение попарно ортогональных квадратов в 1938 г. опубликовал Р. Боуз (R.S. Bose) (потом выяснилось, что этот способ был открыт Муром в 1896 г.). Оказывается, ортогональными будут квадраты L1 и L2, где* $L_i(x,y) = a_i \cdot x + y, i = 1,2$. *Сложение и умножение выполняются в поле* $GF(p^t)$*,* $a_i \neq 0$*,* $a_1 \neq a_2$.

б) Рассмотрим для примера следующий латинский квадрат $\begin{matrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{matrix}$. *Переобозначим* в нем элементы: 1 заменим на 2, 2 – на 3, 3 – на 1. В результате, естественно, вновь получим латинский квадрат: $\begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix}$. Несложно видеть, что если в двух ортогональных квадратах переобозначить элементы (не обязательно одинаковым образом!), то полученные квадраты тоже будут ортогональными.

Пусть теперь есть множество из k попарно ортогональных квадратов. Переобозначим в каждом квадрате элементы так, чтобы, как в разобранном примере, у каждого квадрата первая строка была:$1,2, \dots, n$. Теперь посмотрим, какое число стоит у всех этих квадратов на первом месте во второй строке. Во-первых, так как квадраты латинские, это число отлично от 1. Во-вторых, у разных квадратов эти числа должны быть различными, так как они ортогональны. Всего имеется только $n - 1$ различных чисел, не равных 1. Значит, $k \leq n - 1$. Утверждение доказано.

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

$\boldsymbol{x}^{(1)} = \left(x_1^{(1)}, x_2^{(1)}, x_3^{(1)}, x_4^{(1)}, x_5^{(1)}, x_6^{(1)}, x_7^{(1)}, x_8^{(1)}\right)$ 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 $\boldsymbol{x}^{in} = (0{,}0{,}0{,}0{,}0{,}0{,}0{,}0)$преобразуется в байт $\boldsymbol{x}^{out} = (0{,}1{,}1{,}0{,}1{,}1{,}0{,}1)$.

Решение: Обозначим $\boldsymbol{x}^{in} = \boldsymbol{x}^{(0)}$. На i-том такте выполняется преобразование $\boldsymbol{x}^{(i)} = \boldsymbol{f}_i(\boldsymbol{x}^{(i-1)})$, которое в покомпонентной записи выглядит, согласно условию, следующим образом:

$$x_1^{(i)} = x_2^{(i-1)} \oplus k_i, x_2^{(i)} = x_3^{(i-1)}, x_3^{(i)} = x_4^{(i-1)} \oplus k_i, x_4^{(i)} = x_5^{(i-1)}, x_5^{(i)} = x_6^{(i-1)} \oplus k_i, x_6^{(i)} = \\ = x_7^{(i-1)},\ x_7^{(i)} = x_8^{(i-1)} \oplus k_i, x_8^{(i)} = x_2^{(i-1)} x_7^{(i-1)} \oplus x_1^{(i-1)}.$$

Требуется найти такой ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, что

$$\boldsymbol{x}^{(8)} = \boldsymbol{f}_8\left(\boldsymbol{f}_7\left(\dots \boldsymbol{f}_1(\boldsymbol{x}^{(0)})\right)\right). \qquad (1)$$

Несложно проверить, что отображение $\boldsymbol{x}^{(i-1)} = \boldsymbol{g}_i(\boldsymbol{x}^{(i)})$, покомпонентная запись которого имеет вид

$$x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = \\ = x_6^{(i)},\ x_8^{(i-1)} = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}\left(x_1^{(i)} \oplus k_i\right),$$

является обратным к $\boldsymbol{x}^{(i)} = \boldsymbol{f}_{i-1}\left(\boldsymbol{x}^{(i-1)}\right)$. (Эти формулы обращения следуют из элементарных соображений типа $a = b \oplus c \Leftrightarrow b = a \oplus c$, поэтому выражение для $x_1^{(i-1)}$ естественно получить в последнюю очередь, когда остальные $x_j^{(i-1)}$ уже найдены.) Уравнение (1) эквивалентно уравнению $\boldsymbol{f}_4\left(\boldsymbol{f}_3\left(\boldsymbol{f}_2\left(\boldsymbol{f}_1(\boldsymbol{x}^{(0)})\right)\right)\right) = \boldsymbol{g}_5\left(\boldsymbol{g}_6\left(\boldsymbol{g}_7\left(\boldsymbol{g}_8(\boldsymbol{x}^{(8)})\right)\right)\right)$. Последнее решается полным перебором "половинок" ключа: мы вычисляем правую часть при всевозможных значениях (k_5, k_6, k_7, k_8) (16 вариантов), а затем левую часть для всех (k_1, k_2, k_3, k_4) (также 16 вариантов). Те "половинки", при которых левая и правая части окажутся равными, дадут искомый ключ. Результаты вычислений представлены в таблице.

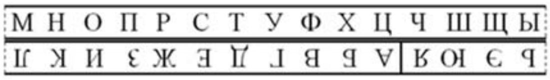
k_1, k_2, k_3, k_4	$\boldsymbol{f}_4\left(\boldsymbol{f}_3\left(\boldsymbol{f}_2\left(\boldsymbol{f}_1(\boldsymbol{x}^{(0)})\right)\right)\right)$	k_5, k_6, k_7, k_8	$\boldsymbol{g}_5\left(\boldsymbol{g}_6\left(\boldsymbol{g}_7\left(\boldsymbol{g}_8(\boldsymbol{x}^{(8)})\right)\right)\right)$
0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0	0 1 1 1 0 1 1 0
0 0 0 1	1 0 1 0 1 0 1 0	0 0 0 1	0 1 1 0 1 1 0 0
0 0 1 0	0 1 0 1 0 1 0 1	0 0 1 0	1 0 0 0 0 0 1 1
0 0 1 1	1 1 1 1 1 1 1 1	0 0 1 1	0 1 1 1 1 0 0 1
0 1 0 0	1 0 1 0 1 0 1 0	0 1 0 0	0 1 0 1 1 1 0 0
0 1 0 1	0 0 0 0 0 0 0 0	0 1 0 1	0 1 0 0 0 1 1 0
0 1 1 0	1 1 1 1 1 1 1 0	0 1 1 0	0 1 1 0 1 0 0 1
0 1 1 1	0 1 0 1 0 1 0 0	0 1 1 1	1 0 0 1 0 0 1 1
1 0 0 0	0 1 0 1 0 1 0 1	1 0 0 0	1 0 1 0 0 0 1 1
1 0 0 1	1 1 1 1 1 1 1 1	1 0 0 1	0 0 1 1 1 0 0 1
1 0 1 0	0 0 0 0 0 0 0 0	$\boxed{1\ 0\ 1\ 0}$	$\boxed{0\ 1\ 0\ 1\ 0\ 1\ 1\ 0}$
1 0 1 1	1 0 1 0 1 0 1 0	1 0 1 1	0 0 1 0 1 1 0 0
1 1 0 0	1 1 1 1 1 1 0 0	1 1 0 0	0 0 0 0 1 0 0 1
$\boxed{1\ 1\ 0\ 1}$	$\boxed{0\ 1\ 0\ 1\ 0\ 1\ 1\ 0}$	1 1 0 1	1 0 0 1 0 0 1 1
1 1 1 0	1 0 1 0 1 0 0 0	1 1 1 0	0 0 1 1 1 1 0 0
1 1 1 1	0 0 0 0 0 0 1 0	1 1 1 1	0 1 0 0 0 1 1 0

Ответ: 1, 1, 0, 1, 1, 0, 1, 0.

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

2 вариант

1. На бумажную ленту в строку записан 30-буквенный русский алфавит (Е=Ё, И=Й, Ь=Ъ). Из ленты вырезается фрагмент, содержащий 15 букв (например, от М до Ы).Остальные части ленты располагаются под ним "вверх ногами" так, чтобы на краях получившейся таблицы друг над другом оказались соседние буквы алфавита. Для зашифрования сообщения каждую его букву заменяют на вторую букву, стоящую в том же столбце таблицы. Например, зашифровав слово ДЕПО с помощью таблицы на рисунке, получим ТСЗИ. Расшифруйте сообщение **ЕВПРШЛОЯЖЗЗ ГЗЖВЕРЗ ЗОРГВОЗШ**, полученное указанным способом (возможно, с использованием другой таблицы).



Решение: Всего ленту можно разрезать 16 способами, так что задача может быть решена перебором. С другой стороны, заметим, что удвоенная З на конце второго слова может соответствовать только сочетаниям ИИ, ИЙ, ЯЯ или ЕЕ в открытом сообщении (по условию, при зашифровании разные буквы заменяются разными, а одинаковые – одинаковыми). Есть еще и простое дополнительное соображение: при зашифровании буквы с нечетными номерами заменяются на буквы с четными номерами и наоборот, поэтому буква З (8-я буква) не могла быть заменена на Я (30-я буква) и на Е (6-я буква). Поэтому остается убедиться, что в случае, когда буква И заменяется на З, действительно получается осмысленное сообщение.

И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
З	Ж	Е	Д	Г	В	Б	А	Я	Ю	Э	Ь	Ы	Щ	Ш

Ответ: ЛОБАЧЕВСКИЙ НИКОЛАЙ ИВАНОВИЧ

2. Отпирающие комбинации кодового замка представляют собой набор из четырех цифр x_1, x_2, x_3, x_4, каждая из которых равна либо 0, либо 1. Про эти комбинации известно следующее: 1) ровно половина всех наборов открывают замок, 2) если в наборе $x_4 = 1$, то замок откроется в 75% случаев, 3) если $x_2 \cdot x_4 = 1$, то замок откроется в 50% случаев, 4) если $x_3 = 1$, то замок откроется в 25% случаев и 5) если $x_1 + x_2 = 1$, то в 62,5% случаев. Найдите все отпирающие комбинации.

Решение: Выпишем и пронумеруем все комбинации, и для каждой укажем, каким из свойств 2–5 она удовлетворяет.

Номер	Комбинация	Свойство
0	0000	
1	0001	2
2	0010	4
3	0011	2,4
4	0100	5
5	0101	2,3,5
6	0110	4,5
7	0111	2,3,4,5

Номер	Комбинация	Свойство
8	1000	5
9	1001	2,5
10	1010	4,5
11	1011	2,4,5
12	1100	
13	1101	2,3
14	1110	4
15	1111	2,3,4

Введем 16 неизвестных $y_0, \ldots, y_{15}$, полагая $y_i = 1$, если комбинация с номером i отпирает замок, и $y_i = 0$, если i-тая комбинация замок не отпирает. Согласно условию, составим 5 уравнений:

$$\begin{cases} \mathbf{1})\ y_0 + \cdots + y_{15} = 8 \text{ (свойство 1: ровно половина комбинаций открывают замок)} \\ \mathbf{2})\ y_1 + y_3 + y_5 + y_7 + y_9 + y_{11} + y_{13} + y_{15} = 6 \text{ (свойство 2)} \\ \mathbf{3})\ y_5 + y_7 + y_{13} + y_{15} = 2 \text{ (свойство 3: половина комбинаций 5,7,13,15 отпирает замок)} \\ \mathbf{4})\ y_2 + y_3 + y_6 + y_7 + y_{10} + y_{11} + y_{14} + y_{15} = 2 \text{ (свойство 4)} \\ \mathbf{5})\ y_4 + y_5 + y_6 + y_7 + y_8 + y_9 + y_{10} + y_{11} = 5 \text{ (свойство 5: 62,5\% от 8 равно 5)} \end{cases}$$

Вычтя из второго уравнения третье, получим $y_1 + y_3 + y_9 + y_{11} = 4$. Следовательно, $y_1 = y_3 = y_9 = y_{11} = 1$, то есть комбинации 1, 3, 9, 11 отпирают замок. Подставив $y_3 = y_{11} = 1$ в уравнение (4), получим $y_2 + y_6 + y_7 + y_{10} + y_{14} + y_{15} = 0$. Значит, $y_2 = y_6 = y_7 = y_{10} = y_{14} = y_{15} = 0$. С учетом найденного, уравнения (1), (3) и (5) принимают вид:

$$\begin{cases} y_0 + y_4 + y_5 + y_8 + y_{12} + y_{13} = 4 \\ y_5 + y_{13} = 2 \\ y_4 + y_5 + y_8 = 3. \end{cases}$$

Отсюда находим недостающие 4 отпирающие комбинации: 4, 5, 8, 13.

Ответ: Замок отпирают комбинации 1, 3, 4, 5, 8, 9, 11, 13.

3. 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.

Решение: По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	4	6	8	10	12	14	16	18	17	15	13	11	9	7	5	3	1

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте:

1→2→4→8→16→5→10→17→3→6→12→13→11→15→7→14→9→18→**1**→…

То есть, после того как буквы переставили 18 раз, первая буква снова оказалась на первом месте. При этом она побывала на всех местах от 1 до 18. Очевидно поэтому, что и остальные буквы сообщения, также займут исходное положение на 18-м шаге.

Всего текст был преобразован 74 раза, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).

Ответ: ТЕОРИЯ ВЕРОЯТНОСТЕЙ.

4. Для формирования защищенного соединения Алиса, Боб и Стелла используют хранящийся в секрете многочлен с целыми коэффициентами a, b, c вида

$$f(x,y) = ax^2 + bx + cxy + by + ay^2,$$

и целые числа (ключи) k_A, k_B, k_C, которые имеют различные остатки при делении на 173. Чтобы отправить Бобу и Стелле сообщение, Алиса формирует новые ключи k_{AB} и k_{AC} по формулам:

$$k_{AB} = r_{173}\big(f(k_A, k_B)\big), \qquad k_{AC} = r_{173}\big(f(k_A, k_C)\big),$$

где $r_{173}(z)$ – остаток от деления числа z на 173. Аналогично Боб для отправки сообщений Стелле вычисляет $k_{BC} = r_{173}\big(f(k_B, k_C)\big)$. Известно, что $k_A = 22$, $k_{AB} = k_{AC} = 41$, и при всех целых x выполняется равенство $r_{173}\big(f(x, k_A)\big) = r_{173}(x^2 + 62x + 37)$. Найдите ключ k_{BC}.

Решение: Из вида многочлена $f(x,y)$ нетрудно понять, что $f(x,y) = f(y,x)$, поэтому

$$r_{173}\big(f(x, k_A)\big) = r_{173}\big(f(k_A, x)\big).$$

Следовательно,

$$k_{AC} = r_{173}\big(f(k_A, k_C)\big) = r_{173}\big({k_C}^2 + 62k_C + 37\big) = 41,$$

А в силу равенства $k_{AB} = k_{AC}$, ключи k_B, k_C являются решениями уравнения:

$$r_{173}(x^2 + 62x + 37) = 41.$$

Запишем, по определению остатка:

$$x^2 + 62x + 37 = 41 + 173t \; (t \in \mathbb{Z}) \Leftrightarrow x^2 + 62x - 4 = 173t \Leftrightarrow$$
$$\Leftrightarrow x^2 + 62x + 961 - 4 - 961 = 173t \Leftrightarrow (x+31)^2 - 965 = 173t \Leftrightarrow$$
$$\Leftrightarrow (x+31)^2 - 100 = 173t' \Leftrightarrow (x+21)(x+41) = 173t'.$$

Из простоты числа 173 вытекает, что либо $x + 21 \,\vdots\, 173$ либо $x + 41 \,\vdots\, 173$. Таким образом:

$$x = -21 + 173t_1, x = -41 + 173t_2.$$

Но согласно условию числа k_B, k_C имеют различные остатки от деления на 173, поэтому, без ограничения общности, можно считать, что $k_B = -21 + 173t_1, k_C = -41 + 173t_2$.

Для нахождения k_{BC} найдем коэффициенты многочлена $f(x,y)$. Имеем для любого целого x равенство:

$$r_{173}(x^2+62x+37) = r_{173}(ax^2+(b+22c)x+138a+22b).$$

Отсюда $r_{173}(a)=1, r_{173}(b+22c)=62, r_{173}(138a+22b)=37$.Значит,

$$138+22b = 37+173t \Leftrightarrow b = -5+8t+\frac{9-3t}{22}$$

$$\Leftrightarrow 9-3t = 22k \Leftrightarrow t = 3-\frac{22k}{3} \Leftrightarrow k = 3n.$$

В итоге, $b = 19-173n$, т.е. $r_{173}(b)=19$. Аналогично, находим$c = 57+173k$, т.е. $r_{173}(c)=57$. Теперь, осталось подставить полученные значения в равенство

$$k_{BC} = r_{173}\big(f(k_B,k_C)\big) = 24.$$

Ответ: k_{BC} =24.

5. *Латинским квадратом порядка n* называется квадратная таблица из *n* строк и *n* столбцов, заполненная натуральными числами от 1 до *n* таким образом, что каждый столбец и каждая строка не содержат одинаковые числа. Пусть L – латинский квадрат порядка *n*. Число, стоящее в этом квадрате в строке с номером i и столбце с номером j, обозначим $L(i,j)$.

Два латинских квадрата L_1 и L_2 назовем *ортогональными*, если при их "наложении" не образуется одинаковых пар элементов в разных ячейках таблицы. А именно, если $(i,j) \neq (s,t)$, то $\big(L_1(i,j), L_2(i,j)\big) \neq \big(L_1(s,t), L_2(s,t)\big)$.

а) Постройте пару ортогональных латинских квадратов порядка 4.

б) Докажите, что множество, состоящее из попарно не ортогональных латинских квадратов порядка *n*, не может содержать более чем $n-1$ квадрат.

Решение: а) Например,

$$L_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix} \quad \text{и} \quad L_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \end{bmatrix}.$$

Замечание. *Ортогональные квадраты существуют для всех* n, *отличных от 2 и 6. Для* $n = p^t$, *где* p *– простое* ($t > 1$, *если* $p = 2$), *способ построение попарно ортогональных квадратов в 1938 г. опубликовал Р. Боуз (R.S. Bose) (потом выяснилось, что этот способ был открыт Муром в 1896 г.). Оказывается, ортогональными будут квадраты L1 и L2, где* $L_i(x,y) = a_i \cdot x + y, i = 1,2$. *Сложение и умножение выполняются в поле* $GF(p^t)$, $a_i \neq 0$, $a_1 \neq a_2$.

б) Рассмотрим для примера следующий латинский квадрат $\begin{matrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{matrix}$. *Переобозначим* в нем элементы: 1 заменим на 2, 2 – на 3, 3 – на 1. В результате, естественно, вновь получим латинский квадрат: $\begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix}$. Несложно видеть, что если в двух ортогональных квадратах переобозначить элементы (не обязательно одинаковым образом!), то полученные квадраты тоже будут ортогональными.

Пусть теперь есть множество из k попарно ортогональных квадратов. Переобозначим в каждом квадрате элементы так, чтобы, как в разобранном примере, у каждого квадрата первая строка была:$1,2,\dots,n$. Теперь посмотрим, какое число стоит у всех этих квадратов на первом месте во второй строке. Во-первых, так как квадраты латинские, это число отлично от 1. Во-вторых, у разных квадратов эти числа должны быть различными, так как они ортогональны. Всего имеется только $n-1$ различных чисел, не равных 1. Значит, $k \leq n-1$. Утверждение доказано.

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 $x_1^{(1)} = x_2 \oplus k_1, x_2^{(1)} = x_3, x_3^{(1)} = x_4 \oplus k_1, x_4^{(1)} = x_5, x_5^{(1)} = x_6 \oplus k_1, x_6^{(1)} = x_7, x_7^{(1)} = x_8 \oplus k_1, x_8^{(1)} = x_2x_7 \oplus x_1$. 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 $\boldsymbol{x}^{(\mathbf{1})}$ на 2-м такте преобразуется в байт $\boldsymbol{x}^{(\mathbf{2})} = (x_1^{(2)}, \dots, x_8^{(2)})$ по аналогичным формулам: $x_1^{(2)} = x_2^{(1)} \oplus k_2, \dots$ На 8-м такте вычисляется выходной байт $\boldsymbol{x}^{out} = \boldsymbol{x}^{(\mathbf{8})}$. Найдите ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, на котором байт $\boldsymbol{x}^{in} = (0,0,0,0,0,0,0,0)$преобразуется в байт $\boldsymbol{x}^{out} = (0,0,1,0,0,1,1,1)$.

Решение: Обозначим $\boldsymbol{x}^{in} = \boldsymbol{x}^{(\mathbf{0})}$. На i-том такте выполняется преобразование $\boldsymbol{x}^{(i)} = \boldsymbol{f}_{\boldsymbol{i}}(\boldsymbol{x}^{(i-1)})$, которое в покомпонентной записи выглядит, согласно условию, следующим образом:

$$x_1^{(i)} = x_2^{(i-1)} \oplus k_i, x_2^{(i)} = x_3^{(i-1)}, x_3^{(i)} = x_4^{(i-1)} \oplus k_i, x_4^{(i)} = x_5^{(i-1)}, x_5^{(i)} = x_6^{(i-1)} \oplus k_i, x_6^{(i)} = \\ = x_7^{(i-1)},\ x_7^{(i)} = x_8^{(i-1)} \oplus k_i, x_8^{(i)} = x_2^{(i-1)} x_7^{(i-1)} \oplus x_1^{(i-1)}.$$

Требуется найти такой ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, что

$$\boldsymbol{x}^{(\mathbf{8})} = \boldsymbol{f}_{\mathbf{8}}\left(\boldsymbol{f}_{\mathbf{7}}\left(\dots \boldsymbol{f}_{\mathbf{1}}(\boldsymbol{x}^{(\mathbf{0})})\right)\right). \qquad (1)$$

Несложно проверить, что отображение $\boldsymbol{x}^{(\boldsymbol{i}-\mathbf{1})} = \boldsymbol{g}_{\boldsymbol{i}}(\boldsymbol{x}^{(i)})$, покомпонентная запись которого имеет вид

$$x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = \\ = x_6^{(i)},\ x_8^{(i-1)} = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}\left(x_1^{(i)} \oplus k_i\right),$$

является обратным к $\boldsymbol{x}^{(i)} = \boldsymbol{f}_{\boldsymbol{i}-\mathbf{1}}(\boldsymbol{x}^{(\boldsymbol{i}-\mathbf{1})})$. (Эти формулы обращения следуют из элементарных соображений типа $a = b \oplus c \Leftrightarrow b = a \oplus c$, поэтому выражение для $x_1^{(i-1)}$ естественно получить в последнюю очередь, когда остальные $x_j^{(i-1)}$ уже найдены.) Уравнение (1) эквивалентно уравнению $\boldsymbol{f}_{\mathbf{4}}\left(\boldsymbol{f}_{\mathbf{3}}\left(\boldsymbol{f}_{\mathbf{2}}\left(\boldsymbol{f}_{\mathbf{1}}(\boldsymbol{x}^{(\mathbf{0})})\right)\right)\right) = \boldsymbol{g}_{\mathbf{5}}\left(\boldsymbol{g}_{\mathbf{6}}\left(\boldsymbol{g}_{\mathbf{7}}\left(\boldsymbol{g}_{\mathbf{8}}(\boldsymbol{x}^{(\mathbf{8})})\right)\right)\right)$. Последнее решается полным перебором "половинок" ключа: мы вычисляем правую часть при всевозможных значениях (k_5, k_6, k_7, k_8) (16 вариантов), а затем левую часть для всех (k_1, k_2, k_3, k_4) (также 16 вариантов). Те "половинки", при которых левая и правая части окажутся равными, дадут искомый ключ. Результаты вычислений представлены в таблице.

k_1, k_2, k_3, k_4	$\boldsymbol{f}_{\mathbf{4}}\left(\boldsymbol{f}_{\mathbf{3}}\left(\boldsymbol{f}_{\mathbf{2}}\left(\boldsymbol{f}_{\mathbf{1}}(\boldsymbol{x}^{(\mathbf{0})})\right)\right)\right)$	k_5, k_6, k_7, k_8	$\boldsymbol{g}_{\mathbf{5}}\left(\boldsymbol{g}_{\mathbf{6}}\left(\boldsymbol{g}_{\mathbf{7}}\left(\boldsymbol{g}_{\mathbf{8}}(\boldsymbol{x}^{(\mathbf{8})})\right)\right)\right)$
0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0	1 1 1 1 0 0 1 0
0 0 0 1	1 0 1 0 1 0 1 0	0 0 0 1	1 1 0 0 1 0 0 0
0 0 1 0	0 1 0 1 0 1 0 1	0 0 1 0	1 1 1 0 0 1 1 1
0 0 1 1	1 1 1 1 1 1 1 1	0 0 1 1	1 1 1 1 1 1 0 1
0 1 0 0	1 0 1 0 1 0 1 0	0 1 0 0	1 1 0 1 1 0 0 0
0 1 0 1	0 0 0 0 0 0 0 0	0 1 0 1	1 1 1 0 0 0 1 0
0 1 1 0	1 1 1 1 1 1 1 0	0 1 1 0	1 0 0 0 1 1 0 1
0 1 1 1	0 1 0 1 0 1 0 0	0 1 1 1	0 0 0 1 0 1 1 1
1 0 0 0	0 1 0 1 0 1 0 1	1 0 0 0	0 0 1 0 0 1 1 1
1 0 0 1	1 1 1 1 1 1 1 1	1 0 0 1	1 0 0 1 1 1 0 1
1 0 1 0	0 0 0 0 0 0 0 0	1 0 1 0	0 0 1 1 0 0 1 0
1 0 1 1	1 0 1 0 1 0 1 0	$\boxed{1\ 0\ 1\ 1}$	$\boxed{1\ 0\ 1\ 0\ 1\ 0\ 0\ 0}$
1 1 0 0	1 1 1 1 1 1 0 0	1 1 0 0	1 0 0 0 1 1 0 1
1 1 0 1	0 1 0 1 0 1 1 0	1 1 0 1	0 0 1 1 0 1 1 1
$\boxed{1\ 1\ 1\ 0}$	$\boxed{1\ 0\ 1\ 0\ 1\ 0\ 0\ 0}$	1 1 1 0	1 1 0 1 1 0 0 0
1 1 1 1	0 0 0 0 0 0 1 0	1 1 1 1	1 1 0 0 0 0 1 0

Ответ: 1, 1, 1, 0, 1, 0, 1, 1.

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

1 вариант

1. В тексте, состоящем из 24 букв и записанном без пробелов, буквы переставлены по следующему правилу: 24-я буква поставлена на 1-е место, 1-я буква – на 2-е место, 23-я – на 3-е место, 2-я – на 4-е и так далее (в конце 13-я буква поставлена на 23-е место, 12-я – на 24-е). Затем такую же процедуру повторили ещё 85 раз. В результате получилось **ТЯИМАИВУКЦНЛИКАЬЛНЯТПУФИ.** Найдите исходный текст.

Решение: По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	4	6	8	10	12	14	16	18	20	22	24	23	21	19	17	15	13	11	9	7	5	3	1

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте:
1→2→4→8→16→17→15→19→11→22→5→10→20→9→18→13→23→3→6→12→24→**1**→ …
То есть, после того как буквы переставили 21 раз, первая буква снова оказалась на первом месте. Попутно получили еще последовательность промежуточных положений первой буквы, а именно: 2,4,...,24. Очевидно, что буквы, стоявшие на этих местах, также займут исходное положение на 21-м шаге. Оставшиеся три буквы, стоящие на местах 7, 14, 21, перемещаются по циклу длины 3: **7**→14→21→**7**→…
Следовательно, после 21 преобразования текст будет совпадать с исходным.
Всего текст был преобразован 86 раз, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).
Ответ: МУЛЬТИПЛИКАТИВНАЯ ФУНКЦИЯ.

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

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

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

Решение: Пусть $L = (L_1, L_2, \dots, L_8)$, $M = (M_1, M_2, \dots, M_8)$ – латинские прямоугольники замка и путешественника соответственно, $L_i, M_i, i \in \{1, \dots, 8\}$, – столбцы этих прямоугольников. Построим множества $A_1, A_2, \dots, A_8$, где $A_i, i \in \{1, \dots, 8\}$, – множество тех и только тех чисел от 1 до 8, которые не встречаются в столбцах L_i и M_i. Например, если M – это ключ Кати, то $A_1 = \{2,4\}$, так как каждым из этих чисел (и только ими) можно дополнить первый столбец прямоугольников L и M. Тогда общее продолжение латинских прямоугольников L и M существует в том и только том случае, когда семейство множеств $A_1, A_2, \dots, A_8$ обладает *системой различных представителей*, т.е. существует такой упорядоченный набор чисел $(a_1, a_2, \dots, a_8)$, что $a_i \neq a_j$ при $i \neq j, a_i \in A_i$. Каждая такая система – это дополнительная строка, которая может быть дописана и к прямоугольнику путешественника, и к прямоугольнику замка. По условию замок открывается, только когда такая дополнительная строка единственна.

Дополнительные строки для ключа Кати: $\{\{4,7,1,6,2,8,3,5\}, \{4,7,3,6,1,8,2,5\}, \{4,7,3,6,2,8,1,5\}\}$.

Дополнительные строки для ключа Юры: $\{\{5,2,7,8,1,4,6,3\}\}$.

Ответ: Ключ Юры правильный.

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.

Решение: Докажем утверждение индукцией по k (числу наборов).

- Для одного набора $\mathbf{w_1}$ утверждение очевидно.
- Предположим, что утверждение верно для любых $k-1$ различных наборов ($k > 1$).
- Докажем на основании этого предположения, что утверждение справедливо и для произвольных k различных наборов $\boldsymbol{w_1} = (w_{11}, w_{12}, \dots, w_{1n}), \dots, \boldsymbol{w_k} = (w_{k1}, w_{k2}, \dots, w_{kn})$. По предположению индукции для первых $k-1$ наборов $\boldsymbol{w_1}, \dots, \boldsymbol{w_{k-1}}$ существует такое отображение $\sigma: \mathbb{N} \to \{1,2,\dots,k-1\}$, что наборы $\boldsymbol{w_1^\sigma} = \big(\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})\big), \dots, \boldsymbol{w_{k-1}^\sigma} = \Big(\sigma\big(w_{k-1,1}\big), \sigma\big(w_{k-1,2}\big), \dots, \sigma\big(w_{k-1,n}\big)\Big)$ различны. Если при этом и все k наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}, \boldsymbol{w_k^\sigma}$ оказались различными, то утверждение доказано. Если же это не так, то набор $\boldsymbol{w_k^\sigma}$ совпадает с одним из наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$, причем *ровно с одним*, так как, по предположению, эти $k-1$ наборов различны. Не ограничивая общности, можно считать, что $\boldsymbol{w_1^\sigma} = \boldsymbol{w_k^\sigma}$. Поскольку исходные наборы $\boldsymbol{w_1}$ и $\boldsymbol{w_k}$ различны, то $w_{1i} \neq w_{ki}$ для некоторого i, и при этом $\sigma(w_{1i}) = \sigma(w_{ki})$. Переопределим тогда отображение σ, положив $\sigma(w_{ki}) = k$. Для так переопределенного σ наборы $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$ по-прежнему останутся различными, и при этом набор $\boldsymbol{w_k^\sigma}$ будет отличен от них. Утверждение доказано.

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 111) 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	1	0	0
001	1	1	1	0
010	1	0	0	0
011	1	0	1	1
100	1	1	1	1
101	0	0	0	1
110	1	1	0	1
111	0	1	0	1

Решение: Если, например, подать на вход 000, то на выходе мы получим 0, если устройство работает правильно или имеет неисправность типа Н2 или Н3, либо 1, если имеется неисправность Н1. Значит, вход 000 позволяет *различить*, скажем, неисправности Н1 и Н3, но не позволяет отличить ПР от Н2. Составим таблицу, где для каждого входа укажем, какие пары режимов этот вход различить может (символ 1), а какие – нет (символ 0).

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

Чтобы определить режим работы устройства, нужно подать на вход такие комбинации, что им соответствующие строки покрывают единицами все столбцы (то есть в каждом столбце есть хотя бы одна единица, стоящая в одной из этих строк). Сразу можно заметить, что входных комбинаций потребуется по крайней мере 3, так как никакие 2 строки не покрывают все столбцы.

Вход 111 покрывает 4 столбца. Непокрытыми остаются столбец ПР и Н2 (покрывается входами 010 и 110) и столбец Н1 и Н3 (покрывается входами 000, 001, 011, 101).

Таким образом, имеем 8 наборов, по 3 входные комбинации в каждом:

111-{010,110}-{000, 001, 011, 101}.

Ответ: Минимальное количество входных комбинаций равно 3. Всего 8 наборов: 111-{010,110}-{000, 001, 011, 101}.

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 `48,DB,05,9F,15` (но неизвестно какому числу какой именно байт соответствует). Найдите d, если $n = 64159, y = 5653$. *Указание*: фигурирующие в задаче числа представимы в виде двух байтов, например $64159 = 15 \cdot 16^3 + 10 \cdot 16^2 + 9 \cdot 16^1 + 15 \cdot 16^0 =$ `FA 9F` (см. таблицу); `9F` – младший байт числа 64159.

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

Решение: Постараемся определить, какой именно из данных в задаче байтов 48,DB,05,9F,15 – младший байт числа p. Байт 9F – это байт n; 15 – это байт сообщения y, так как можно подсчитать, что $5653 = 22 \cdot 16^2 + 1 \cdot 16 + 5$; 48 также не годится, поскольку число p нечетно. Таким обзом, младший байт p – это или DB, или 05.

Заметим, что или у числа p, или у числа q старший байт равен 00. Действительно, если это не так, то каждое из этих чисел было бы больше, чем 256, а их произведение превосходило $n = 64159$. Предположим, что 00 – старший байт числа p. Тогда или $p = 00\ \ 05 = 5$, что невозможно, поскольку n на 5 не делится, или $p = 00\ \ D5 = 219$, что также невозможно, так как p – простое, но 219 делится на 3.

Итак, установили, что старший байт q равен 00, а младший байт p – это или DB, или 05. Найдем теперь число q. (Зная q, мы найдем $p = n/q$, а затем, решив уравнение $r_{(p-1)(q-1)}(3d) = 1$, получим искомое d.) Пусть $p = p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0$ и $q = q_1 \cdot 16^1 + q_0 \cdot 16^0$. Так как

$$n = p \cdot q = (p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0) \cdot (q_1 \cdot 16^1 + q_0 \cdot 16^0),$$

то

$$r_{16}(n) = r_{16}(p_0 q_0),$$
$$r_{16}\left(\frac{n - p_0 q_0}{16}\right) = r_{16}(p_1 q_0 + p_0 q_1). \qquad (1)$$

Пусть $p_0 = 5, p_1 = 0$. Далее $r_{16}(n) = 15 = r_{16}(5q_0) \Longrightarrow q_0 = 3$. Из второй формулы (1) находим $r_{16}(p_1 q_0 + p_0 q_1) = 9 \Longrightarrow q_1 = 5$. В итоге $q = 83 \Rightarrow p = 773 \Rightarrow (p-1)(q-1) = 63304$. Из уравнения $r_{(p-1)(q-1)}(3d) = 1$ следует, что $d = \frac{1 + t \cdot (p-1)(q-1)}{3}$. Здесь натуральное число t не превосходит 3, так как, по условию, число d представимо в виде двух байтов, то есть $d \le 65535$. Непосредственной проверкой убеждаемся, что числитель делится нацело на 3 при $t = 2 \Rightarrow d = 42203$.

В случае, когда младший байт p – это DB, ответ получен быть не может, так как n не поделится на q нацело.

Ответ: $d = 42203$.

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 $\boldsymbol{x^{out}} = (1,1,1,0,0,0,1,1)$, а байт $\boldsymbol{x^{in}} = (1,1,1,1,1,1,1,1)$ – в байт $\boldsymbol{x^{out}} = (0,1,1,1,1,0,1,0)$.

Решение: Обозначим $\boldsymbol{x^{in}} = \boldsymbol{x^{(0)}}$. На i-том такте выполняется преобразование $\boldsymbol{x^{(i)}} = \boldsymbol{f_i}(\boldsymbol{x^{(i-1)}})$, которое в покомпонентной записи выглядит, согласно условию, следующим образом:

$$x_1^{(i)} = x_2^{(i-1)} \oplus k_i, x_2^{(i)} = x_3^{(i-1)}, x_3^{(i)} = x_4^{(i-1)} \oplus k_i, x_4^{(i)} = x_5^{(i-1)}, x_5^{(i)} = x_6^{(i-1)} \oplus k_i, x_6^{(i)} = x_7^{(i-1)},\ x_7^{(i)} = \\ = x_8^{(i-1)} \oplus k_i, x_8^{(i)} = x_2^{(i-1)} x_7^{(i-1)} \oplus x_1^{(i-1)}.$$

Будем искать такой ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, чтобы пока только для первой пары $\boldsymbol{x^{(0)}}$, $\boldsymbol{x^{(8)}}$ (то есть для $\boldsymbol{x^{(0)}} = (1,0,1,0,1,0,1,0)$ и $\boldsymbol{x^{(8)}} = (1,1,1,0,0,0,1,1)$) выполнялось требуемое:

$$\boldsymbol{x^{(8)}} = \boldsymbol{f_8}\left(\boldsymbol{f_7}\left(\dots \boldsymbol{f_1}(\boldsymbol{x^{(0)}})\right)\right). \qquad (1)$$

Несложно проверить, что отображение $\boldsymbol{x^{(i-1)}} = \boldsymbol{g_i}(\boldsymbol{x^{(i)}})$, покомпонентная запись которого имеет вид

$$x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = x_6^{(i)},\ x_8^{(i-1)} = \\ = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}\left(x_1^{(i)} \oplus k_i\right),$$

является обратным к $\boldsymbol{x^{(i)}} = \boldsymbol{f_{i-1}}(\boldsymbol{x^{(i-1)}})$. (Эти формулы обращения следуют из элементарных соображений типа $a = b \oplus c \Leftrightarrow b = a \oplus c$, поэтому выражение для $x_1^{(i-1)}$ естественно получить в последнюю очередь, когда остальные $x_j^{(i-1)}$ уже найдены.) Уравнение (1) эквивалентно уравнению $\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}(\boldsymbol{x^{(0)}})\right)\right)\right) = \boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}(\boldsymbol{x^{(8)}})\right)\right)\right)$. Последнее решается полным перебором "половинок" ключа: мы вычисляем правую часть при всевозможных значениях (k_5, k_6, k_7, k_8) (16 вариантов), а затем левую часть для всех (k_1, k_2, k_3, k_4) (также 16 вариантов). Те "половинки", при которых левая и правая части окажутся равными, дадут искомый ключ. Результаты вычислений представлены в таблице.

k_1, k_2, k_3, k_4	$\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}\left(\boldsymbol{x}^{(\mathbf{0})}\right)\right)\right)\right)$	k_5, k_6, k_7, k_8	$\boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}\left(\boldsymbol{x}^{(\mathbf{8})}\right)\right)\right)\right)$
0 0 0 0	1 0 1 0 1 0 1 0	0 0 0 0	0 0 1 1 1 1 1 0
0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 1	1 0 1 1 0 1 0 0
0 0 1 0	1 1 1 1 1 1 1 0	0 0 1 0	0 0 1 0 1 0 1 1
0 0 1 1	0 1 0 1 0 1 0 0	0 0 1 1	1 1 0 0 0 0 0 1
0 1 0 0	0 0 0 0 0 0 0 0	0 1 0 0	1 0 0 1 0 1 0 0
0 1 0 1	1 0 1 0 1 0 1 0	0 1 0 1	0 0 0 1 1 1 1 0
0 1 1 0	0 1 0 1 0 1 0 1	0 1 1 0	1 1 0 0 0 0 0 1
0 1 1 1	1 1 1 1 1 1 1 1	0 1 1 1	0 0 1 0 1 0 1 1
1 0 0 0	1 1 1 1 1 0 0 1	1 0 0 0	1 1 1 0 1 0 1 1
1 0 0 1	0 1 0 1 0 0 1 1	1 0 0 1	1 1 1 0 0 0 0 1
1 0 1 0	1 0 1 0 1 1 0 1	1 0 1 0	1 1 1 1 1 1 1 0
1 0 1 1	0 0 0 0 0 1 1 1	1 0 1 1	1 0 0 1 0 1 0 0
1 1 0 0	0 1 0 1 0 0 0 1	1 1 0 0	1 1 0 0 0 0 0 1
1 1 0 1	1 1 1 1 1 0 1 1	1 1 0 1	1 1 0 0 1 0 1 1
1 1 1 0	0 0 0 0 0 1 0 0	1 1 1 0	1 0 0 1 0 1 0 0
1 1 1 1	1 0 1 0 1 1 1 0	1 1 1 1	1 1 1 1 1 1 1 0

Имеется, таким образом, два ключа, $\boldsymbol{k_1} = (0, 0, 1, 0, 1, 0, 1, 0)$ и $\boldsymbol{k_2} = (0, 0, 1, 0, 1, 1, 1, 1)$, на которых для первой пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ выполняется (1). Непосредственной проверкой убеждаемся, что на ключе $\boldsymbol{k_2}$ для второй пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ равенство (1) также выполняется, а на ключе $\boldsymbol{k_1}$ – нет.

Ответ: $0, 0, 1, 0, 1, 1, 1, 1$.

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

2 вариант

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.

Решение: По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2	4	6	8	10	12	14	16	18	20	22	21	19	17	15	13	11	9	7	5	3	1

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте:

1→2→4→8→16→13→19→7→14→17→11→22→**1**→…

То есть, после того как буквы переставили 12 раз, первая буква снова оказалась на первом месте. Попутно получили еще последовательность промежуточных положений первой буквы, а именно: 2,4,...,22. Очевидно, что буквы, стоявшие на этих местах, также займут исходное положение на 21-м шаге. Оставшиеся буквы, перемещаются по циклам длины 4, 3 и 2: **3**→6→12→21→**3**→…, **5**→10→20→**5**→…, **9**→18→**9**→…

Следовательно, после 12 преобразований текст будет совпадать с исходным.

Всего текст был преобразован 50 раз, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).

Ответ: ТЕОРЕТИЧЕСКАЯ СТОЙКОСТЬ.

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

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

Ключ Кати

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

Ключ Юры

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

Решение: Пусть $L = (L_1, L_2, \dots, L_8)$, $M = (M_1, M_2, \dots, M_8)$ – латинские прямоугольники замка и путешественника соответственно, $L_i, M_i, i \in \{1, \dots, 8\}$, – столбцы этих прямоугольников. Построим множества $A_1, A_2, \dots, A_8$, где $A_i, i \in \{1, \dots, 8\}$, – множество тех и только тех чисел от 1 до 8, которые не встречаются в столбцах L_i и M_i. Например, если M – это ключ Кати, то $A_1 = \{5,7,8\}$, так как каждым из этих чисел (и только ими) можно дополнить первый столбец прямоугольников L и M. Тогда общее продолжение латинских прямоугольников L и M существует в том и только том случае, когда семейство множеств $A_1, A_2, \dots, A_8$ обладает *системой различных представителей*, т.е. существует такой упорядоченный набор чисел $(a_1, a_2, \dots, a_8)$, что $a_i \neq a_j$ при $i \neq j, a_i \in A_i$. Каждая такая система – это дополнительная строка, которая может быть дописана и к прямоугольнику путешественника, и к прямоугольнику замка. По условию замок открывается, только когда такая дополнительная строка единственна.

Дополнительные строки для ключа Кати: $\{\{5,7,2,4,6,1,3,8\}\}$.

Дополнительных строк для ключа Юры нет.

Ответ: Ключ Кати правильный.

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 $\boldsymbol{w_1^\sigma} = (\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})), \dots, \boldsymbol{w_k^\sigma} = (\sigma(w_{k1}), \sigma(w_{k2}), \dots, \sigma(w_{kn}))$ также будут различны.

Решение: Докажем утверждение индукцией по k (числу наборов).

- Для одного набора $\mathbf{w_1}$ утверждение очевидно.
- Предположим, что утверждение верно для любых $k-1$ различных наборов ($k > 1$).

- Докажем на основании этого предположения, что утверждение справедливо и для произвольных k различных наборов $\boldsymbol{w_1} = (w_{11}, w_{12}, \dots, w_{1n}), \dots, \boldsymbol{w_k} = (w_{k1}, w_{k2}, \dots, w_{kn})$. По предположению индукции для первых $k-1$ наборов $\boldsymbol{w_1}, \dots, \boldsymbol{w_{k-1}}$ существует такое отображение $\sigma: \mathbb{N} \to \{1,2,\dots,k-1\}$, что наборы $\boldsymbol{w_1^\sigma} = (\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})), \dots, \boldsymbol{w_{k-1}^\sigma} = \left(\sigma(w_{k-1,1}), \sigma(w_{k-1,2}), \dots, \sigma(w_{k-1,n})\right)$ различны. Если при этом и все k наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}, \boldsymbol{w_k^\sigma}$ оказались различными, то утверждение доказано. Если же это не так, то набор $\boldsymbol{w_k^\sigma}$ совпадает с одним из наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$, причем *ровно с одним*, так как, по предположению, эти $k-1$ наборов различны. Не ограничивая общности, можно считать, что $\boldsymbol{w_1^\sigma} = \boldsymbol{w_k^\sigma}$. Поскольку исходные наборы $\boldsymbol{w_1}$ и $\boldsymbol{w_k}$ различны, то $w_{1i} \neq w_{ki}$ для некоторого i, и при этом $\sigma(w_{1i}) = \sigma(w_{ki})$. Переопределим тогда отображение σ, положив $\sigma(w_{ki}) = k$. Для так переопределенного σ наборы $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$ по-прежнему останутся различными, и при этом набор $\boldsymbol{w_k^\sigma}$ будет отличен от них. Утверждение доказано.

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 000) 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	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

Решение: Если, например, подать на вход 000, то на выходе мы получим 0, если устройство работает правильно или имеет неисправность типа Н2, либо 1, если имеется неисправность Н1 или Н3. Значит, вход 000 позволяет *различить*, скажем, неисправности Н2 и Н3, но не позволяет отличить ПР от Н2. Составим таблицу, где для каждого входа укажем, какие пары режимов этот вход различить может (символ 1), а какие – нет (символ 0).

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

Чтобы определить режим работы устройства, нужно подать на вход такие комбинации, что им соответствующие строки покрывают единицами все столбцы (то есть в каждом столбце есть хотя бы одна единица, стоящая в одной из этих строк). Сразу можно заметить, что входных комбинаций потребуется по крайней мере 3, так как никакие 2 строки не покрывают все столбцы.

Вход 000 покрывает 4 столбца. Непокрытыми остаются столбец ПР и Н2 (покрывается входами 101 и 100) и столбец Н1 и Н3 (покрывается входами 001, 010, 011, 110).

Таким образом, имеем 8 наборов, по 3 входные комбинации в каждом:

000-{100,101}-{001, 010, 011, 110}

Ответ: Минимальное количество входных комбинаций равно 3. Всего 8 наборов: 000-{010,110}-{000, 001, 011, 101}.

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 `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

Решение: Постараемся определить, какой именно из данных в задаче байтов `6B,5F,4B,F0,29` – младший байт числа p. Байт `5F` – это байт n; `6B` – это байт сообщения y, так как можно подсчитать, что $38507 = 150 \cdot 16^2 + 6 \cdot 16 + 11$; `F0` также не годится, поскольку число p нечетно. Таким обзом, младший байт p – это или `29`, или `4B`.
Заметим, что или у числа p, или у числа q старший байт равен `00`. Действительно, если это не так, то каждое из этих чисел было бы больше, чем 256, а их произведение превосходило $n = 57439$. Предположим, что `00` – старший байт числа p. Тогда или $p = \mathtt{00\ 29} = 41$, что невозможно, поскольку n на 41 не делится, или $p = \mathtt{00\ 4B} = 75$, что также невозможно, так как p – простое, но 75 делится на 5.
Итак, установили, что старший байт q равен `00`, а младший байт p – это или `29`, или `4B`. Найдем теперь число q. (Зная q, мы найдем $p = n/q$, а затем, решив уравнение $r_{(p-1)(q-1)}(3d) = 1$, получим искомое d.)
Пусть $p = p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0$ и $q = q_1 \cdot 16^1 + q_0 \cdot 16^0$. Так как

$$n = p \cdot q = (p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0) \cdot (q_1 \cdot 16^1 + q_0 \cdot 16^0),$$

то

$$r_{16}(n) = r_{16}(p_0 q_0),$$
$$r_{16}\left(\frac{n - p_0 q_0}{16}\right) = r_{16}(p_1 q_0 + p_0 q_1). \qquad (1)$$

Пусть $p_0 = 9, p_1 = 2$. Далее $r_{16}(n) = 15 = r_{16}(9q_0) \Longrightarrow q_0 = 7$. Из второй формулы (1) находим $r_{16}(p_1 q_0 + p_0 q_1) = 2 \Longrightarrow q_1 = 5$. В итоге $q = 71 \Rightarrow p = 809 \Rightarrow\ (p-1)(q-1) = 56560$. Из уравнения $r_{(p-1)(q-1)}(3d) = 1$ следует, что $d = \frac{1 + t \cdot (p-1)(q-1)}{3}$. Здесь натуральное число t не превосходит 3, так как, по условию, число d представимо в виде двух байтов, то есть $d \le 65535$. Непосредственной проверкой убеждаемся, что числитель делится нацело на 3 при $t = 2 \Rightarrow d = 37707$.
В случае, когда младший байт p – это `4B`, ответ получен быть не может, так как n не поделится на q нацело.
Ответ: $d = 37707$.

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 $\boldsymbol{x^{out}} = (0,0,0,0,0,1,1,1)$, а байт $\boldsymbol{x^{in}} = (1,1,1,1,1,1,1,1)$ – в байт $\boldsymbol{x^{out}} = (1,0,0,1,1,1,0,1)$.
Решение: Обозначим $\boldsymbol{x^{in}} = \boldsymbol{x^{(0)}}$. На i-том такте выполняется преобразование $\boldsymbol{x^{(i)}} = \boldsymbol{f_i}(\boldsymbol{x^{(i-1)}})$, которое в покомпонентной записи выглядит, согласно условию, следующим образом:

$$x_1^{(i)} = x_2^{(i-1)} \oplus k_i, x_2^{(i)} = x_3^{(i-1)}, x_3^{(i)} = x_4^{(i-1)} \oplus k_i, x_4^{(i)} = x_5^{(i-1)}, x_5^{(i)} = x_6^{(i-1)} \oplus k_i, x_6^{(i)} = x_7^{(i-1)},\ x_7^{(i)} = x_8^{(i-1)} \oplus k_i, x_8^{(i)} = x_2^{(i-1)} x_7^{(i-1)} \oplus x_1^{(i-1)}.$$

Будем искать такой ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, чтобы пока только для первой пары $\boldsymbol{x^{(0)}}$, $\boldsymbol{x^{(8)}}$ (то есть для $\boldsymbol{x^{(0)}} = (1,0,1,0,1,0,1,0)$ и $\boldsymbol{x^{(8)}} = (0,0,0,0,0,1,1,1)$) выполнялось требуемое:

$$\boldsymbol{x^{(8)}} = \boldsymbol{f_8}\left(\boldsymbol{f_7}\left(\dots \boldsymbol{f_1}(\boldsymbol{x^{(0)}})\right)\right). \qquad (1)$$

Несложно проверить, что отображение $\boldsymbol{x^{(i-1)}} = \boldsymbol{g_i}(\boldsymbol{x^{(i)}})$, покомпонентная запись которого имеет вид

$$x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = x_6^{(i)},\ x_8^{(i-1)} = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}\left(x_1^{(i)} \oplus k_i\right),$$

является обратным к $\boldsymbol{x^{(i)}} = \boldsymbol{f_{i-1}}(\boldsymbol{x^{(i-1)}})$. (Эти формулы обращения следуют из элементарных соображений типа $a = b \oplus c \Leftrightarrow b = a \oplus c$, поэтому выражение для $x_1^{(i-1)}$ естественно получить в последнюю очередь, когда остальные $x_j^{(i-1)}$ уже найдены.) Уравнение (1) эквивалентно уравнению $\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}(\boldsymbol{x^{(0)}})\right)\right)\right) = \boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}(\boldsymbol{x^{(8)}})\right)\right)\right)$**.** Последнее решается полным перебором "половинок" ключа: мы вычисляем правую часть при всевозможных значениях (k_5, k_6, k_7, k_8) (16 вариантов), а затем левую часть для всех (k_1, k_2, k_3, k_4) (также 16 вариантов). Те "половинки", при которых левая и правая части окажутся равными, дадут искомый ключ. Результаты вычислений представлены в таблице.

k_1, k_2, k_3, k_4	$\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}(\boldsymbol{x}^{(\mathbf{0})})\right)\right)\right)$	k_5, k_6, k_7, k_8	$\boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}(\boldsymbol{x}^{(\mathbf{8})})\right)\right)\right)$
0 0 0 0	1 0 1 0 1 0 1 0	0 0 0 0	0 1 1 1 0 0 0 0
0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 1	0 1 0 0 1 0 1 0
0 0 1 0	1 1 1 1 1 1 1 0	0 0 1 0	0 1 1 0 0 1 0 1
0 0 1 1	0 1 0 1 0 1 0 0	0 0 1 1	0 1 1 1 1 1 1 1
0 1 0 0	0 0 0 0 0 0 0 0	0 1 0 0	0 1 0 1 1 0 1 0
0 1 0 1	1 0 1 0 1 0 1 0	0 1 0 1	0 1 1 0 0 0 0 0
0 1 1 0	0 1 0 1 0 1 0 1	0 1 1 0	1 0 0 0 1 1 1 1
0 1 1 1	1 1 1 1 1 1 1 1	0 1 1 1	0 0 0 1 0 1 0 1
1 0 0 0	1 1 1 1 1 0 0 1	1 0 0 0	0 0 1 0 0 1 0 1
1 0 0 1	0 1 0 1 0 0 1 1	1 0 0 1	1 0 0 1 1 1 1 1
1 0 1 0	1 0 1 0 1 1 0 1	1 0 1 0	0 0 1 1 0 0 0 0
1 0 1 1	0 0 0 0 0 1 1 1	1 0 1 1	1 0 1 0 1 0 1 0
1 1 0 0	0 1 0 1 0 0 0 1	1 1 0 0	1 0 0 0 1 1 1 1
1 1 0 1	1 1 1 1 1 0 1 1	1 1 0 1	0 0 1 1 0 1 0 1
1 1 1 0	0 0 0 0 0 1 0 0	1 1 1 0	0 1 0 1 1 0 1 0
1 1 1 1	1 0 1 0 1 1 1 0	1 1 1 1	0 1 0 0 0 0 0 0

Имеется, таким образом, два ключа, $\boldsymbol{k_1} = (0, 0, 0, 0, 1, 0, 1, 1)$ и $\boldsymbol{k_2} = (0, 1, 0, 1, 1, 0, 1, 1)$, на которых для первой пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ выполняется (1). Непосредственной проверкой убеждаемся, что на ключе $\boldsymbol{k_1}$ для второй пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ равенство (1) также выполняется, а на ключе $\boldsymbol{k_2}$ – нет.

Ответ: $0, 0, 0, 0, 1, 0, 1, 1$.

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

3 вариант

1. В тексте, состоящем из 24 букв и записанном без пробелов, буквы переставлены по следующему правилу: 24-я буква поставлена на 1-е место, 1-я буква – на 2-е место, 23-я на 3-е место, 2-я – на 4-е и так далее (в конце 13-я буква поставлена на 23-е место, 12-я – на 24-е). Затем такую же процедуру повторили ещё 85 раз. В результате получилось **ААЯАНМШСЧЕИИИТФМРСРМТИСЕ.** Найдите исходный текст.

Решение: По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	4	6	8	10	12	14	16	18	20	22	24	23	21	19	17	15	13	11	9	7	5	3	1

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте:
1→2→4→8→16→17→15→19→11→22→5→10→20→9→18→13→23→3→6→12→24→**1**→ …
То есть, после того как буквы переставили 21 раз, первая буква снова оказалась на первом месте. Попутно получили еще последовательность промежуточных положений первой буквы, а именно: 2,4,...,24. Очевидно, что буквы, стоявшие на этих местах, также займут исходное положение на 21-м шаге. Оставшиеся три буквы, стоящие на местах 7, 14, 21, перемещаются по циклу длины 3: **7**→14→21→**7**→…
Следовательно, после 21 преобразования текст будет совпадать с исходным.
Всего текст был преобразован 86 раз, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).
Ответ: АСИММЕТРИЧНАЯ ШИФРСИСТЕМА.

2. Чтобы попасть в Криптоландию, необходимо пройти через ворота с электронным замком, предъявив правильный ключ. В микросхеме замка хранится таблица размерами 3х8 (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 4х8. 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 4х8 и 5х8, 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
$$\begin{pmatrix} 4 & 6 & 3 & 5 & 7 & 1 & 2 & 8 \\ 8 & 5 & 4 & 1 & 6 & 7 & 3 & 2 \\ 3 & 4 & 5 & 2 & 8 & 6 & 1 & 7 \end{pmatrix}$$

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

Решение: Пусть $L = (L_1, L_2, \dots, L_8)$, $M = (M_1, M_2, \dots, M_8)$ – латинские прямоугольники замка и путешественника соответственно, $L_i, M_i, i \in \{1, \dots, 8\}$, – столбцы этих прямоугольников. Построим множества $A_1, A_2, \dots, A_8$, где $A_i, i \in \{1, \dots, 8\}$, – множество тех и только тех чисел от 1 до 8, которые не встречаются в столбцах L_i и M_i. Например, если M – это ключ Кати, то $A_1 = \{2,5\}$, так как каждым из этих чисел (и только ими) можно дополнить первый столбец прямоугольников L и M. Тогда общее продолжение латинских прямоугольников L и M существует в том и только том случае, когда семейство множеств $A_1, A_2, \dots, A_8$ обладает *системой различных представителей*, т.е. существует такой упорядоченный набор чисел $(a_1, a_2, \dots, a_8)$, что $a_i \neq a_j$ при $i \neq j, a_i \in A_i$. Каждая такая система – это дополнительная строка, которая может быть дописана и к прямоугольнику путешественника, и к прямоугольнику замка. По условию замок открывается, только когда такая дополнительная строка единственна.

Дополнительных строк для ключа Кати нет.

Дополнительные строки для ключа Юры: {{7,2,6,3,1,4,8,5}}.

Ответ: Ключ Юры правильный.

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 $\boldsymbol{w_1^\sigma} = (\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})), \dots, \boldsymbol{w_k^\sigma} = (\sigma(w_{k1}), \sigma(w_{k2}), \dots, \sigma(w_{kn}))$ также будут различны.

Решение: Докажем утверждение индукцией по k (числу наборов).

- Для одного набора $\mathbf{w_1}$ утверждение очевидно.
- Предположим, что утверждение верно для любых $k-1$ различных наборов ($k > 1$).
- Докажем на основании этого предположения, что утверждение справедливо и для произвольных k различных наборов $\boldsymbol{w_1} = (w_{11}, w_{12}, \dots, w_{1n}), \dots, \boldsymbol{w_k} = (w_{k1}, w_{k2}, \dots, w_{kn})$. По предположению индукции для первых $k-1$ наборов $\boldsymbol{w_1}, \dots, \boldsymbol{w_{k-1}}$ существует такое отображение $\sigma: \mathbb{N} \to \{1,2,\dots,k-1\}$, что наборы $\boldsymbol{w_1^\sigma} = (\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})), \dots, \boldsymbol{w_{k-1}^\sigma} = \left(\sigma(w_{k-1,1}), \sigma(w_{k-1,2}), \dots, \sigma(w_{k-1,n})\right)$ различны. Если при этом и все k наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}, \boldsymbol{w_k^\sigma}$ оказались различными, то утверждение доказано. Если же это не так, то набор $\boldsymbol{w_k^\sigma}$ совпадает с одним из наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$, причем *ровно с одним*, так как, по предположению, эти $k-1$ наборов различны. Не ограничивая общности, можно считать, что $\boldsymbol{w_1^\sigma} = \boldsymbol{w_k^\sigma}$. Поскольку исходные наборы $\boldsymbol{w_1}$ и $\boldsymbol{w_k}$ различны, то $w_{1i} \neq w_{ki}$ для некоторого i, и при этом $\sigma(w_{1i}) = \sigma(w_{ki})$. Переопределим тогда отображение σ, положив $\sigma(w_{ki}) = k$. Для так переопределенного σ наборы $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$ по-прежнему останутся различными, и при этом набор $\boldsymbol{w_k^\sigma}$ будет отличен от них. Утверждение доказано.

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 110) 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	1	0	0	0
001	1	0	1	1
010	0	1	0	0
011	1	1	1	0
100	0	0	0	1
101	1	1	1	1
110	0	1	0	1
111	1	1	0	1

Решение: Если, например, подать на вход 000, то на выходе мы получим 0, если имеется неисправность Н1, Н2 или Н3, либо 1, если устройство работает правильно. Значит, вход 000 позволяет *различить*, скажем, режим ПР и Н3, но не позволяет отличить Н1 от Н2. Составим таблицу, где для каждого входа укажем, какие пары режимов этот вход различить может (символ 1), а какие – нет (символ 0).

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

Чтобы определить режим работы устройства, нужно подать на вход такие комбинации, что им соответствующие строки покрывают единицами все столбцы (то есть в каждом столбце есть хотя бы одна единица, стоящая в одной из этих строк). Сразу можно заметить, что входных комбинаций потребуется по крайней мере 3, так как никакие 2 строки не покрывают все столбцы.
Вход 110 покрывает 4 столбца. Непокрытыми остаются столбец ПР и Н2 (покрывается входами 000 и 111) и столбец Н1 и Н3 (покрывается входами 001, 010, 011, 100).
Таким образом, имеем 8 наборов, по 3 входные комбинации в каждом:
110-{000,111}-{001, 010, 011, 100}.
Ответ: Минимальное количество входных комбинаций равно 3. Всего 8 наборов: 110-{000,111}-{001, 010, 011, 100}.

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 `1B,A1,7F,2B,40` (но неизвестно какому числу какой именно байт соответствует). Найдите d, если $n = 54811, y = 5759$. *Указание*: фигурирующие в задаче числа представимы в виде двух байтов, например $54811 = 13\cdot16^3 + 6\cdot16^2 + 1\cdot16^1 + 11\cdot16^0 =$ `D6 1B` (см. таблицу); `1B` – младший байт числа 54811.

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

Решение: Постараемся определить, какой именно из данных в задаче байтов `1B,A1,7F,2B,40` – младший байт числа p. Байт `1B` – это байт n; `7F` – это байт сообщения y, так как можно подсчитать, что $5759 = 22 \cdot 16^2 + 7 \cdot 16 + 15$; `40` также не годится, поскольку число p нечетно. Таким обзом, младший байт p – это или `A1`, или `2B`.
Заметим, что или у числа p, или у числа q старший байт равен `00`. Действительно, если это не так, то каждое из этих чисел было бы больше, чем 256, а их произведение превосходило $n = 54811$. Предположим, что `00` – старший байт числа p. Тогда или $p = 00\ \ 2B = 43$, что невозможно, поскольку n на 43 не делится, или $p = 00\ \ A1 = 161$, что также невозможно, так как p – простое, но 161 делится на 7.
Итак, установили, что старший байт q равен `00`, а младший байт p – это или `A1`, или `2B`. Найдем теперь число q. (Зная q, мы найдем $p = n/q$, а затем, решив уравнение $r_{(p-1)(q-1)}(3d) = 1$, получим искомое d.)
Пусть $p = p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0$ и $q = q_1 \cdot 16^1 + q_0 \cdot 16^0$. Так как

$$n = p \cdot q = (p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0) \cdot (q_1 \cdot 16^1 + q_0 \cdot 16^0),$$

то

$$r_{16}(n) = r_{16}(p_0 q_0),$$
$$r_{16}\left(\frac{n - p_0 q_0}{16}\right) = r_{16}(p_1 q_0 + p_0 q_1). \qquad (1)$$

Пусть $p_0 = 1, p_1 = 10$. Далее $r_{16}(n) = 11 = r_{16}(1 \cdot q_0) \Longrightarrow q_0 = 11$. Из второй формулы (1) находим $r_{16}(p_1 q_0 + p_0 q_1) = 1 \Longrightarrow q_1 = 3$. В итоге $q = 59 \Rightarrow p = 929 \Rightarrow (p-1)(q-1) = 53824$. Из уравнения $r_{(p-1)(q-1)}(3d) = 1$ следует, что $d = \frac{1 + t \cdot (p-1)(q-1)}{3}$. Здесь натуральное число t не превосходит 3, так как, по условию, число d представимо в виде двух байтов, то есть $d \leq 65535$. Непосредственной проверкой убеждаемся, что числитель делится нацело на 3 при $t = 2 \Rightarrow d = 35883$.
В случае, когда младший байт p – это `2B`, ответ получен быть не может, так как n не поделится на q нацело.
Ответ: $d = 35883$.

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 $\boldsymbol{x^{(2)}} = (x_1^{(2)}, \ldots, x_8^{(2)})$ по аналогичным формулам: $x_1^{(2)} = x_2^{(1)} \oplus k_2, \ldots$ 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 $\boldsymbol{x^{out}} = (0,1,0,1,0,0,1,1)$, а байт $\boldsymbol{x^{in}} = (1,1,1,1,1,1,1,1)$ – в байт $\boldsymbol{x^{out}} = (1,1,1,0,0,0,0,0)$.
Решение: Обозначим $\boldsymbol{x^{in}} = \boldsymbol{x^{(0)}}$. На i-том такте выполняется преобразование $\boldsymbol{x^{(i)}} = \boldsymbol{f_i}(\boldsymbol{x^{(i-1)}})$, которое в покомпонентной записи выглядит, согласно условию, следующим образом:

$$x_1^{(i)} = x_2^{(i-1)} \oplus k_i, x_2^{(i)} = x_3^{(i-1)}, x_3^{(i)} = x_4^{(i-1)} \oplus k_i, x_4^{(i)} = x_5^{(i-1)}, x_5^{(i)} = x_6^{(i-1)} \oplus k_i, x_6^{(i)} = x_7^{(i-1)},\ x_7^{(i)} = x_8^{(i-1)} \oplus k_i, x_8^{(i)} = x_2^{(i-1)} x_7^{(i-1)} \oplus x_1^{(i-1)}.$$

Будем искать такой ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, чтобы пока только для первой пары $\boldsymbol{x^{(0)}}$, $\boldsymbol{x^{(8)}}$ (то есть для $\boldsymbol{x^{(0)}} = (1,0,1,0,1,0,1,0)$ и $\boldsymbol{x^{(8)}} = (0,1,0,1,0,0,1,1)$) выполнялось требуемое:

$$\boldsymbol{x^{(8)}} = \boldsymbol{f_8}\left(\boldsymbol{f_7}\left(\ldots \boldsymbol{f_1}(\boldsymbol{x^{(0)}})\right)\right). \qquad (1)$$

Несложно проверить, что отображение $\boldsymbol{x^{(i-1)}} = \boldsymbol{g_i}(\boldsymbol{x^{(i)}})$, покомпонентная запись которого имеет вид

$$x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = x_6^{(i)},\ x_8^{(i-1)} = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}\left(x_1^{(i)} \oplus k_i\right),$$

является обратным к $\boldsymbol{x^{(i)}} = \boldsymbol{f_{i-1}}\left(\boldsymbol{x^{(i-1)}}\right)$. (Эти формулы обращения следуют из элементарных соображений типа $a = b \oplus c \Leftrightarrow b = a \oplus c$, поэтому выражение для $x_1^{(i-1)}$ естественно получить в последнюю очередь, когда остальные $x_j^{(i-1)}$ уже найдены.) Уравнение (1) эквивалентно уравнению $\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}(\boldsymbol{x^{(0)}})\right)\right)\right) = \boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}(\boldsymbol{x^{(8)}})\right)\right)\right)$**.** Последнее решается полным перебором "половинок" ключа: мы вычисляем правую часть при всевозможных значениях (k_5, k_6, k_7, k_8) (16 вариантов), а затем левую часть для всех (k_1, k_2, k_3, k_4) (также 16 вариантов). Те "половинки", при которых левая и правая части окажутся равными, дадут искомый ключ. Результаты вычислений представлены в таблице.

k_1, k_2, k_3, k_4	$\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}(\boldsymbol{x}^{(\mathbf{0})})\right)\right)\right)$	k_5, k_6, k_7, k_8	$\boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}(\boldsymbol{x}^{(\mathbf{8})})\right)\right)\right)$
0 0 0 0	1 0 1 0 1 0 1 0	0 0 0 0	0 1 1 1 0 1 0 1
0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 1	0 1 1 1 1 1 1 1
0 0 1 0	1 1 1 1 1 1 1 0	0 0 1 0	0 1 1 0 0 0 0 0
0 0 1 1	0 1 0 1 0 1 0 0	0 0 1 1	0 1 0 0 1 0 1 0
0 1 0 0	0 0 0 0 0 0 0 0	0 1 0 0	1 0 0 1 1 1 1 1
0 1 0 1	1 0 1 0 1 0 1 0	0 1 0 1	0 0 0 1 0 1 0 1
0 1 1 0	0 1 0 1 0 1 0 1	0 1 1 0	0 1 0 0 1 0 1 0
0 1 1 1	1 1 1 1 1 1 1 1	0 1 1 1	0 1 1 0 0 0 0 0
1 0 0 0	1 1 1 1 1 0 0 1	1 0 0 0	0 0 1 0 0 0 0 0
1 0 0 1	0 1 0 1 0 0 1 1	1 0 0 1	1 0 1 0 1 0 1 0
1 0 1 0	1 0 1 0 1 1 0 1	1 0 1 0	0 0 1 1 0 1 0 1
1 0 1 1	0 0 0 0 0 1 1 1	1 0 1 1	1 0 0 1 1 1 1 1
1 1 0 0	0 1 0 1 0 0 0 1	1 1 0 0	0 1 0 0 1 0 1 0
1 1 0 1	1 1 1 1 1 0 1 1	1 1 0 1	0 1 0 0 0 0 0 0
1 1 1 0	0 0 0 0 0 1 0 0	1 1 1 0	1 0 0 1 1 1 1 1
1 1 1 1	1 0 1 0 1 1 1 0	1 1 1 1	0 0 1 1 0 1 0 1

Имеется, таким образом, два ключа, $\boldsymbol{k_1} = (0, 0, 0, 0, 1, 0, 0, 1)$ и $\boldsymbol{k_2} = (0, 1, 0, 1, 1, 0, 0, 1)$, на которых для первой пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ выполняется (1). Непосредственной проверкой убеждаемся, что на ключе $\boldsymbol{k_2}$ для второй пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ равенство (1) также выполняется, а на ключе $\boldsymbol{k_1}$ – нет.

Ответ: $0, 1, 0, 1, 1, 0, 0, 1$.

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.

Решение: По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	4	6	8	10	12	14	16	18	17	15	13	11	9	7	5	3	1

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте:
1→2→4→8→16→5→10→17→3→6→12→13→11→15→7→14→9→18→**1**→…
То есть, после того как буквы переставили 18 раз, первая буква снова оказалась на первом месте. При этом она побывала на всех местах от 1 до 18. Очевидно поэтому, что и остальные буквы сообщения, также займут исходное положение на 18-м шаге.
Всего текст был преобразован 74 раза, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).
Ответ: ТЕОРИЯ ВЕРОЯТНОСТЕЙ.

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

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

КлючЮры

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

Решение: Пусть $L = (L_1, L_2, \dots, L_8)$, $M = (M_1, M_2, \dots, M_8)$ – латинские прямоугольники замка и путешественника соответственно, $L_i, M_i, i \in \{1, \dots, 8\}$, – столбцы этих прямоугольников. Построим множества $A_1, A_2, \dots, A_8$, где $A_i, i \in \{1, \dots, 8\}$, – множество тех и только тех чисел от 1 до 8, которые не встречаются в столбцах L_i и M_i. Например, если M – это ключ Кати, то $A_1 = \{2,7\}$, так как каждым из этих чисел (и только ими) можно дополнить первый столбец прямоугольников L и M. Тогда общее продолжение латинских прямоугольников L и M существует в том и только том случае, когда семейство множеств $A_1, A_2, \dots, A_8$ обладает *системой различных представителей*, т.е. существует такой упорядоченный набор чисел $(a_1, a_2, \dots, a_8)$, что $a_i \neq a_j$ при $i \neq j, a_i \in A_i$. Каждая такая система – это дополнительная строка, которая может быть дописана и к прямоугольнику путешественника, и к прямоугольнику замка. По условию замок открывается, только когда такая дополнительная строка единственна.

Дополнительные строки для ключа Кати: {{2,1,3,6,4,5,7,8},{2,5,3,6,4,1,7,8}}.

Дополнительные строки для ключа Юры: {{6,2,1,5,7,3,4,8}}.

Ответ: Ключ Юры правильный.

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 $\boldsymbol{w_1^\sigma} = (\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})), \dots, \boldsymbol{w_k^\sigma} = (\sigma(w_{k1}), \sigma(w_{k2}), \dots, \sigma(w_{kn}))$ также будут различны.

Решение: Докажем утверждение индукцией по k (числу наборов).

- Для одного набора $\mathbf{w_1}$ утверждение очевидно.
- Предположим, что утверждение верно для любых $k-1$ различных наборов ($k > 1$).
- Докажем на основании этого предположения, что утверждение справедливо и для произвольных k различных наборов $\boldsymbol{w_1} = (w_{11}, w_{12}, \dots, w_{1n}), \dots, \boldsymbol{w_k} = (w_{k1}, w_{k2}, \dots, w_{kn})$. По предположению индукции для первых $k-1$ наборов $\boldsymbol{w_1}, \dots, \boldsymbol{w_{k-1}}$ существует такое отображение $\sigma: \mathbb{N} \to \{1,2,\dots,k-1\}$, что наборы $\boldsymbol{w_1^\sigma} = (\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})), \dots, \boldsymbol{w_{k-1}^\sigma} = \left(\sigma(w_{k-1,1}), \sigma(w_{k-1,2}), \dots, \sigma(w_{k-1,n})\right)$ различны. Если при этом и все k наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}, \boldsymbol{w_k^\sigma}$ оказались различными, то утверждение доказано. Если же это не так, то набор $\boldsymbol{w_k^\sigma}$ совпадает с одним из наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$, причем *ровно с одним*, так как, по предположению, эти $k-1$ наборов различны. Не ограничивая общности, можно считать, что $\boldsymbol{w_1^\sigma} = \boldsymbol{w_k^\sigma}$. Поскольку исходные наборы $\boldsymbol{w_1}$ и $\boldsymbol{w_k}$ различны, то $w_{1i} \neq w_{ki}$ для некоторого i, и при этом $\sigma(w_{1i}) = \sigma(w_{ki})$. Переопределим тогда отображение σ, положив $\sigma(w_{ki}) = k$. Для так переопределенного σ наборы $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$ по-прежнему останутся различными, и при этом набор $\boldsymbol{w_k^\sigma}$ будет отличен от них. Утверждение доказано.

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

Решение: Если, например, подать на вход 000, то на выходе мы получим 0, если устройство работает правильно или имеется неисправность Н1 или Н2, либо 1, если имеется неисправность Н3. Значит, вход 000 позволяет *различить*, скажем, режим ПР и Н3, но не позволяет отличить Н1 от Н2. Составим таблицу, где для каждого входа укажем, какие пары режимов этот вход различить может (символ 1), а какие – нет (символ 0).

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

Чтобы определить режим работы устройства, нужно подать на вход такие комбинации, что им соответствующие строки покрывают единицами все столбцы (то есть в каждом столбце есть хотя бы одна единица, стоящая в одной из этих строк). Сразу можно заметить, что входных комбинаций потребуется по крайней мере 3, так как никакие 2 строки не покрывают все столбцы.

Вход 010 покрывает 4 столбца. Непокрытыми остаются столбец ПР и Н2 (покрывается входами 001 и 101) и столбец Н1 и Н3 (покрывается входами 000, 011,100, 110).

Таким образом, имеем 8 наборов, по 3 входные комбинации в каждом:

010-{001,101}-{000, 011,100, 110}.

Ответ: Минимальное количество входных комбинаций равно 3. Всего 8 наборов: 010-{001,101}-{000, 011,100, 110}.

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

Решение: Постараемся определить, какой именно из данных в задаче байтов `85,00,C1,F5,AB` – младший байт числа p. Байт `F5` – это байт n; `85` – это байт сообщения y, так как можно подсчитать, что $59781 = 233 \cdot 16^2 + 8 \cdot 16 + 5$; `00` также не годится, поскольку число p нечетно. Таким обзом, младший байт p – это или `C1`, или `AB`.
Заметим, что или у числа p, или у числа q старший байт равен `00`. Действительно, если это не так, то каждое из этих чисел было бы больше, чем 256, а их произведение превосходило $n = 64501$. Предположим, что `00` – старший байт числа p. Тогда или $p = 00\ \mathrm{C1} = 193$, что невозможно, поскольку n на 193 не делится, или $p = 00\ \mathrm{AB} = 171$, что также невозможно, так как p – простое, но 171 делится на 3.
Итак, установили, что старший байт q равен `00`, а младший байт p – это или `C1`, или `AB`. Найдем теперь число q. (Зная q, мы найдем $p = n/q$, а затем, решив уравнение $r_{(p-1)(q-1)}(3d) = 1$, получим искомое d.)
Пусть $p = p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0$ и $q = q_1 \cdot 16^1 + q_0 \cdot 16^0$. Так как

$$n = p \cdot q = (p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0) \cdot (q_1 \cdot 16^1 + q_0 \cdot 16^0),$$

то

$$r_{16}(n) = r_{16}(p_0 q_0),$$
$$r_{16}\left(\frac{n - p_0 q_0}{16}\right) = r_{16}(p_1 q_0 + p_0 q_1). \qquad (1)$$

Пусть $p_0 = 1, p_1 = 12$. Далее $r_{16}(n) = 5 = r_{16}(1 \cdot q_0) \Longrightarrow q_0 = 5$. Из второй формулы (1) находим $r_{16}(p_1 q_0 + p_0 q_1) = 15 \Longrightarrow q_1 = 3$. В итоге $q = 53 \Rightarrow p = 1217 \Rightarrow (p-1)(q-1) = 63232$. Из уравнения $r_{(p-1)(q-1)}(3d) = 1$ следует, что $d = \frac{1 + t \cdot (p-1)(q-1)}{3}$. Здесь натуральное число t не превосходит 3, так как, по условию, число d представимо в виде двух байтов, то есть $d \le 65535$. Непосредственной проверкой убеждаемся, что числитель делится нацело на 3 при $t = 2 \Rightarrow d = 42155$.
В случае, когда младший байт p – это `AB`, ответ получен быть не может, так как n не поделится на q нацело.
Ответ: $d = 42155$.

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 $\boldsymbol{x^{out}} = (0,0,1,1,0,0,0,0)$.
Решение: Обозначим $\boldsymbol{x^{in}} = \boldsymbol{x^{(0)}}$. На i-том такте выполняется преобразование $\boldsymbol{x^{(i)}} = \boldsymbol{f_i}(\boldsymbol{x^{(i-1)}})$, которое в покомпонентной записи выглядит, согласно условию, следующим образом:

$$x_1^{(i)} = x_2^{(i-1)} \oplus k_i, x_2^{(i)} = x_3^{(i-1)}, x_3^{(i)} = x_4^{(i-1)} \oplus k_i, x_4^{(i)} = x_5^{(i-1)}, x_5^{(i)} = x_6^{(i-1)} \oplus k_i, x_6^{(i)} = x_7^{(i-1)},\ x_7^{(i)} = x_8^{(i-1)} \oplus k_i, x_8^{(i)} = x_2^{(i-1)} x_7^{(i-1)} \oplus x_1^{(i-1)}.$$

Будем искать такой ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, чтобы пока только для первой пары $\boldsymbol{x^{(0)}}$, $\boldsymbol{x^{(8)}}$ (то есть для $\boldsymbol{x^{(0)}} = (1,0,1,0,1,0,1,0)$ и $\boldsymbol{x^{(8)}} = (1,0,0,0,1,0,1,1)$) выполнялось требуемое:

$$\boldsymbol{x^{(8)}} = \boldsymbol{f_8}\left(\boldsymbol{f_7}\left(\dots \boldsymbol{f_1}(\boldsymbol{x^{(0)}})\right)\right). \qquad (1)$$

Несложно проверить, что отображение $\boldsymbol{x^{(i-1)}} = \boldsymbol{g_i}(\boldsymbol{x^{(i)}})$, покомпонентная запись которого имеет вид

$$x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = x_6^{(i)},\ x_8^{(i-1)} = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}\left(x_1^{(i)} \oplus k_i\right),$$

является обратным к $\boldsymbol{x^{(i)}} = \boldsymbol{f_{i-1}}(\boldsymbol{x^{(i-1)}})$. (Эти формулы обращения следуют из элементарных соображений типа $a = b \oplus c \Leftrightarrow b = a \oplus c$, поэтому выражение для $x_1^{(i-1)}$ естественно получить в последнюю очередь, когда остальные $x_j^{(i-1)}$ уже найдены.) Уравнение (1) эквивалентно уравнению $\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}(\boldsymbol{x^{(0)}})\right)\right)\right) = \boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}(\boldsymbol{x^{(8)}})\right)\right)\right)$**.** Последнее решается полным перебором "половинок" ключа: мы вычисляем правую часть при всевозможных значениях (k_5, k_6, k_7, k_8) (16 вариантов), а затем левую часть для всех (k_1, k_2, k_3, k_4) (также 16 вариантов). Те "половинки", при которых левая и правая части окажутся равными, дадут искомый ключ. Результаты вычислений представлены в таблице.

k_1, k_2, k_3, k_4	$\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}\left(\boldsymbol{x}^{(\mathbf{0})}\right)\right)\right)\right)$	k_5, k_6, k_7, k_8	$\boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}\left(\boldsymbol{x}^{(\mathbf{8})}\right)\right)\right)\right)$
0 0 0 0	1 0 1 0 1 0 1 0	0 0 0 0	1 0 0 1 1 0 0 0
0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 1	0 0 0 1 0 0 1 0
0 0 1 0	1 1 1 1 1 1 1 0	0 0 1 0	1 0 1 0 1 1 0 1
0 0 1 1	0 1 0 1 0 1 0 0	0 0 1 1	1 1 0 0 0 1 1 1
0 1 0 0	0 0 0 0 0 0 0 0	0 1 0 0	0 0 1 1 0 0 1 0
0 1 0 1	1 0 1 0 1 0 1 0	0 1 0 1	1 0 1 1 1 0 0 0
0 1 1 0	0 1 0 1 0 1 0 1	0 1 1 0	1 1 0 0 0 1 1 1
0 1 1 1	1 1 1 1 1 1 1 1	0 1 1 1	1 0 1 0 1 1 0 1
1 0 0 0	1 1 1 1 1 0 0 1	1 0 0 0	1 1 0 0 1 1 0 1
1 0 0 1	0 1 0 1 0 0 1 1	1 0 0 1	1 1 0 0 0 1 1 1
1 0 1 0	1 0 1 0 1 1 0 1	1 0 1 0	1 1 1 1 1 0 0 0
1 0 1 1	0 0 0 0 0 1 1 1	1 0 1 1	0 0 0 1 0 0 1 0
1 1 0 0	0 1 0 1 0 0 0 1	1 1 0 0	1 1 1 0 0 1 1 1
1 1 0 1	1 1 1 1 1 0 1 1	1 1 0 1	1 1 1 0 1 1 0 1
1 1 1 0	0 0 0 0 0 1 0 0	1 1 1 0	0 0 0 1 0 0 1 0
1 1 1 1	1 0 1 0 1 1 1 0	1 1 1 1	1 1 1 1 1 0 0 0

Имеется, таким образом, два ключа, $\boldsymbol{k_1} = (1, 0, 1, 0, 0, 0, 1, 0)$ и $\boldsymbol{k_2} = (1, 0, 1, 0, 0, 1, 1, 1)$, на которых для первой пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ выполняется (1). Непосредственной проверкой убеждаемся, что на ключе $\boldsymbol{k_2}$ для второй пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ равенство (1) также выполняется, а на ключе $\boldsymbol{k_1}$ – нет.

Ответ: $1, 0, 1, 0, 0, 1, 1, 1$.

5 вариант

1. В тексте, состоящем из 24 букв и записанном без пробелов, буквы переставлены по следующему правилу: 24-я буква поставлена на 1-е место, 1-я буква – на 2-е место, 23-я – на 3-е место, 2-я – на 4-е и так далее (в конце 13-я буква поставлена на 23-е место, 12-я – на 24-е). Затем такую же процедуру повторили ещё 85 раз. В результате получилось **КААМСКЯАЕИСТЧТТЕИСАМТИТА.** Найдите исходный текст.

Решение: По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	4	6	8	10	12	14	16	18	20	22	24	23	21	19	17	15	13	11	9	7	5	3	1

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте:
1→2→4→8→16→17→15→19→11→22→5→10→20→9→18→13→23→3→6→12→24→**1**→ …
То есть, после того как буквы переставили 21 раз, первая буква снова оказалась на первом месте. Попутно получили еще последовательность промежуточных положений первой буквы, а именно: 2,4,...,24. Очевидно, что буквы, стоявшие на этих местах, также займут исходное положение на 21-м шаге. Оставшиеся три буквы, стоящие на местах 7, 14, 21, перемещаются по циклу длины 3: **7**→14→21→**7**→…
Следовательно, после 21 преобразования текст будет совпадать с исходным.
Всего текст был преобразован 86 раз, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).
Ответ: МАТЕМАТИЧЕСКАЯ СТАТИСТИКА.

2. Чтобы попасть в Криптоландию, необходимо пройти через ворота с электронным замком, предъявив правильный ключ. В микросхеме замка хранится таблица размерами 3х8 (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 4х8. 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 4х8 и 5х8, 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
$$\begin{pmatrix} 5 & 4 & 8 & 6 & 7 & 2 & 3 & 1 \\ 6 & 3 & 7 & 4 & 1 & 8 & 5 & 2 \\ 8 & 6 & 5 & 1 & 4 & 7 & 2 & 3 \end{pmatrix}$$

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

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

Решение: Пусть $L = (L_1, L_2, \dots, L_8)$, $M = (M_1, M_2, \dots, M_8)$ – латинские прямоугольники замка и путешественника соответственно, $L_i, M_i, i \in \{1, \dots, 8\}$, – столбцы этих прямоугольников. Построим множества $A_1, A_2, \dots, A_8$, где $A_i, i \in \{1, \dots, 8\}$, – множество тех и только тех чисел от 1 до 8, которые не встречаются в столбцах L_i и M_i. Например, если M – это ключ Кати, то $A_1 = \{2,1\}$, так как каждым из этих чисел (и только ими) можно дополнить первый столбец прямоугольников L и M. Тогда общее продолжение латинских прямоугольников L и M существует в том и только том случае, когда семейство множеств $A_1, A_2, \dots, A_8$ обладает *системой различных представителей*, т.е. существует такой упорядоченный набор чисел $(a_1, a_2, \dots, a_8)$, что $a_i \neq a_j$ при $i \neq j, a_i \in A_i$. Каждая такая система – это дополнительная строка, которая может быть дописана и к прямоугольнику путешественника, и к прямоугольнику замка. По условию замок открывается, только когда такая дополнительная строка единственна.

Дополнительные строки для ключа Кати: {{2,7,1,3,5,6,8,4}}.

Дополнительные строки для ключа Юры: {{1,2,3,7,6,4,8,5},{4,1,2,7,6,3,8,5},{4,2,3,7,6,1,8,5}}.

Ответ: Ключ Кати правильный.

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 $\boldsymbol{w_1^\sigma} = \left(\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})\right), \dots, \boldsymbol{w_k^\sigma} = \left(\sigma(w_{k1}), \sigma(w_{k2}), \dots, \sigma(w_{kn})\right)$ также будут различны.

Решение: Докажем утверждение индукцией по k (числу наборов).

- Для одного набора $\mathbf{w_1}$ утверждение очевидно.
- Предположим, что утверждение верно для любых $k-1$ различных наборов ($k > 1$).
- Докажем на основании этого предположения, что утверждение справедливо и для произвольных k различных наборов $\boldsymbol{w_1} = (w_{11}, w_{12}, \dots, w_{1n}), \dots, \boldsymbol{w_k} = (w_{k1}, w_{k2}, \dots, w_{kn})$. По предположению индукции для первых $k-1$ наборов $\boldsymbol{w_1}, \dots, \boldsymbol{w_{k-1}}$ существует такое отображение $\sigma: \mathbb{N} \to \{1,2,\dots,k-1\}$, что наборы $\boldsymbol{w_1^\sigma} = \left(\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})\right), \dots, \boldsymbol{w_{k-1}^\sigma} = \left(\sigma(w_{k-1,1}), \sigma(w_{k-1,2}), \dots, \sigma(w_{k-1,n})\right)$ различны. Если при этом и все k наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}, \boldsymbol{w_k^\sigma}$ оказались различными, то утверждение доказано. Если же это не так, то набор $\boldsymbol{w_k^\sigma}$ совпадает с одним из наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$, причем *ровно с одним*, так как, по предположению, эти $k-1$ наборов различны. Не ограничивая общности, можно считать, что $\boldsymbol{w_1^\sigma} = \boldsymbol{w_k^\sigma}$. Поскольку исходные наборы $\boldsymbol{w_1}$ и $\boldsymbol{w_k}$ различны, то $w_{1i} \neq w_{ki}$ для некоторого i, и при этом $\sigma(w_{1i}) = \sigma(w_{ki})$. Переопределим тогда отображение σ, положив $\sigma(w_{ki}) = k$. Для так переопределенного σ наборы $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$ по-прежнему останутся различными, и при этом набор $\boldsymbol{w_k^\sigma}$ будет отличен от них. Утверждение доказано.

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 110) 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	1	0	0	0
001	0	1	0	0
010	1	0	1	1
011	1	1	1	0
100	1	1	1	0
101	1	1	1	1
110	0	1	0	1
111	0	0	1	0

Решение: Если, например, подать на вход 000, то на выходе мы получим 0, если имеется неисправность Н1,Н2 или Н3, либо 1, если устройство работает правильно. Значит, вход 000 позволяет *различить*, скажем, режим ПР и Н3, но не позволяет отличить Н1 от Н2. Составим таблицу, где для каждого входа укажем, какие пары режимов этот вход различить может (символ 1), а какие – нет (символ 0).

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

Чтобы определить режим работы устройства, нужно подать на вход такие комбинации, что им соответствующие строки покрывают единицами все столбцы (то есть в каждом столбце есть хотя бы одна единица, стоящая в одной из этих строк). Сразу можно заметить, что входных комбинаций потребуется по крайней мере 3, так как никакие 2 строки не покрывают все столбцы.
Вход 110 покрывает 4 столбца. Непокрытыми остаются столбец ПР и Н2 (покрывается входами 000 и 111) и столбец Н1 и Н3 (покрывается входами 001, 010, 011, 100).
Таким образом, имеем 8 наборов, по 3 входные комбинации в каждом:
110-{000,111}-{001, 010, 011, 100}.
Ответ: Минимальное количество входных комбинаций равно 3. Всего 8 наборов: 110-{000,111}-{001, 010, 011, 100}.

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 `03,7B,50,8B,F5` (но неизвестно какому числу какой именно байт соответствует). Найдите d, если $n = 52603, y = 49141$. *Указание*: фигурирующие в задаче числа представимы в виде двух байтов, например $52603 = 12 \cdot 16^3 + 13 \cdot 16^2 + 7 \cdot 16^1 + 11 \cdot 16^0 =$ `CD 7B` (см. таблицу); `7B` – младший байт числа 52603.

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

Решение: Постараемся определить, какой именно из данных в задаче байтов 03,7B,50,8B,F5 – младший байт числа p. Байт 7B – это байт n; F5 – это байт сообщения y, так как можно подсчитать, что $49141 = 191 \cdot 16^2 + 15 \cdot 16 + 5$; 50 также не годится, поскольку число p нечетно. Таким обзом, младший байт p – это или 03, или 8B.

Заметим, что или у числа p, или у числа q старший байт равен 00. Действительно, если это не так, то каждое из этих чисел было бы больше, чем 256, а их произведение превосходило $n = 52603$. Предположим, что 00 – старший байт числа p. Тогда или $p = 00\ 03 = 3$, или $p = 00\ 8B = 139$, что невозможно, поскольку n не делится ни на 3, ни на 139.

Итак, установили, что старший байт q равен 00, а младший байт p – это или 03, или 8B. Найдем теперь число q. (Зная q, мы найдем $p = n/q$, а затем, решив уравнение $r_{(p-1)(q-1)}(3d) = 1$, получим искомое d.) Пусть $p = p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0$ и $q = q_1 \cdot 16^1 + q_0 \cdot 16^0$. Так как

$$n = p \cdot q = (p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0) \cdot (q_1 \cdot 16^1 + q_0 \cdot 16^0),$$

то

$$\begin{gathered} r_{16}(n) = r_{16}(p_0 q_0), \\ r_{16}\left(\frac{n - p_0 q_0}{16}\right) = r_{16}(p_1 q_0 + p_0 q_1). \end{gathered} \qquad (1)$$

Пусть $p_0 = 3, p_1 = 0$. Далее $r_{16}(n) = 11 = r_{16}(3 \cdot q_0) \Longrightarrow q_0 = 9$. Из второй формулы (1) находим $r_{16}(p_1 q_0 + p_0 q_1) = 6 \Longrightarrow q_1 = 2$. В итоге $q = 41 \Rightarrow p = 1283 \Rightarrow (p-1)(q-1) = 51280$. Из уравнения $r_{(p-1)(q-1)}(3d) = 1$ следует, что $d = \frac{1+t\cdot(p-1)(q-1)}{3}$. Здесь натуральное число t не превосходит 3, так как, по условию, число d представимо в виде двух байтов, то есть $d \le 65535$. Непосредственной проверкой убеждаемся, что числитель делится нацело на 3 при $t = 2 \Rightarrow d = 34187$.

В случае, когда младший байт p – это 8B, ответ получен быть не может, так как n не поделится на q нацело.

Ответ: $d = 34187$.

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 $\boldsymbol{x^{out}} = (1,1,1,1,1,0,1,1)$, а байт $\boldsymbol{x^{in}} = (1,1,1,1,1,1,1,1)$– в байт $\boldsymbol{x^{out}} = (0,1,0,0,1,0,1,0)$.

Решение: Обозначим $\boldsymbol{x^{in}} = \boldsymbol{x^{(0)}}$. На i-том такте выполняется преобразование $\boldsymbol{x^{(i)}} = \boldsymbol{f_i}(\boldsymbol{x^{(i-1)}})$, которое в покомпонентной записи выглядит, согласно условию, следующим образом:

$$x_1^{(i)} = x_2^{(i-1)} \oplus k_i, x_2^{(i)} = x_3^{(i-1)}, x_3^{(i)} = x_4^{(i-1)} \oplus k_i, x_4^{(i)} = x_5^{(i-1)}, x_5^{(i)} = x_6^{(i-1)} \oplus k_i, x_6^{(i)} = x_7^{(i-1)},\ x_7^{(i)} = x_8^{(i-1)} \oplus k_i, x_8^{(i)} = x_2^{(i-1)} x_7^{(i-1)} \oplus x_1^{(i-1)}.$$

Будем искать такой ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, чтобы пока только для первой пары $\boldsymbol{x^{(0)}}, \boldsymbol{x^{(8)}}$ (то есть для $\boldsymbol{x^{(0)}} = (1,0,1,0,1,0,1,0)$ и $\boldsymbol{x^{(8)}} = (1,1,1,1,1,0,1,1)$) выполнялось требуемое:

$$\boldsymbol{x^{(8)}} = \boldsymbol{f_8}\left(\boldsymbol{f_7}\left(\dots \boldsymbol{f_1}\left(\boldsymbol{x^{(0)}}\right)\right)\right). \qquad (1)$$

Несложно проверить, что отображение $\boldsymbol{x^{(i-1)}} = \boldsymbol{g_i}(\boldsymbol{x^{(i)}})$, покомпонентная запись которого имеет вид

$$x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = x_6^{(i)},\ x_8^{(i-1)} = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}\left(x_1^{(i)} \oplus k_i\right),$$

является обратным к $\boldsymbol{x^{(i)}} = \boldsymbol{f_{i-1}}\left(\boldsymbol{x^{(i-1)}}\right)$. (Эти формулы обращения следуют из элементарных соображений типа $a = b \oplus c \Leftrightarrow b = a \oplus c$, поэтому выражение для $x_1^{(i-1)}$ естественно получить в последнюю очередь, когда остальные $x_j^{(i-1)}$ уже найдены.) Уравнение (1) эквивалентно уравнению $\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}\left(\boldsymbol{x^{(0)}}\right)\right)\right)\right) = \boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}\left(\boldsymbol{x^{(8)}}\right)\right)\right)\right)$. Последнее решается полным перебором "половинок" ключа: мы вычисляем правую часть при всевозможных значениях (k_5, k_6, k_7, k_8) (16 вариантов), а затем левую часть для всех (k_1, k_2, k_3, k_4) (также 16 вариантов). Те "половинки", при которых левая и правая части окажутся равными, дадут искомый ключ. Результаты вычислений представлены в таблице.

k_1, k_2, k_3, k_4	$\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}\left(\boldsymbol{x}^{(\mathbf{0})}\right)\right)\right)\right)$	k_5, k_6, k_7, k_8	$\boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}\left(\boldsymbol{x}^{(\mathbf{8})}\right)\right)\right)\right)$
$\boxed{0\,0\,0\,0}$	$\boxed{1\,0\,1\,0\,1\,0\,1\,0}$	0 0 0 0	1 0 0 1 1 1 1 1
0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 1	0 0 0 1 0 1 0 1
0 0 1 0	1 1 1 1 1 1 1 0	0 0 1 0	0 1 1 0 1 0 1 0
0 0 1 1	0 1 0 1 0 1 0 0	0 0 1 1	0 1 0 0 0 0 0 0
0 1 0 0	0 0 0 0 0 0 0 0	0 1 0 0	0 1 1 1 0 1 0 1
$\boxed{0\,1\,0\,1}$	$\boxed{1\,0\,1\,0\,1\,0\,1\,0}$	0 1 0 1	0 1 1 1 1 1 1 1
0 1 1 0	0 1 0 1 0 1 0 1	0 1 1 0	0 1 0 0 0 0 0 0
0 1 1 1	1 1 1 1 1 1 1 1	0 1 1 1	0 1 1 0 1 0 1 0
1 0 0 0	1 1 1 1 1 0 0 1	1 0 0 0	0 1 0 0 1 0 1 0
1 0 0 1	0 1 0 1 0 0 1 1	1 0 0 1	0 1 0 0 0 0 0 0
1 0 1 0	1 0 1 0 1 1 0 1	1 0 1 0	1 0 1 1 1 1 1 1
1 0 1 1	0 0 0 0 0 1 1 1	1 0 1 1	0 0 0 1 0 1 0 1
1 1 0 0	0 1 0 1 0 0 0 1	1 1 0 0	0 0 1 0 0 0 0 0
1 1 0 1	1 1 1 1 1 0 1 1	$\boxed{1\,1\,0\,1}$	$\boxed{1\,0\,1\,0\,1\,0\,1\,0}$
1 1 1 0	0 0 0 0 0 1 0 0	1 1 1 0	0 0 0 1 0 1 0 1
1 1 1 1	1 0 1 0 1 1 1 0	1 1 1 1	1 0 1 1 1 1 1 1

Имеется, таким образом, два ключа, $\boldsymbol{k_1} = (0, 0, 0, 0, 1, 1, 0, 1)$ и $\boldsymbol{k_2} = (0, 1, 0, 1, 1, 1, 0, 1)$, на которых для первой пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ выполняется (1). Непосредственной проверкой убеждаемся, что на ключе $\boldsymbol{k_2}$ для второй пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ равенство (1) также выполняется, а на ключе $\boldsymbol{k_1}$ – нет.

Ответ: $0, 1, 0, 1, 1, 1, 0, 1$.

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

6 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 **ОДРКТОНОАТЫМНЕЙБИМ.** Найдите исходный текст.

Решение: По условию, после одной перестановки положение букв изменяется в соответствии со следующей таблицей:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	4	6	8	10	12	14	16	18	17	15	13	11	9	7	5	3	1

Посмотрим как в результате перестановок меняется положение буквы, стоявшей на первом месте:
1→2→4→8→16→5→10→17→3→6→12→13→11→15→7→14→9→18→**1**→…
То есть, после того как буквы переставили 18 раз, первая буква снова оказалась на первом месте. При этом она побывала на всех местах от 1 до 18. Очевидно поэтому, что и остальные буквы сообщения, также займут исходное положение на 18-м шаге.
Всего текст был преобразован 74 раза, а значит, для получения исходного текста нужно, в соответствии с таблицей, выполнить две "обратные" перестановки букв зашифрованного текста (то есть, 2-я буква зашифрованного текста теперь переставляется на 1-е место, 4-я буква – на 2-е место и т.д.).
Ответ: КОМБИНАТОРНЫЙ МЕТОД.

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

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

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

Решение: Пусть $L = (L_1, L_2, \dots, L_8)$, $M = (M_1, M_2, \dots, M_8)$ – латинские прямоугольники замка и путешественника соответственно, $L_i, M_i, i \in \{1, \dots, 8\}$, – столбцы этих прямоугольников. Построим множества $A_1, A_2, \dots, A_8$, где $A_i, i \in \{1, \dots, 8\}$, – множество тех и только тех чисел от 1 до 8, которые не встречаются в столбцах L_i и M_i. Например, если M – это ключ Кати, то $A_1 = \{3,5,6\}$, так как каждым из этих чисел (и только ими) можно дополнить первый столбец прямоугольников L и M. Тогда общее продолжение латинских прямоугольников L и M существует в том и только том случае, когда семейство множеств $A_1, A_2, \dots, A_8$ обладает *системой различных представителей*, т.е. существует такой упорядоченный набор чисел $(a_1, a_2, \dots, a_8)$, что $a_i \neq a_j$ при $i \neq j, a_i \in A_i$. Каждая такая система – это дополнительная строка, которая может быть дописана и к прямоугольнику путешественника, и к прямоугольнику замка. По условию замок открывается, только когда такая дополнительная строка единственна.

Дополнительные строки для ключа Кати: {{5,6,7,3,4,8,1,2}}.

Дополнительные строки для ключа Юры: {{2,6,3,5,7,1,8,4},{2,6,3,7,4,1,8,5}}.

Ответ: Ключ Кати правильный.

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 $\boldsymbol{w_1^\sigma} = (\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})), \dots, \boldsymbol{w_k^\sigma} = (\sigma(w_{k1}), \sigma(w_{k2}), \dots, \sigma(w_{kn}))$ также будут различны.

Решение: Докажем утверждение индукцией по k (числу наборов).

- Для одного набора $\mathbf{w_1}$ утверждение очевидно.
- Предположим, что утверждение верно для любых $k-1$ различных наборов ($k>1$).
- Докажем на основании этого предположения, что утверждение справедливо и для произвольных k различных наборов $\boldsymbol{w_1} = (w_{11}, w_{12}, \dots, w_{1n}), \dots, \boldsymbol{w_k} = (w_{k1}, w_{k2}, \dots, w_{kn})$. По предположению индукции для первых $k-1$ наборов $\boldsymbol{w_1}, \dots, \boldsymbol{w_{k-1}}$ существует такое отображение $\sigma: \mathbb{N} \to \{1,2,\dots,k-1\}$, что наборы $\boldsymbol{w_1^\sigma} = (\sigma(w_{11}), \sigma(w_{12}), \dots, \sigma(w_{1n})), \dots, \boldsymbol{w_{k-1}^\sigma} = \left(\sigma(w_{k-1,1}), \sigma(w_{k-1,2}), \dots, \sigma(w_{k-1,n})\right)$ различны. Если при этом и все k наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}, \boldsymbol{w_k^\sigma}$ оказались различными, то утверждение доказано. Если же это не так, то набор $\boldsymbol{w_k^\sigma}$ совпадает с одним из наборов $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$, причем *ровно с одним*, так как, по предположению, эти $k-1$ наборов различны. Не ограничивая общности, можно считать, что $\boldsymbol{w_1^\sigma} = \boldsymbol{w_k^\sigma}$. Поскольку исходные наборы $\boldsymbol{w_1}$ и $\boldsymbol{w_k}$ различны, то $w_{1i} \neq w_{ki}$ для некоторого i, и при этом $\sigma(w_{1i}) = \sigma(w_{ki})$. Переопределим тогда отображение σ, положив $\sigma(w_{ki}) = k$. Для так переопределенного σ наборы $\boldsymbol{w_1^\sigma}, \dots, \boldsymbol{w_{k-1}^\sigma}$ по-прежнему останутся различными, и при этом набор $\boldsymbol{w_k^\sigma}$ будет отличен от них. Утверждение доказано.

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 таблицеуказано, 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 однозначноопределить 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	0	0	1	0
010	1	0	1	0
011	0	1	0	0
100	0	0	0	1
101	1	0	0	0
110	1	0	1	1
111	0	0	0	0

Решение: Если, например, подать на вход 000, то на выходе мы получим 0, если устройство работает правильно или имеется неисправность Н1 или Н2, либо 1, если имеется неисправность Н3. Значит, вход 000 позволяет *различить*, скажем, режим ПР и Н3, но не позволяет отличить Н1 от Н2. Составим таблицу, где для каждого входа укажем, какие пары режимов этот вход различить может (символ 1), а какие – нет (символ 0).

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

Чтобы определить режим работы устройства, нужно подать на вход такие комбинации, что им соответствующие строки покрывают единицами все столбцы (то есть в каждом столбце есть хотя бы одна единица, стоящая в одной из этих строк). Сразу можно заметить, что входных комбинаций потребуется по крайней мере 3, так как никакие 2 строки не покрывают все столбцы.
Вход 010 покрывает 4 столбца. Непокрытыми остаются столбец ПР и Н2 (покрывается входами 001 и 101) и столбец Н1 и Н3 (покрывается входами 000, 011,100, 110).
Таким образом, имеем 8 наборов, по 3 входные комбинации в каждом:
010-{001,101}-{000, 011,100, 110}.
Ответ: Минимальное количество входных комбинаций равно 3. Всего 8 наборов: 010-{001,101}-{000, 011,100, 110}.

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 `DF,ED,60,51,EB` (но неизвестно какому числу какой именно байт соответствует). Найдите d, если $n = 63967, y = 60909$. *Указание*: фигурирующие в задаче числа представимы в виде двух байтов, например $63967 = 15 \cdot 16^3 + 9 \cdot 16^2 + 13 \cdot 16^1 + 15 \cdot 16^0 =$ `F9 DF`(см. таблицу); `DF` – младший байт числа 63967.

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

Решение: Постараемся определить, какой именно из данных в задаче байтов `DF,ED,60,51,EB` – младший байт числа p. Байт `DF` – это байт n; `ED` – это байт сообщения y, так как можно подсчитать, что

$60909 = 237 \cdot 16^2 + 14 \cdot 16 + 13$; `60` также не годится, поскольку число p нечетно. Таким обзом, младший байт p – это или `51`, или `EB`.

Заметим, что или у числа p, или у числа q старший байт равен `00`. Действительно, если это не так, то каждое из этих чисел было бы больше, чем 256, а их произведение превосходило $n = 63967$. Предположим, что `00` – старший байт числа p. Тогда или $p = $ `00 51` $= 81$, или $p = $ `00 EB` $= 235$, что невозможно, так как p – простое, но 81 и 235 – составные числа.

Итак, установили, что старший байт q равен `00`, а младший байт p – это или `51`, или `EB`. Найдем теперь число q. (Зная q, мы найдем $p = n/q$, а затем, решив уравнение $r_{(p-1)(q-1)}(3d) = 1$, получим искомое d.)

Пусть $p = p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0$ и $q = q_1 \cdot 16^1 + q_0 \cdot 16^0$. Так как

$$n = p \cdot q = (p_3 \cdot 16^3 + p_2 \cdot 16^2 + p_1 \cdot 16^1 + p_0 \cdot 16^0) \cdot (q_1 \cdot 16^1 + q_0 \cdot 16^0),$$

то

$$r_{16}(n) = r_{16}(p_0 q_0),$$
$$r_{16}\left(\frac{n - p_0 q_0}{16}\right) = r_{16}(p_1 q_0 + p_0 q_1). \qquad (1)$$

Пусть $p_0 = 1, p_1 = 5$. Далее $r_{16}(n) = 15 = r_{16}(1 \cdot q_0) \Longrightarrow q_0 = 15$. Из второй формулы (1) находим $r_{16}(p_1 q_0 + p_0 q_1) = 13 \Longrightarrow q_1 = 2$. В итоге $q = 47 \Rightarrow p = 1361 \Rightarrow (p-1)(q-1) = 62560$. Из уравнения $r_{(p-1)(q-1)}(3d) = 1$ следует, что $d = \frac{1 + t \cdot (p-1)(q-1)}{3}$. Здесь натуральное число t не превосходит 3, так как, по условию, число d представимо в виде двух байтов, то есть $d \leq 65535$. Непосредственной проверкой убеждаемся, что числитель делится нацело на 3 при $t = 2 \Rightarrow d = 41707$.

В случае, когда младший байт p – это `EB`, ответ получен быть не может, так как n не поделится на q нацело.

Ответ: $d = 41707$.

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 $\boldsymbol{x^{(2)}} = (x_1^{(2)}, \ldots, x_8^{(2)})$ по аналогичным формулам: $x_1^{(2)} = x_2^{(1)} \oplus k_2, \ldots$ 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 $\boldsymbol{x^{out}} = (0,0,0,0,0,1,1,1)$, а байт $\boldsymbol{x^{in}} = (1,1,1,1,1,1,1,1)$– в байт $\boldsymbol{x^{out}} = (1,0,0,1,1,1,0,1)$.

Решение: Обозначим $\boldsymbol{x^{in}} = \boldsymbol{x^{(0)}}$. На i-том такте выполняется преобразование $\boldsymbol{x^{(i)}} = \boldsymbol{f_i}(\boldsymbol{x^{(i-1)}})$, которое в покомпонентной записи выглядит, согласно условию, следующим образом:

$$x_1^{(i)} = x_2^{(i-1)} \oplus k_i, x_2^{(i)} = x_3^{(i-1)}, x_3^{(i)} = x_4^{(i-1)} \oplus k_i, x_4^{(i)} = x_5^{(i-1)}, x_5^{(i)} = x_6^{(i-1)} \oplus k_i, x_6^{(i)} = x_7^{(i-1)},\ x_7^{(i)} = x_8^{(i-1)} \oplus k_i, x_8^{(i)} = x_2^{(i-1)} x_7^{(i-1)} \oplus x_1^{(i-1)}.$$

Будем искать такой ключ $(k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$, чтобы пока только для первой пары $\boldsymbol{x^{(0)}}$, $\boldsymbol{x^{(8)}}$ (то есть для $\boldsymbol{x^{(0)}} = (1,0,1,0,1,0,1,0)$ и $\boldsymbol{x^{(8)}} = (0,0,0,0,0,1,1,1)$) выполнялось требуемое:

$$\boldsymbol{x^{(8)}} = \boldsymbol{f_8}\left(\boldsymbol{f_7}\left(\ldots \boldsymbol{f_1}\left(\boldsymbol{x^{(0)}}\right)\right)\right). \qquad (1)$$

Несложно проверить, что отображение $\boldsymbol{x^{(i-1)}} = \boldsymbol{g_i}(\boldsymbol{x^{(i)}})$, покомпонентная запись которого имеет вид

$$x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = x_6^{(i)},\ x_8^{(i-1)} = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}\left(x_1^{(i)} \oplus k_i\right),$$

является обратным к $\boldsymbol{x^{(i)}} = \boldsymbol{f_{i-1}}\left(\boldsymbol{x^{(i-1)}}\right)$. (Эти формулы обращения следуют из элементарных соображений типа $a = b \oplus c \Leftrightarrow b = a \oplus c$, поэтому выражение для $x_1^{(i-1)}$ естественно получить в последнюю очередь, когда остальные $x_j^{(i-1)}$ уже найдены.) Уравнение (1) эквивалентно уравнению $\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}\left(\boldsymbol{x^{(0)}}\right)\right)\right)\right) = \boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}\left(\boldsymbol{x^{(8)}}\right)\right)\right)\right)$. Последнее решается полным перебором "половинок" ключа: мы вычисляем правую часть при всевозможных значениях (k_5, k_6, k_7, k_8) (16 вариантов), а затем левую часть для всех (k_1, k_2, k_3, k_4) (также 16 вариантов). Те "половинки", при которых левая и правая части окажутся равными, дадут искомый ключ. Результаты вычислений представлены в таблице.

k_1, k_2, k_3, k_4	$\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}(\boldsymbol{x}^{(\mathbf{0})})\right)\right)\right)$	k_5, k_6, k_7, k_8	$\boldsymbol{g_5}\left(\boldsymbol{g_6}\left(\boldsymbol{g_7}\left(\boldsymbol{g_8}(\boldsymbol{x}^{(\mathbf{8})})\right)\right)\right)$
0 0 0 0	1 0 1 0 1 0 1 0	0 0 0 0	0 1 1 1 0 0 0 0
0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 1	0 1 0 0 1 0 1 0
0 0 1 0	1 1 1 1 1 1 1 0	0 0 1 0	0 1 1 0 0 1 0 1
0 0 1 1	0 1 0 1 0 1 0 0	0 0 1 1	0 1 1 1 1 1 1 1
0 1 0 0	0 0 0 0 0 0 0 0	0 1 0 0	0 1 0 1 1 0 1 0
0 1 0 1	1 0 1 0 1 0 1 0	0 1 0 1	0 1 1 0 0 0 0 0
0 1 1 0	0 1 0 1 0 1 0 1	0 1 1 0	1 0 0 0 1 1 1 1
0 1 1 1	1 1 1 1 1 1 1 1	0 1 1 1	0 0 0 1 0 1 0 1
1 0 0 0	1 1 1 1 1 0 0 1	1 0 0 0	0 0 1 0 0 1 0 1
1 0 0 1	0 1 0 1 0 0 1 1	1 0 0 1	1 0 0 1 1 1 1 1
1 0 1 0	1 0 1 0 1 1 0 1	1 0 1 0	0 0 1 1 0 0 0 0
1 0 1 1	0 0 0 0 0 1 1 1	1 0 1 1	1 0 1 0 1 0 1 0
1 1 0 0	0 1 0 1 0 0 0 1	1 1 0 0	1 0 0 0 1 1 1 1
1 1 0 1	1 1 1 1 1 0 1 1	1 1 0 1	0 0 1 1 0 1 0 1
1 1 1 0	0 0 0 0 0 1 0 0	1 1 1 0	0 1 0 1 1 0 1 0
1 1 1 1	1 0 1 0 1 1 1 0	1 1 1 1	0 1 0 0 0 0 0 0

Имеется, таким образом, два ключа, $\boldsymbol{k_1} = (0, 0, 0, 0, 1, 0, 1, 1)$ и $\boldsymbol{k_2} = (0, 1, 0, 1, 1, 0, 1, 1)$, на которых для первой пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ выполняется (1). Непосредственной проверкой убеждаемся, что на ключе $\boldsymbol{k_1}$ для второй пары $\boldsymbol{x}^{(\mathbf{0})}$, $\boldsymbol{x}^{(\mathbf{8})}$ равенство (1) также выполняется, а на ключе $\boldsymbol{k_2}$ – нет.

Ответ: $0, 0, 0, 0, 1, 0, 1, 1$.