

РЕШЕНИЯ ЗАДАЧ

Задача 1

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

Задача 2

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.

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:

$$1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 16 \rightarrow 17 \rightarrow 15 \rightarrow 19 \rightarrow 11 \rightarrow 22 \rightarrow 5 \rightarrow 10 \rightarrow 20 \rightarrow 9 \rightarrow 18 \rightarrow 13 \rightarrow 23 \rightarrow 3 \rightarrow 6 \rightarrow 12 \rightarrow 24 \rightarrow 1 \rightarrow \dots$$

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: $7 \rightarrow 14 \rightarrow 21 \rightarrow 7 \rightarrow \dots$

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.

Задача 4

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:

$$x^2 + 61x + 11 = 73 + 83t \quad (t \in \mathbb{Z}) \Leftrightarrow x^2 + 61x - 62 = 83t \Leftrightarrow \\ \Leftrightarrow (x - 1)(x + 62) = 83t.$$

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

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

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

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

Ответ: $k_{BC} = 13$.

Задача 5

а) Например,

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

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: $\begin{matrix} & 3 & 1 & 2 \\ 3 & 1 & 2 & \\ & 2 & 3 & 1 \end{matrix}$. 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 разобранным 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.

Задача 6

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

$$x^{(8)} = f_8(f_7(\dots f_1(x^{(0)}))). \quad (1)$$

Несложно проверить, что отображение $x^{(i-1)} = g_i(x^{(i)})$, покомпонентная запись которого имеет вид
 $x_2^{(i-1)} = x_1^{(i)} \oplus k_i, x_3^{(i-1)} = x_2^{(i)}, x_4^{(i-1)} = x_3^{(i)} \oplus k_i, x_5^{(i-1)} = x_4^{(i)}, x_6^{(i-1)} = x_5^{(i)} \oplus k_i, x_7^{(i-1)} = x_6^{(i)},$
 $x_8^{(i-1)} = x_7^{(i)} \oplus k_i, x_1^{(i-1)} = x_8^{(i)} \oplus x_6^{(i)}(x_1^{(i)} \oplus k_i),$

является обратным к $x^{(i)} = f_{i-1}(x^{(i-1)})$. (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

$$f_4(f_3(f_2(f_1(x^{(0)})))) = g_5(g_6(g_7(g_8(x^{(8)})))).$$

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.

XXVII Межрегиональная олимпиада школьников по математике и криптографии

k_1, k_2, k_3, k_4	$f_4(f_3(f_2(f_1(x^{(0)}))))$	k_5, k_6, k_7, k_8	$g_5(g_6(g_7(g_8(x^{(8)}))))$
0000	00000000	0000	11001110
0001	10101010	0001	11010100
0010	01010101	0010	00011011
0011	11111111	0011	11100001
0100	10101010	0100	11100100
0101	00000000	0101	11111110
0110	11111110	0110	11110001
0111	01010100	0111	00001011
1000	01010101	1000	00011011
1001	11111111	1001	10000001
1010	00000000	1010	11001110
1011	10101010	1011	10110100
1100	11111100	1100	10110001
1101	01010110	1101	00101011
1110	10101000	1110	10100100
1111	00000010	1111	11011110

Ответ: 0, 1, 1, 0, 0, 1, 0, 1.