РЕШЕНИЯ ЗАДАЧ

Задача 1

Пусть $p_1 < p_2 < p_3$. По условию $p^3 - 2p^2 - 16p + 32 = p_1 \cdot p_2 \cdot p_3$. Разложим левую часть на множители:

$$(p-2)(p-4)(p+4) = p_1 \cdot p_2 \cdot p_3. \qquad (1)$$

Непосредственной проверкой убеждаемся, что $p \neq 2,3,5$. Значит $p > 5$. Следовательно, числа в левой части (1) различны и отличны от 1. Поэтому $p-4 = p_1,\ p-2 = p_2,\ p+4 = p_3$. Поскольку p на 3 не делится, возможны случаи:

- число p при делении на 3 дает остаток 1. Тогда на 3 делится число $p-4$. Такое возможно только, когда $p-4 = 3$, так как число $p-4$ простое. Отсюда $p = 7, p_1 = 3, p_2 = 5, p_3 = 11$.
- число p при делении на 3 дает остаток 2. Тогда на 3 делится $p+4$. Значит $p+4 = 3$, что невозможно.

Ответ: $p = 7, p_1 = 3, p_2 = 5, p_3 = 11$ (при условии $p_1 < p_2 < p_3$).

Задача 2

Нетрудно понять, что длина слова $n = 7$, а также несложно найти остаток $r_{32}(19^{11}) = 11$.

Преобразуем зашифрованный текст в последовательность чисел:

$$y_0 = 10, y_1 = 9, y_2 = 27, y_3 = 22, y_4 = 13, y_5 = 1, y_6 = 13,$$
$$y_7 = 22, y_8 = 11.$$

Из условия следует, что $x_8 - x_0 = 11$. Рассмотрим разность

$$r_{32}(y_8 - y_0) = r_{32}(x_8 + 6x_8 \cdot k^3 + k - x_0 - 6x_0 \cdot k^3 - k) =$$
$$= r_{32}\big((1+6k^3)\cdot(x_8 - x_0)\big) = r_{32}\big(11 \cdot (1+6k^3)\big).$$

Имеем:

$$r_{32}\big(11 \cdot (1+6k^3)\big) = 1.$$

Заметим, что $r_{32}(3 \cdot 11) = 1$. Откуда находим $r_{32}(1+6k^3) = 3$. Значит,

$$1 + 6k^3 = 3 + 32t \Leftrightarrow 3k^3 = 1 + 16t \Leftrightarrow 33k^3 = 11 + 11 \cdot 16t$$

Значит, $r_{16}(33k^3) = r_{16}(k^3) = 11$. В итоге

$$k^3 = 11 + 16p.$$

При $p = 1$ получим $k^3 = 27$. Отсюда $k = 3$. Опробуем полученное значение. Согласно правилу зашифрования

$$y_1 = 9 = r_{32}(x_1 + 6x_1 \cdot 27 + 3) = r_{32}(x_1 \cdot 3 + 3),$$
$$\Leftrightarrow 3x_1 + 3 = 9 + 32t \Leftrightarrow 3x_1 = 6 + 32t$$

Т.е. $r_{32}(3x_1) = 6 \Longrightarrow r_{32}(x_1) = 2$. Продолжая дальше получим:

$$y_2 = 27 = r_{32}(x_2 + 6x_2 \cdot 27 + 3) = r_{32}(x_2 \cdot 3 + 3),$$
$$\Leftrightarrow 3x_2 + 3 = 27 + 32t \Leftrightarrow 3x_2 = 24 + 32t$$

Т.е. $r_{32}(3x_2) = 24 \Longrightarrow r_{32}(x_2) = 8$. В итоге получим

Ответ: ВИСОКОС.

Задача 3

Пусть w_0, x_0, y_0, z_0 – значения секретных битов w, x, y, z. Решим прежде задачу, предполагая, что все секретные биты равны нулю: $w_0 = x_0 = y_0 = z_0 = 0$. Затем в

уравнениях можно будет сделать замену $w \to w + w_0, \dots, z \to z + z_0$ и тем самым получить решение задачи в общем случае.

Запишем теперь какую-нибудь систему из четырех уравнений, которой удовлетворяют *только* нулевые значения. Например,

$$\begin{array}{llll} w + x = 0 & (1) & y + z = 0 & (3) \\ x + y = 0 & (2) & w + x + y = 0 & (4) \end{array}$$

Запишем еще одно уравнение, сложив эти четыре:

$$x + y + z = 0 \qquad (5)$$

Система из *любых* четырех уравнений из набора (1) – (5) имеет только нулевое решение.

Далее идея в следующем. Если пара абонентов должна уметь находить все биты, то этой паре выдадим четыре *различные* уравнения из набора (1) – (5), если же нет, то хоть одно уравнение у этой пары должно быть общим.

Замечание. *Здесь нет четких алгоритмов и успех заранее не гарантирован. Возможно, следовало выбрать какие-то другие уравнения (1) – (4). Заметим, например, что абонентам, которые не должны уметь находить секрет, нельзя выдать уравнения (1), (2) и (4), так как значение бита z они не найдут, но определят, что* $w = x = y = 0$, *а это по условию недопустимо. Никакому абоненту нельзя выдать уравнения (2) и (5), так как из них следует, что* $z = 0$.

Абонентам раздать уравнения можно так: A_1: (1), (2); A_2: (1), (5); A_3: (3), (4); A_4: (4), (5).
Выполнив замену, запишем ответ в общем случае.
Ответ: Например,

$$A_1: w + x = w_0 + x_0,\ x + y = x_0 + y_0;\ A_2:\ w + x = w_0 + x_0,\ x + y + z = x_0 + y_0 + z_0;$$
$$A_3: y + z = y_0 + z_0,\ \ w + x + y = w_0 + x_0 + y_0;$$
$$A_4: w + x + y = w_0 + x_0 + y_0,\ \ x + y + z = x_0 + y_0 + z_0.$$

Задача 4

По условию числа u_k прибавляются к битам открытого текста, а результат заменяется остатком от деления на 2 (то есть на 0 или 1). Поэтому сразу заменим u_k его остатком от деления на 2: считаем, что $u_k = 0$ (если изначально u_k было четным) или $u_k = 1$ (если оно было нечетным). Вычисление остатка от деления на 32 при построении последовательности $u_1, u_2, \dots$ никакой роли не играет (четные числа дают четный остаток, а нечетные – нечетный).

Оказывается, в зависимости от четности чисел Д , М могут быть получены всего три различные последовательности $u_1, u_2, \dots$, а именно:

1. Числа Д , М нечетные. Тогда $u_1 = 0, u_2 = 1, u_3 = 0, \dots$
2. Числа Д , М имеют разную четность. Тогда $u_1 = 1, u_2 = 0, u_3 = 1, \dots$
3. Числа Д , М четные. Тогда $u_1 = u_2 = \dots = u_{32} = 0$. В этом случае текст Машиной записки остался бы без изменения, что, очевидно, не так.

Далее необходимо в первых двух случаях вычислить последовательность $\{u_n\}$ полностью, вычесть ее из зашифрованного текста (**ЗТ**) и убедиться, что читаемый вариант получается во втором случае (см. таблицу).

	Ж	Д	У	Л	Щ	Б	Ш	Л	У	В	Ш	Ц	Ч
	00110	00100	10011	01011	11001	00001	11000	01011	10011	00010	11000	10110	10111
1. Д, М **нечетные**													
$\{u_n\}$	01001	00100	10010	01001	00100	10010	01001	00100	10000	01001	00100	10010	01001
ЗТ-u_n	01111	00000	00001	00010	11101	10011	10001	01111	00011	01011	11100	00100	11110
	П	А	Б	В	Э	У	С	П	Г	Л	Ь	Д	Ю
2. Д, М **разной четности**													
$\{u_n\}$	10111	01110	11101	11011	10111	01110	11101	11011	10110	01110	11101	11011	10111
ЗТ-u_n	10001	01010	01110	10000	01110	01111	00101	10000	00101	01100	00101	01101	00000
	С	К	О	Р	О	П	Е	Р	Е	М	Е	Н	А

Ответ: **СКОРОПЕРЕМЕНА**

Задача 5

Решим задачу в общем случае, когда передача длилась n секунд. Так как переключение между читающими головками происходит раз в секунду, весь звук можно разбить на n фрагментов по 1 секунде и тогда звук, переданный в линию, будет перестановкой этих фрагментов. Обозначис количество возможных перестановок $T(n)$.

Представим весь процесс в виде таблицы, элементами которой являются номера фрагментов. Например, на второй секунде, с которой начинается передача, на пишущей головке будет 3-ий фрагмент звука, 2-ой фрагмент будет на (2)-ой читающей головке, а 1-ый фрагмент на (3)-ей читающей головке. Передача закончится на $n+1$ секунде.

Сек.	Пишущая головка	Читающая головка			В линию передан
		(2)	(3)	(4)	
0	1	–	–	–	–
1	2	1	–	–	–
2	3	2	1	–	2 или 1
3	4	3	2	1	3, 2 или 1
4	5	4	3	2	4, 3 или 2
…	…	…	…	…	
$n-1$	n	$n-1$	$n-2$	$n-3$	
n	–	n	$n-1$	$n-2$	
$n+1$	–	–	n	$n-1$	n или $n-1$

На $n+1$ секунде в линию может быть передан n или $n-1$ фрагмент звука. По очереди рассмотрим оба случая.

1. Пусть на $n+1$ секунде в линию был передан n-ый фрагмент (см. таблицу). Тогда n-ый фрагмент не мог быть передан на предыдущей секунде. Если посмотреть на таблицу то видно, что количество перестановок фрагментов в этом случае совпадает с $T(n-1)$, то есть количеством способов переставить звук длины $n-1$.

Читающая головка			В линию
(2)	(3)	(4)	
2	1	–	2 или 1
3	2	1	3, 2 или 1
4	3	2	4, 3 или 2
…	…	…	
$n-1$	$n-2$	$n-3$	
n	$n-1$	$n-2$	$n-1$ или $n-2$
–	$\boldsymbol{n}$	$n-1$	n

2. Пусть на $n+1$ секунде в линию был передан $(n-1)$-ый фрагмент (см. таблицу). Тогда $(n-1)$-ый фрагмент не мог быть передан на предыдущих секундах. Так как n-ый фрагмент должен уйти в линию, то он должен быть передан в момент времени n. Тогда до $(n-1)$-ой должно быть передано $(n-2)$ последовательных фрагментов, что может быть сделано $T(n-2)$ способами.

Читающая головка			В линию
(2)	(3)	(4)	
2	1	–	2 или 1
3	2	1	3, 2 или 1
4	3	2	4, 3 или 2
…	…	…	
$n-1$	$n-2$	$n-3$	$n-2$ или $n-3$
$\boldsymbol{n}$	$n-1$	$n-2$	n
–	n	$\boldsymbol{n-1}$	$n-1$

Таким образом $T(n) = T(n-1) + T(n-2)$. Тогда для нахождения количества перестановок $T(n)$ для любого n, достаточно найти $T(1)$, $T(2)$.

Читающая головка			В линию
(2)	(3)	(4)	
–	1	–	1

$$T(1) = 1$$

Читающая головка			В линию
(2)	(3)	(4)	
2	1	–	2 или 1
–	2	1	2 или 1

$$T(2) = 2$$

Остается с использованием формулы $T(n) = T(n-1) + T(n-2)$ вычислить нужное значение.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946

Ответ. 10946

Задача 6

Для каждого набора $\boldsymbol{k} = (k_1, \dots, k_9)$ укажем такое минимальное l, что в соответствующей последовательности $u_1, u_2, \dots, u_l$ присутствует каждое из чисел 0, 1 и 2. Затем среди всех таких l останется выбрать наибольшее – это и будет ответом в задаче.

1. В наборе $\boldsymbol{k}$ встречается каждое из чисел 0, 1 и 2. Тогда искомое l не превосходит 9;
2. Набор $\boldsymbol{k}$ состоит только из 1. Тогда $u_{10} = \dots = u_{17} = 2$ и $u_{18} = 0$. Значит $l = 18$;
3. В наборе $\boldsymbol{k}$ присутствуют и 1, и 2, но нет 0. Значит среди чисел $u_1, u_2, \dots, u_9$ есть два соседних (u_s и u_{s+1}), одно из которых равно 1, а другое 2. Тогда $u_{s+9} = 0$ и $l \le 17$;
4. Набор $\boldsymbol{k}$ состоит из 0 и 1. Число 2 впоследствии дадут только две рядом стоящие 1. Поэтому рассмотрим варианты:
   a) в $\boldsymbol{k}$ есть рядом стоящие 1. Тогда $l < 19$;
   b) в $\boldsymbol{k}$ нет рядом стоящих 1. Здесь возможны следующие случаи:
      - Есть хоть одна 1 «не с краю». То есть найдется номер s такой, что $2 \le s \le 8$ и $k_s = 1$. Рядом стоящих 1 нет, поэтому $k_{s-1} = k_{s+1} = 0$. Тогда $u_{s+8} = u_{s+9} = 1$. Следовательно, $u_{s+17} = 2$ и $l \le 25$;
      - 1 есть только «с краю». Пусть $\boldsymbol{k} = (1, 0, \dots, 0)$. В этом случае начало последовательности $u_1, u_2, \dots$ можно вычислить непосредственно: $\{u_n\} = \{1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,$

0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0,…} и убедиться, что $l = 27$. Пусть $\boldsymbol{k} = (1,0,\ldots 0,1)$. Тогда $\{u_n\}$ ={1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0…} и $l = 18$. И, наконец, для $\boldsymbol{k} = (0,\ldots 0,1)$ находим $\{u_n\}$ ={0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0, …}, $l = 26$.

Отметим, что случаи, «$\boldsymbol{k}$ состоит только из 2» и «$\boldsymbol{k}$ состоит только из 0 и 2» эквивалентны случаям 2 и 4 соответственно. Действительно, если в последовательности $\{u_n\}$, отвечающей набору $2 \cdot \boldsymbol{k}$, заменить все 2 на 1, а 1 на 2, то получится последовательность, соответствующая набору $\boldsymbol{k}$.

Ответ: $l = 27$.