РЕШЕНИЯ ЗАДАЧ

Задача 1

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

Задача 2

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	2
3	0011	2,5
4	0100	4
5	0101	4,5
6	0110	2,4
7	0111	2,4,5

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

Задача 3

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.

Задача 4

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:

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

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.

Задача 5

а) Например,

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

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, $k \le n-1$. Утверждение доказано.

Задача 6

Обозначим $\boldsymbol{x^{in}} = \boldsymbol{x^{(0)}}$. На i-том такте выполняется преобразование $\boldsymbol{x^{(i)}} = \boldsymbol{f_i}\left(\boldsymbol{x^{(i-1)}}\right)$, 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

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

Несложно проверить, что отображение $\boldsymbol{x^{(i-1)}} = \boldsymbol{g_i}\left(\boldsymbol{x^{(i)}}\right)$, 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	$f_4\left(f_3\left(f_2\left(f_1\left(x^{(0)}\right)\right)\right)\right)$	k_5, k_6, k_7, k_8	$g_5\left(g_6\left(g_7\left(g_8\left(x^{(8)}\right)\right)\right)\right)$
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	1 0 1 0	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
1 1 0 1	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.