РЕШЕНИЯ ЗАДАЧ

Задача 1

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.

Задача 2

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.

Задача 3

Докажем утверждение индукцией по k (числу наборов).

1) Для одного набора $\mathbf{w_1}$ утверждение очевидно.
2) Предположим, что утверждение верно для любых $k-1$ различных наборов ($k > 1$).
3) 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.

Задача 4

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).

вхо	ПР и	ПР и	ПР и	Н1 и	Н1 и	Н2 и
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}.

Задача 5

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

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

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 $d \leq 65535$. 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: $d = 42203$.

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:

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

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:

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

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	$\boldsymbol{f_4}\left(\boldsymbol{f_3}\left(\boldsymbol{f_2}\left(\boldsymbol{f_1}(\boldsymbol{x^{(0)}})\right)\right)\right)$	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	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 $\boldsymbol{x^{(0)}}$, $\boldsymbol{x^{(8)}}$ выполняется (1). Непосредственной проверкой убеждаемся, что на ключе $\boldsymbol{k_2}$ для второй пары $\boldsymbol{x^{(0)}}$, $\boldsymbol{x^{(8)}}$ равенство (1) также выполняется, а на ключе $\boldsymbol{k_1}$ – нет.

Ответ: $0, 0, 1, 0, 1, 1, 1, 1$.