Задание на десятую неделю.

№1

$$e = 17, q = 23, N = 391$$
$$\Rightarrow d = 3^{-a} \mod 352 = -117 = 235$$

Шифрование:

$$y = 41^3 \mod 391 = 105$$

Дешифррование:

$$x = 105^{235} \mod 391$$
$$391 = 23 \cdot 17$$
$$105_{17}^{235} \equiv 105_{17}^{11} \equiv 3_{17}^{11} = 7$$
$$105_{23}^{235} \equiv 105_{23}^{15} \equiv 10_{23}^{15} = 10^3 \cdot 5_{23}^3 = 10^3 \cdot 10_{23} = 5$$

Из великой китайской теореме об остатках:

$$x = 17k - 7 = 23t + 5 = 41$$

№2

Злоумышленник знает $pq = N$ и $d = e^{-1} \mod (p-1)(q-1) < (p-1)(q-1)$.

$$\Rightarrow de - 1 = (p-1)(q-1)k, k \in N$$
$$0 < de = 3d < 3(p-1)(q-1), \Rightarrow 0 \leq (p-1)(q-1)k \leq 3N$$
$$\Rightarrow 0 \leq k \leq 3.$$

Таким образом, k, а значит и $\alpha = (p-1)(q-1)$ может принимать четыре значения. Для каждого возможного $\alpha = pq+1-p-q$, найдем из системы уравнений (решение квадратного уравнение, полиномиальное время) p и q:

$$\begin{cases} N = pq \\ -\alpha + N + 1 = p + q \end{cases}$$

Найдем произведения чисел pq из полученных пар p, q и сравним с N. Таким образом, найдется искомое разложение.

№3

$$(25, 2021) = (e, N)$$

$$N = 2021 = 47 \cdot 43, (p-1)(q-1) = 42 \cdot 46 = 1932$$

Алгоритмом Евклида находим, $d = e^{-1} \mod 1932 = 541$.

№4

а) Рассмотрим массив длиной k. В нем точно есть хотя бы одна горка, т. к. если 1-ое число слева больше 2-го, то это горка. Если 2-ое больше, то последовательно попарно сравнивая числа, мы либо найдем горку, либо дойдем до крайнего правого k-го числа, которое больше $(k-1)$-го, т. е. горка.
Тогда, сначала проверим горка ли средний элемент, двумя сравнениями с его соседями. Если да, горка найдена. Если нет, пусть для определенности левый сосед был больше серединного элемента, то будем рассматривать только левую половину и искать горку уже в этом массиве длинной $\leq \lceil \frac{n}{2} \rceil$. Из вышесказанного, она обязательно найдется. Таким образом, мы можем каждый раз понижать сложность задачи в два раза:

$$T(n) = T(\lceil \frac{n}{2} \rceil) + 2 = O(\log n)$$

Т. е. данный алгоритм находит горку за $O(\log n)$ сравнений. б) Рассмотрим решающее дерево попарных сравнений, которое в конце на листьях должно выдавать элемент, котор. найден как горка. Всего возможных вариантов такого элемента: n, значит глубина дерева $\Theta(\log n)$. Таким образом, любой алгоритм должен использовать не менее $\Theta(\log n)$ попарных сравнений для нахождения ответа.
$\Rightarrow$ **Ответ:** $\Theta(\log n)$

№6

Данный язык L не принадлежит $co - NP$ (в предположение P≡NP), т. к. $L \in P$. Покажем это:

Если между s и t есть путь длины 10, то между ними есть путь длины S для всех четных $S > 10$, т. к. можно дойти до t за 10 ребер, потом вернуться на одно ребро назад и снова пройти его, и т. д. до нужной длины. Аналогично, если между s и t есть путь длины 11, то между ними есть путь для всех нечетных $S > 10$.
Т. е. (G, s, t) принадлежит языку $L \Leftrightarrow$ между s и t есть путь длиной 10 и 11. Проверим, наличие таких путей следующим способом:
Составим матрицу смежности A для графа. Тогда,

$$(G, s, t) \in L \Leftrightarrow A^{10}_{st} > 0, A^{11}_{st} > 0.$$

Возведение матриц в степень занимает $O(n^3)$, значит вся проверка принадлежности языку занимает полиномиальное время.